

# Bereitstellung von Benutzern und Gruppen für den sicheren Zugriff über eine zusätzliche ID

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurieren von Cisco Secure Access](#)

[Konfiguration der Bereitstellung in Microsoft Entra-ID](#)

[Überprüfung](#)

[Verify in Cisco Secure Access](#)

[Verifizieren in Entra-ID](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie Benutzer und Gruppen von Entra ID bis Cisco Secure Access bereitgestellt werden.

## Voraussetzungen

### Anforderungen

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

- Sicherer Zugriff von Cisco
- Eingabe-ID

### Verwendete Komponenten

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

- Administratorzugriff auf das Cisco Secure Access Dashboard
- Administratorzugriff auf das Entra-ID-Dashboard

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 aus Microsoft Entra ID (ehemals Azure Active Directory).

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 aus Entra ID. 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.

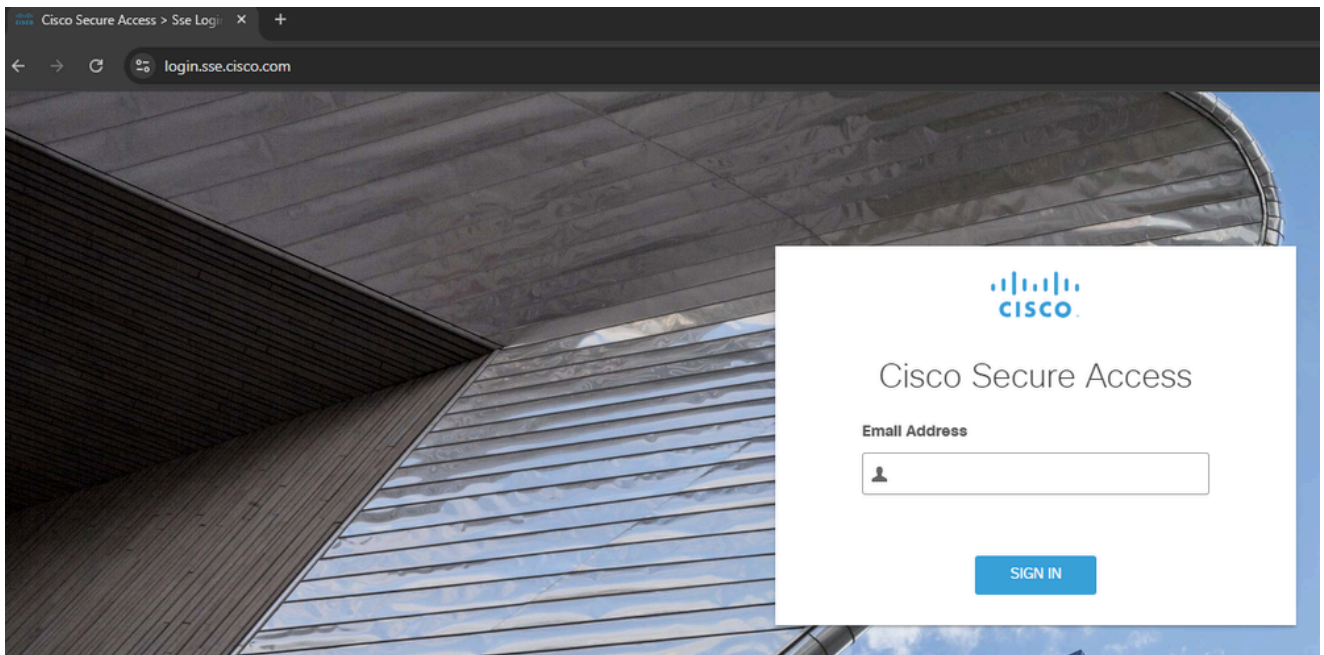
---

## Konfigurieren

### Konfigurieren von Cisco Secure Access

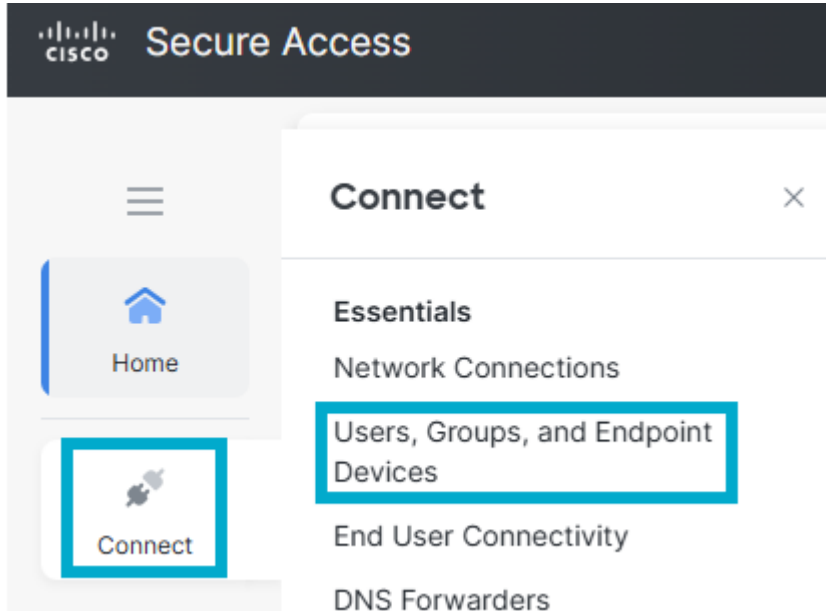
Um mit der Bereitstellung zu beginnen, müssen Sie zunächst die Verzeichnisintegration im Cisco Secure Access Dashboard konfigurieren. In diesem Schritt werden die erforderlichen Anmeldeinformationen und Konfigurationsparameter generiert, die zum Herstellen einer sicheren Verbindung mit der Microsoft Entra-ID erforderlich sind.

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



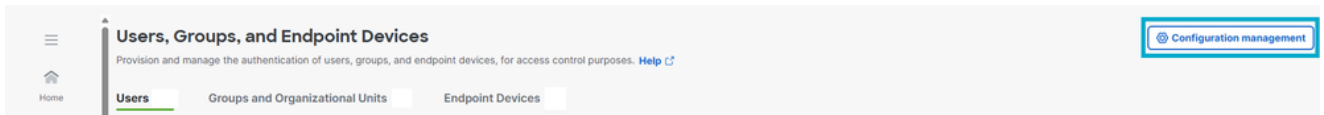
Bei CSA anmelden

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



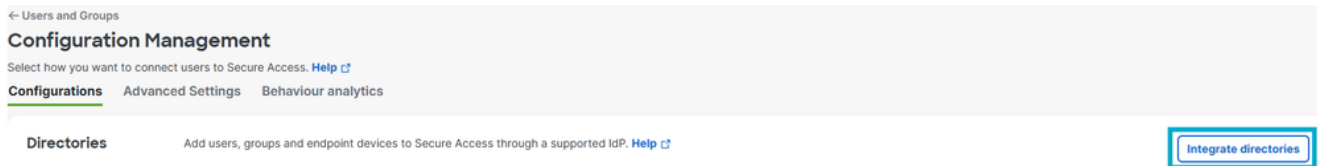
Benutzer und Gruppen

3. Klicken Sie auf **Konfigurationsmanagement**.



Konfigurationsverwaltung

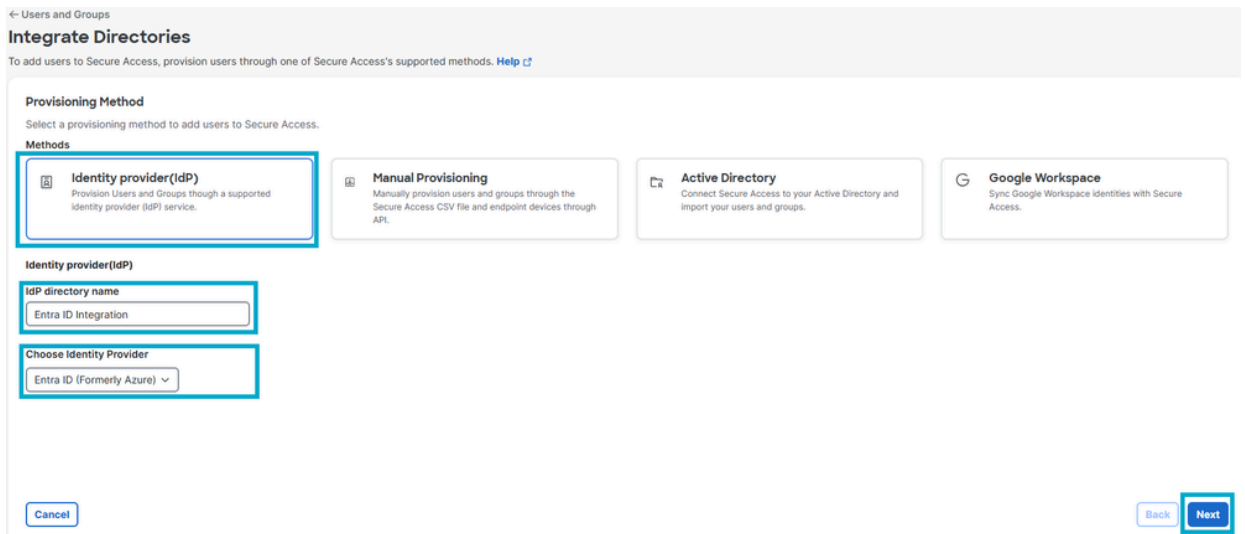
#### 4. Klicken Sie auf **Verzeichnis integrieren**.



Integrate Directory

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

- **IdP-Verzeichnisname: Integration von Entra-IDs.**
- **Identitätsanbieter auswählen: Entra ID (früher Azure).**
- 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**.

← Users and Groups

## Entra ID Integration

Entra ID (Formerly Azure)

Follow the instructions below to provision identities to this directory. [Help](#)

### Start Provisioning

To provision users to Secure Access, you must authenticate to your identity provider (IdP). Generate a token and then use it and the listed provisioning URL to provision users through your IdP. [Help](#)

#### Provisioning token

Once generated, copy and save this authentication token. It is required when configuring your IdP.

**⚠ For security reasons, your token will only be displayed once. For future reference, copy this token and keep it in a safe place**

Token  [Copy token](#) Generated On  
March 17, 2026

---

#### Provisioning URL

Copy and save this provisioning URL. It is required when configuring your IdP.

[Copy URL](#)

---

#### Configure your IdP portal

Use the generated authentication token and provisioning URL to set up Secure Access in your IdP. Once setup, you can provision users to Secure Access. [Help](#)

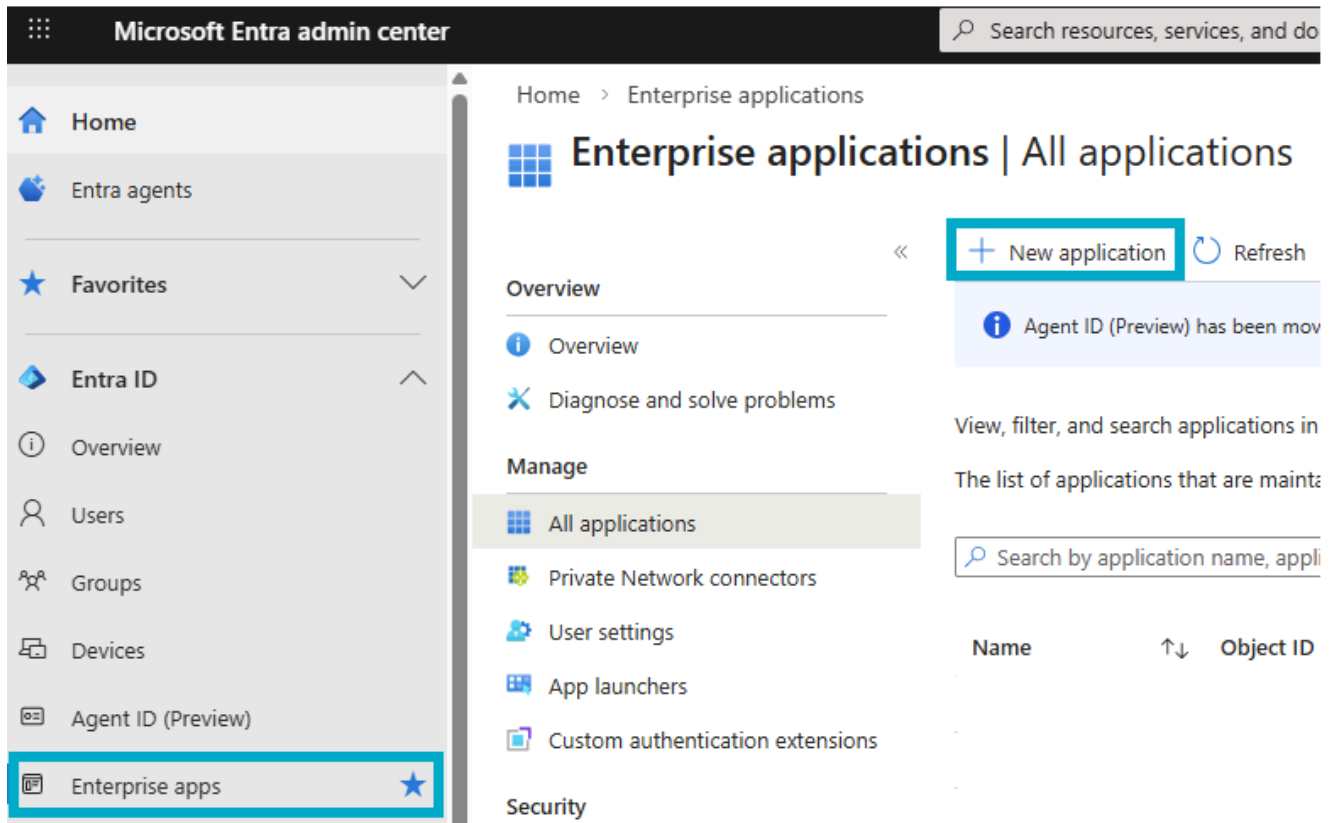
[Cancel](#) [Back](#) [Done](#)

Token generieren

## Konfiguration der Bereitstellung in Microsoft Entra-ID

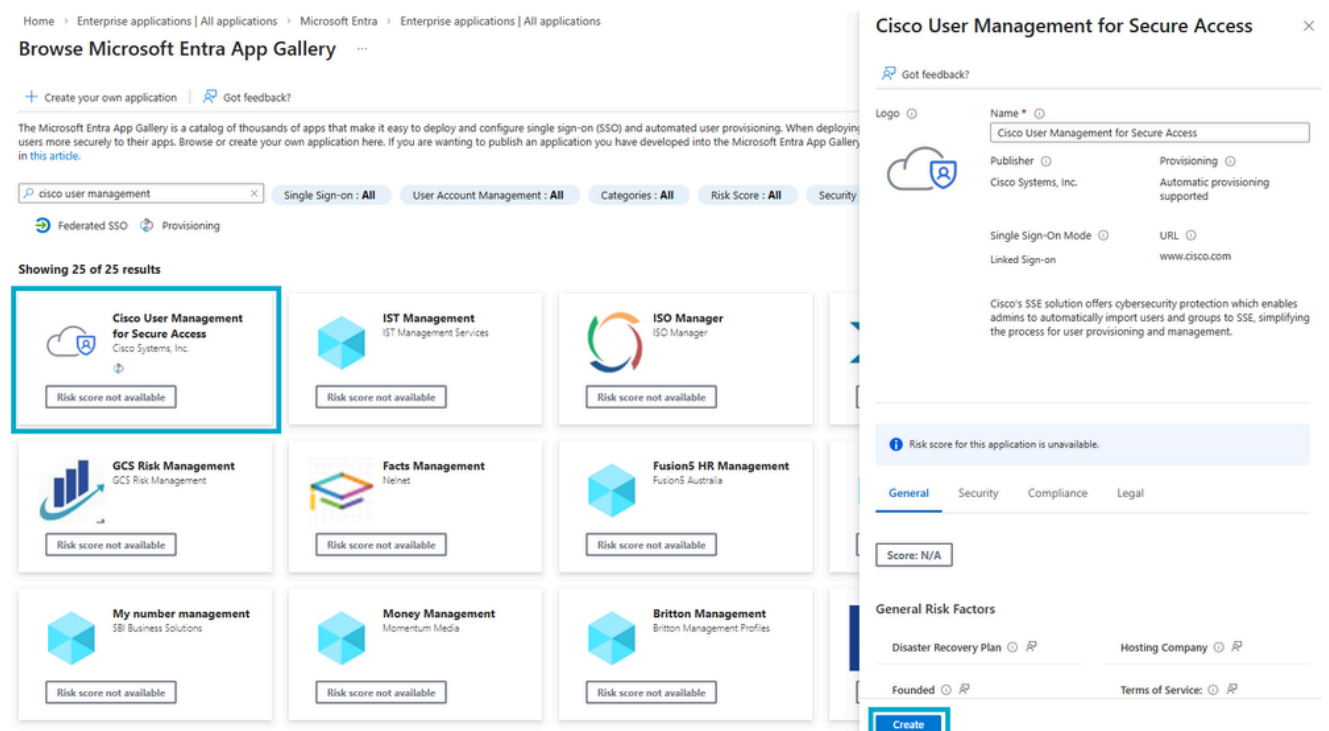
Nachdem Sie Ihre Anmeldeinformationen im Cisco Secure Access Dashboard generiert haben, müssen Sie die Bereitstellungseinstellungen im Microsoft Entra ID-Tenant konfigurieren, um die Synchronisierung von Benutzern und Gruppen zu ermöglichen.

1. Melden Sie sich bei der [Entra-ID an](#).
2. Navigieren Sie zu Enterprise-Anwendungen > Neue Anwendung.



Neue Enterprise-Anwendung

3. Suchen Sie in der Entra App Gallery nach Cisco User Management for Secure Access, und klicken Sie auf Erstellen.



New App

4. Navigieren Sie zu Benutzer und Gruppen > Benutzer/Gruppe hinzufügen.

The screenshot shows the Cisco User Management for Secure Access interface. The main heading is "Cisco User Management for Secure Access | Users and groups" with "Enterprise Application" below it. On the left, there is a navigation menu with options: Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, and Users and groups). The "Users and groups" option is highlighted with a blue box. At the top right, there are action buttons: "+ Add user/group" (highlighted with a blue box), "Edit assignment", "Remove assignment", and a search icon. Below these buttons is a light blue information banner with an 'i' icon and the text: "The application will appear for assigned users within My Apps. Set 'visible to us". Underneath the banner, there is a search bar containing the text "First 200 shown, search all users & groups". Below the search bar is a section titled "Display name" with a horizontal line. At the bottom of this section, it says "No application assignments found".

Zusätzliche Benutzer und Gruppen

5. Weisen Sie die bereitzustellenden Benutzer/Gruppen Cisco Secure Access zu, und klicken Sie auf Auswählen und dann auf Zuweisen.

## Add Assignment

MSFT

⚠ When you assign a group to an application, only users directly in the group will have access. Access does not cascade to nested groups.

### Users and groups

2 groups selected.

Select a role

User

Assign

## Users and groups



🔍 Try changing or adding filters if you don't see what you're looking for

Search

IT

2 results found

All Users Agent users Groups

	Name	Type
<input checked="" type="checkbox"/>	 IT-Admins	Group
<input checked="" type="checkbox"/>	 IT-Cloud-Admins	Group

Select

*Assign Users and Groups*

6. Navigieren Sie zu Provisioning.

Home > Enterprise applications | All applications

**Cisco User Management for Secure Access** | Overview ...  
Enterprise Application

**Properties**

Name  
Cisco User Management for...

Application ID  
dde39dfb-b7a9-4fc8-9aeb-...

Object ID  
2d3f9144-3d65-4235-9bd8-...

**Getting Started**

- 1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)
- 2. Set up single sign on**  
Enable users to sign into their application using their Microsoft Entra credentials  
[Get started](#)
- 3. Provision User Accounts**  
Automatically create and delete user accounts in the application  
[Get started](#)

Bereitstellung von zusätzlichen IDs

7. Klicken Sie auf Übersicht und dann auf Neue Konfiguration.

Home > Enterprise applications | All applications

**Cisco User Management for Secure Access** |

**Overview**

Provision on demand

**Manage**

**Get started**

+ New configuration ▶ Start provisioning

This is a new version of the provisioning

Neue Konfiguration

8. Geben Sie die Tenant-URL und das geheime Token ein, die aus Schritt #6 der Konfiguration für sicheren Zugriff gespeichert wurden. Klicken Sie auf Testkonfiguration und dann auf Erstellen.

Nach dem Erstellen der Konfiguration gelangen Sie zur Seite mit den Konfigurationsdetails, auf der Sie die erweiterten Einstellungen verwalten können.

## New provisioning configuration

Microsoft Entra ID

Got feedback?

This is a new version of the provisioning user experience. You can provide us feedback and suggestions on the new user experience using the "Got feedback" button. [Click here to switch to the legacy experience.](#)

Create a provisioning configuration by completing the setup below. You can edit attribute mappings, scoping rules, and other settings later in the setup. [Learn more](#)

### Admin credentials

Create automatic provisioning configuration for "Cisco User Management for Secure Access". A successful test connection may be required to proceed.

Tenant URL

Secret token

Test connection

### Next steps:

After creating your configuration with default parameters, you will be taken to the configuration details page to manage advanced settings.

Create Cancel

Testintegration

Provisioning test connection  
Connection test for "Cisco User Management for Secure Access" was successful.

## 9. Navigieren Sie zu Übersicht > Bereitstellung starten.

## Cisco User Management for Secure Access | Overview

Overview

Provision on demand

Manage

Start provisioning

Pause provisioning

Restart provisioning

Delete configuration

Refresh

Got feedback?

Get started

Overview

Properties

Bereitstellung starten

Start provisioning  
Start in progress

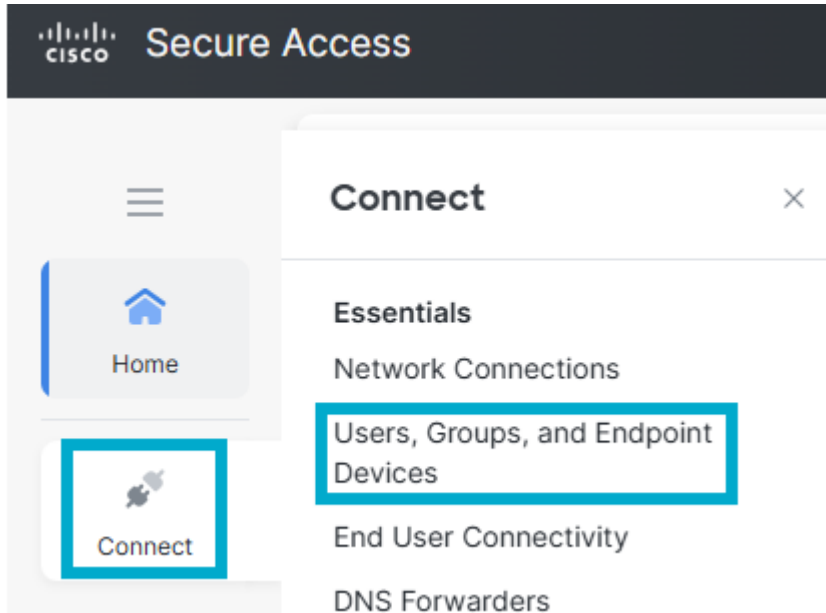


Anmerkung: Wenn die Benutzer/Gruppen im ursprünglichen Bereitstellungszyklus nicht bereitgestellt werden können, klicken Sie auf **Restart provisioning**. Diese Aktion erzwingt, dass Entra ID erneut versucht, die erste Synchronisierung der Benutzer und Gruppen durchzuführen.

## Überprüfung

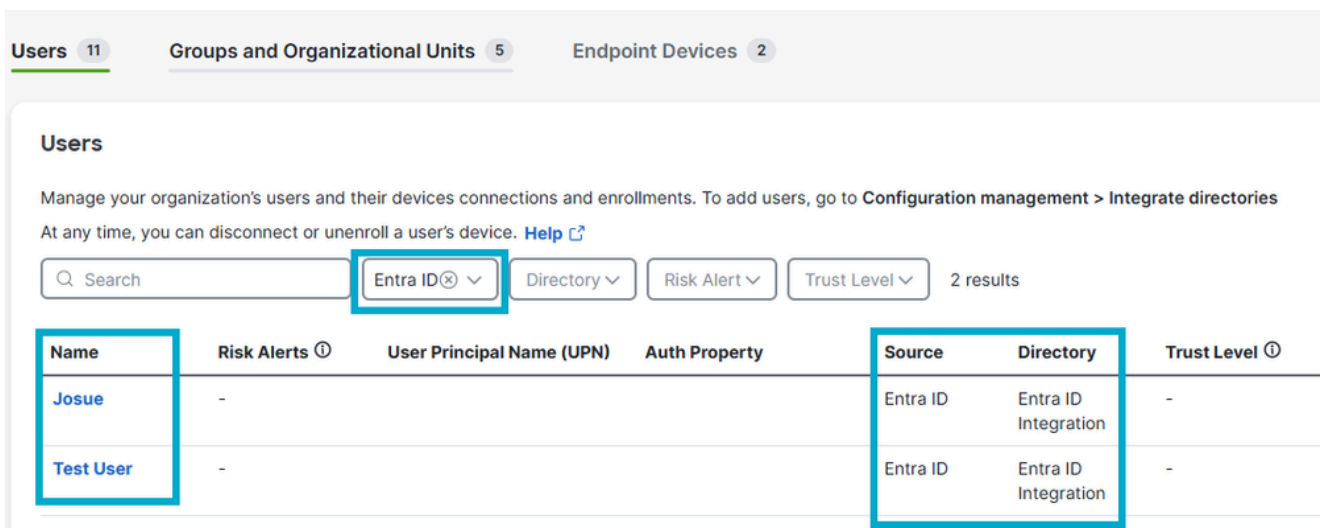
# Verity in Cisco Secure Access

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



Users and Groups in CSA

- Klicken Sie auf Benutzer.



Benutzer in CSA überprüfen

- Klicken Sie auf Gruppen und Organisationseinheiten.

Users 11   **Groups and Organizational Units** 5   Endpoint Devices 2

5 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 c**

Search   Type ▾   Source ▾   Entra ID Integration ⊗ ▾   2 results

Name	Type	Source	Directory
<a href="#">IT-Admins</a>	Groups	Entra ID	Entra ID Integration
<a href="#">IT-Cloud-Admins</a>	Groups	Entra ID	Entra ID Integration

Verify Groups in CSA

## Verifizieren in Entra-ID

- Navigieren Sie zu Enterprise Apps, und klicken Sie auf Cisco User Management for Secure Access.

Home   Entra agents

**Favorites** ▾

**Entra ID** ^

Overview

Users

Groups

Devices

Agent ID (Preview)

**Enterprise apps** ★

... > > > New provisioning configuration > Cisco User Management for Secure Access

## Enterprise applications | All applications

MSFT

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications**
- Private Network connectors
- User settings
- App launchers
- Custom authentication extensions

Security

«   + New application   Refresh   Download

**Agent ID (Preview) has been moved to the Agent I**

View, filter, and search applications in your organization

The list of applications that are maintained by your or

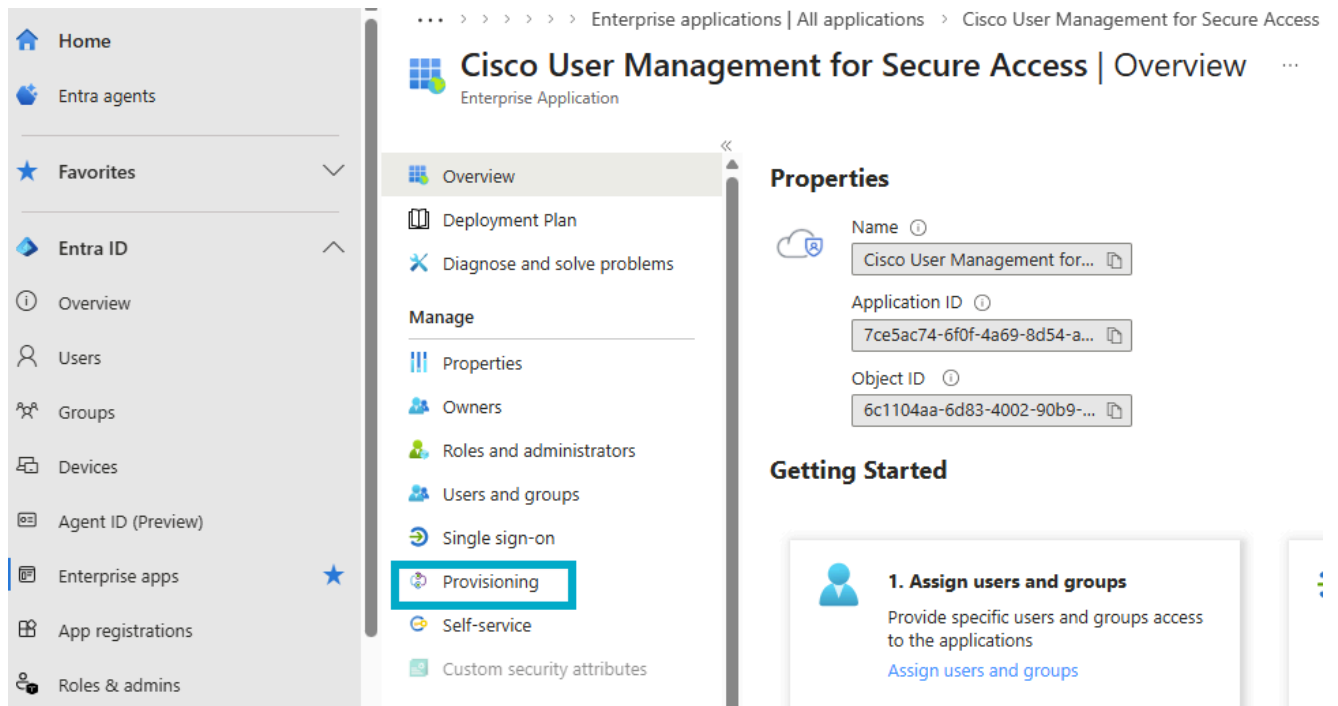
Search: cisco user management

1 application found

**Name**

**Cisco User Management for Secure Access**

- Klicken Sie auf Provisioning.



*Verify in Entra ID*

- Klicken Sie auf Übersicht.

# Cisco User Management for Secure Access | Overview

Start provisioning | Pause provisioning | Restart provisioning | Delete configuration | Refresh

This is a new version of the provisioning user experience. You can provide us feedback and suggestions on the new user

Get started | **Overview** | Properties

### Basic information

Name: Cisco User Management for Secure Access

Service principal object id

Job ID

Last cycle completed time: 3/18/2026, 10:27:27 AM

### Current cycle status

Current cycle status: Incremental sync completed > Provisioning details

100% completed

GROUP	USER
2	2

Verify Provisioning in Entra

- Klicken Sie auf Bereitstellungsprotokolle.

## Cisco User Management for Secure Access | Provisioning logs

Download | Refresh | Manage view | Got feedback?

Search Identity

Show dates as: Local | Date range: Last 24 hours | Action: All | Status: All

Date ↓	Identity	Action	Source system
3/18/26, 8:32:41 AM	Display name IT-Admins	Update	Microsoft Entra ID
3/18/26, 8:32:41 AM	Display name IT-Cloud-Admins	Update	Microsoft Entra ID
3/18/26, 8:32:39 AM	Disolav name IT-Admins	Create	Microsoft Entra ID
3/18/26, 8:32:39 AM	Display name IT-Cloud-Admins	Create	Microsoft Entra ID
3/18/26, 8:32:37 AM	Display name Test User	Create	Microsoft Entra ID
3/18/26, 8:32:37 AM	Display name Josue	Create	Microsoft Entra ID

## Zugehörige Informationen

[Identitätsanbieter konfigurieren](#)

[Bereitstellung von Benutzern und Gruppen über Microsoft Entra ID](#)

## 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.