

Gebruikers en groepen voorzien van beveiligde toegang via Entra ID

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Cisco Secure Access configureren](#)

[Provisioning configureren in Microsoft Entra ID](#)

[Verifiëren](#)

[Versie in Cisco Secure Access](#)

[Verifiëren in Entra ID](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe gebruikers en groepen van Entra ID naar Cisco Secure Access kunnen worden gedistribueerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Access
- Entra-ID

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

- Admin toegang tot Cisco Secure Access Dashboard
- Admin toegang tot Entra ID-dashboard

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco Secure Access ondersteunt de provisioning van gebruikers en groepen vanuit Microsoft Entra ID (voorheen Azure Active Directory).

Met deze voorziening kan Secure Access een directory bijhouden van gebruikers die geautoriseerd zijn om:

- Inschrijven bij Zero Trust Access (ZTA).
- Maak verbinding met VPNaaS.
- Pas op identiteit gebaseerd beleid toe op Umbrella Roaming-gebruikers.



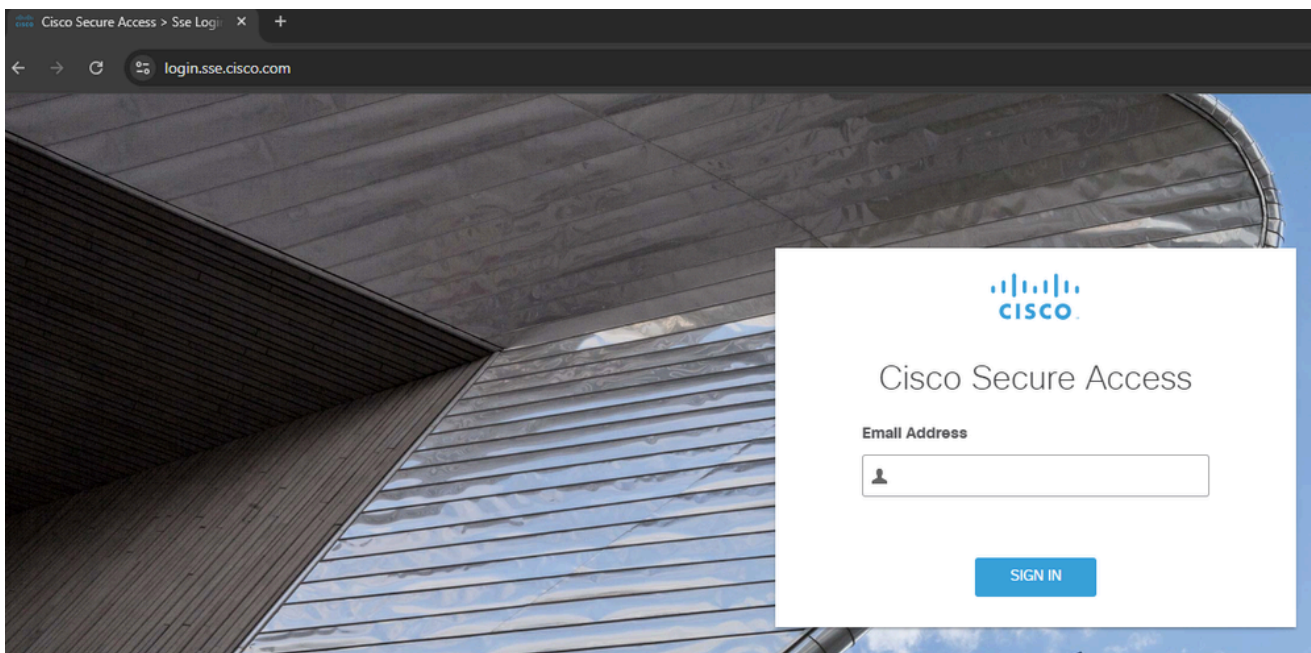
Opmerking: Dit document richt zich specifiek op de voorziening van gebruikers en groepen van Entra ID. De configuratie van Entra ID of andere Identity Providers (IdP) voor ZTA-inschrijving, VPNaaS-verificatie of specifieke Umbrella Roaming-instellingen valt buiten het bereik van deze handleiding.

Configureren

Cisco Secure Access configureren

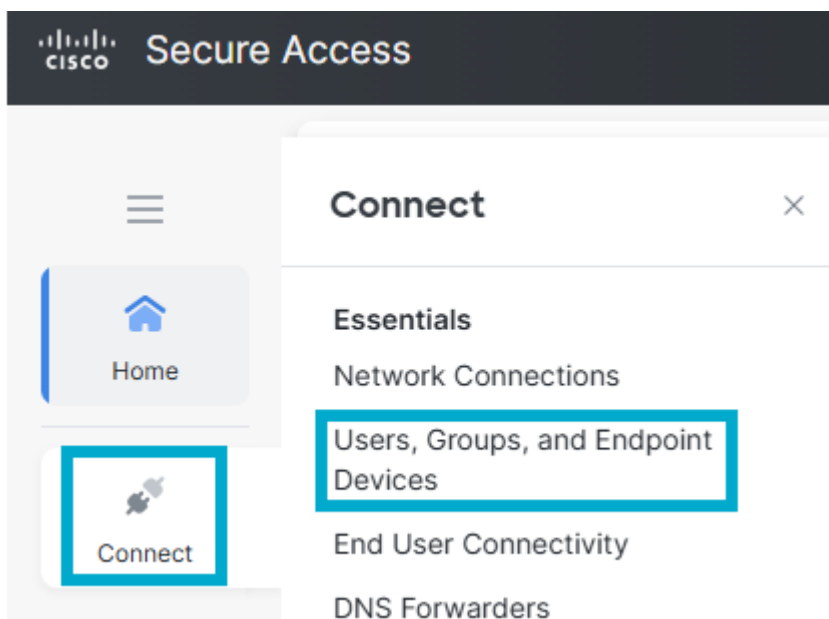
Om het provisioningproces te starten, moet u eerst de directory-integratie configureren in het Cisco Secure Access-dashboard. Deze stap genereert de nodige referenties en configuratieparameters die nodig zijn om een beveiligde verbinding met Microsoft Entra ID tot stand te brengen.

1. Meld u aan bij het **Cisco Secure Access Dashboard**.



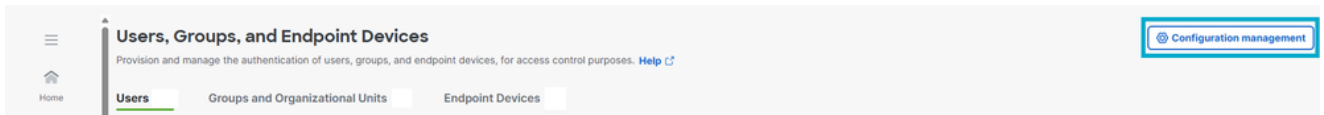
Inloggen bij CSA

2. Navigeer naar **Verbinden > Gebruikers, Groepen en Eindpuntapparaten**.



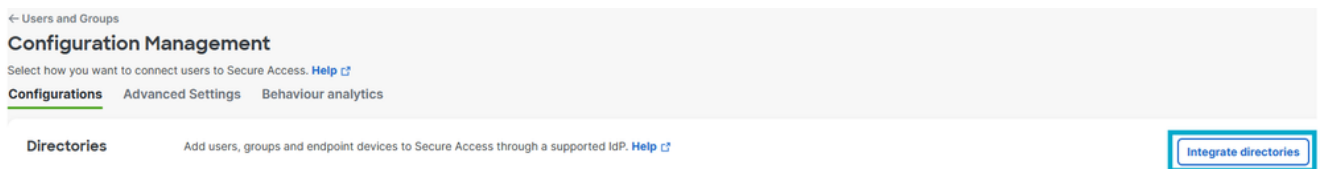
Gebruikers en groepen

3. Klik op **Configuratiebeheer**.



Configuratiebeheer

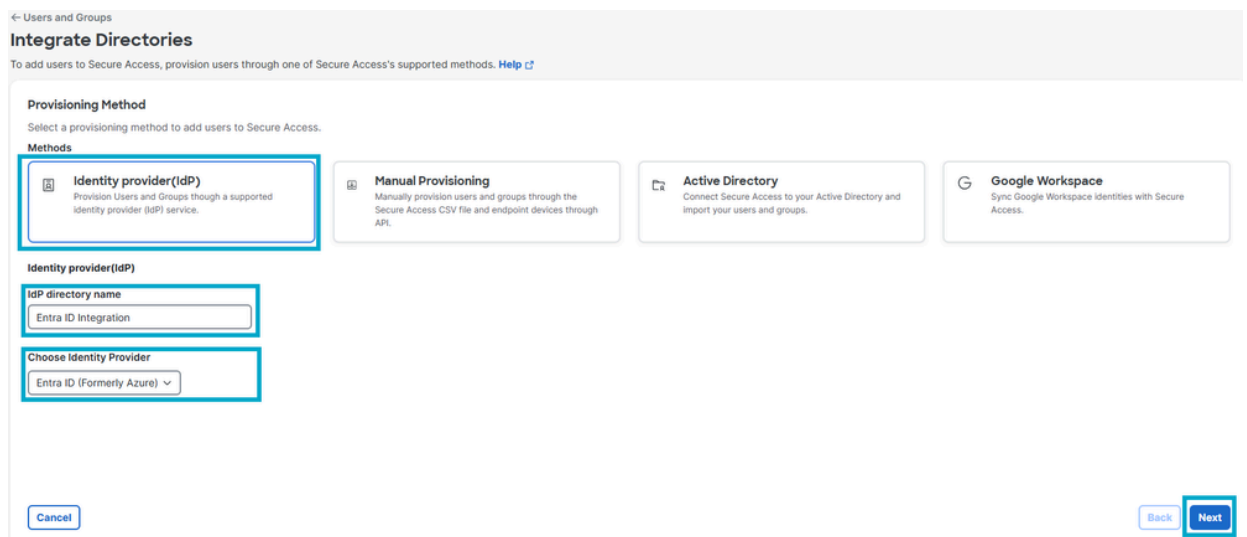
4. Klik op **Directory integreren**.



Integrate Directory

5. Klik onder **Provisioning Method** op **Identity Provider**.

- **IdP directory naam: Entra ID Integration.**
- **Kies Identity Provider: Entra ID (voorheen Azure).**
- **Klik op Next (Volgende).**



Directory-configuratie

6. Klik op **Token genereren**. Sla de **gegenereerde token** en de **provisioning-URL** op en klik op **Gereed**.

[← 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](#)

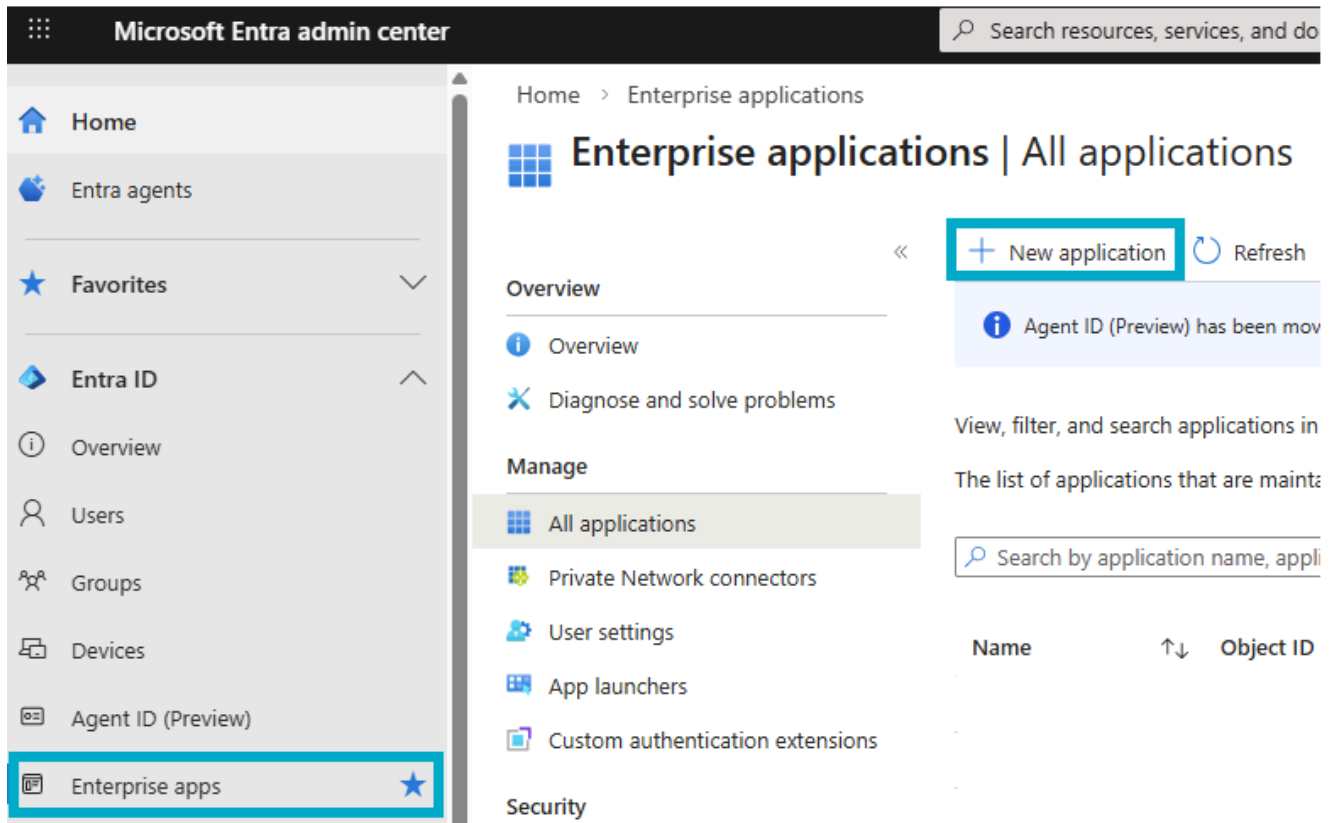
[Cancel](#) [Back](#) [Done](#)

Token genereren

Provisioning configureren in Microsoft Entra ID

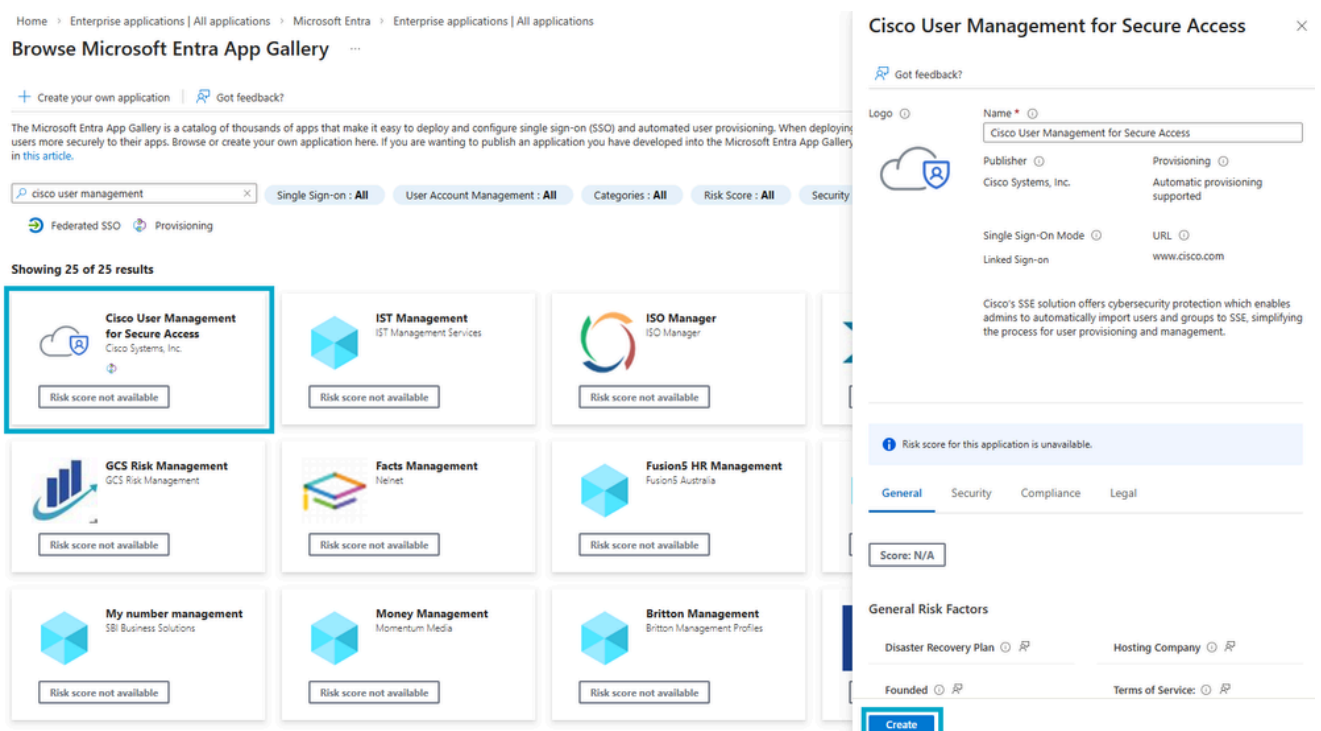
Nadat u uw referenties hebt gegenereerd in het Cisco Secure Access-dashboard, moet u de provisioning-instellingen configureren in uw Microsoft Entra ID-tenant om de synchronisatie van gebruikers en groepen mogelijk te maken.

1. Log in bij [Entra ID](#).
2. Navigeer naar Enterprise Apps > Nieuwe applicatie.



Nieuwe Enterprise-app

3. Zoek in de Entra App Gallery naar Cisco User Management for Secure Access en klik op Create.



New App

4. Navigeer naar Gebruikers en groepen > Gebruiker/groep toevoegen.

The screenshot shows the Cisco User Management for Secure Access interface. The title is "Cisco User Management for Secure Access | Users and groups" with "Enterprise Application" below it. On the left, there is a navigation menu with "Users and groups" highlighted. The main content area has a toolbar with "Add user/group" (highlighted with a red box), "Edit assignment", and "Remove assignment". Below the toolbar is a blue information banner: "The application will appear for assigned users within My Apps. Set 'visible to us". Underneath, there is a search box containing "First 200 shown, search all users & groups". A table header "Display name" is visible, followed by the text "No application assignments found".

Gebruikers en groepen invoeren

5. Wijs de gebruikers/groepen die u wilt aanbieden toe aan Cisco Secure Access en klik op Selecteren en vervolgens op Toewijzen.

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

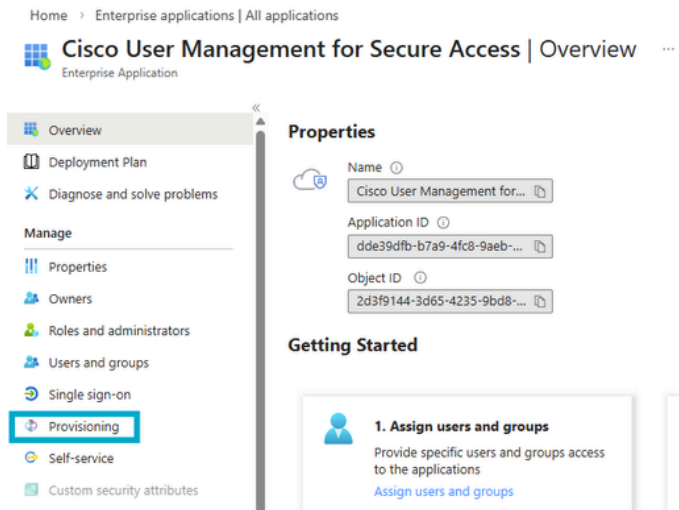
All Users Agent users Groups

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

Select

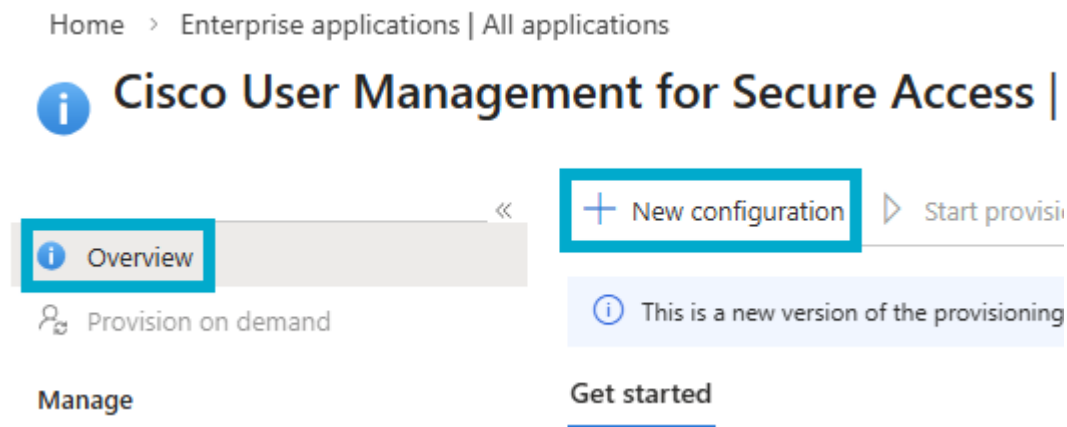
Assign Users and Groups

6. Navigeer naar Provisioning.



Invoer van ID-provisioning

7. Klik op Overzicht en vervolgens op Nieuwe configuratie.



Nieuwe configuratie

8. Voer de URL van de huurder en het geheime token in dat is opgeslagen in stap #6 van de Secure Access Configuratie. Klik op Testconfiguratie en vervolgens op Maken. Nadat u uw configuratie hebt gemaakt, gaat u naar de pagina Configuratiegegevens om geavanceerde instellingen te beheren.

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

Testintegratie

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

9. Ga naar Overzicht > Provisioning starten.

Cisco User Management for Secure Access | Overview

Overview Start provisioning Pause provisioning Restart provisioning Delete configuration Refresh Got feedback?

Provision on demand

Get started Overview Properties

Provisioning starten

Start provisioning
Start in progress

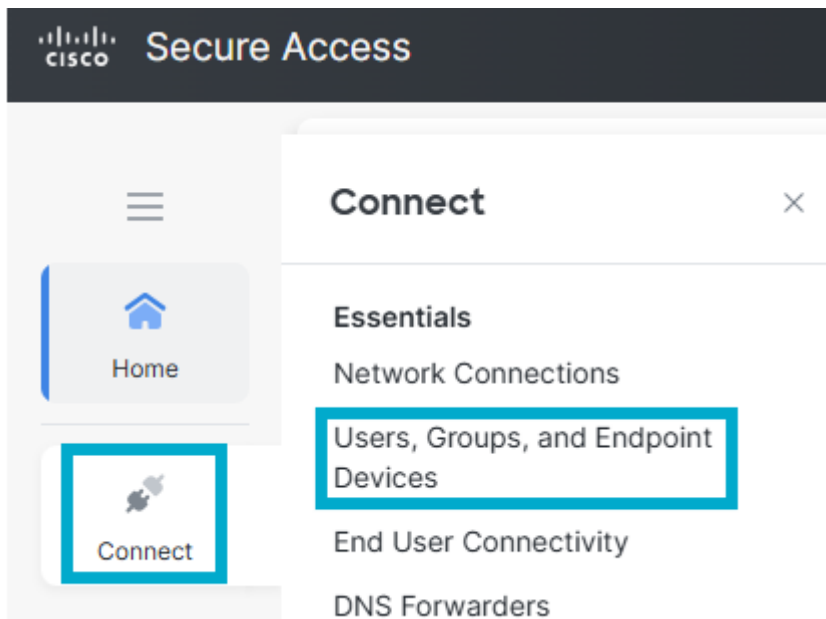


Opmerking: Als de eerste provisioningcyclus geen voorzieningen biedt voor de gebruikers/groepen, klikt u op **Restart provisioning**. Deze actie dwingt Entra ID om de eerste synchronisatie van uw gebruikers en groepen opnieuw te proberen.

Verifiëren

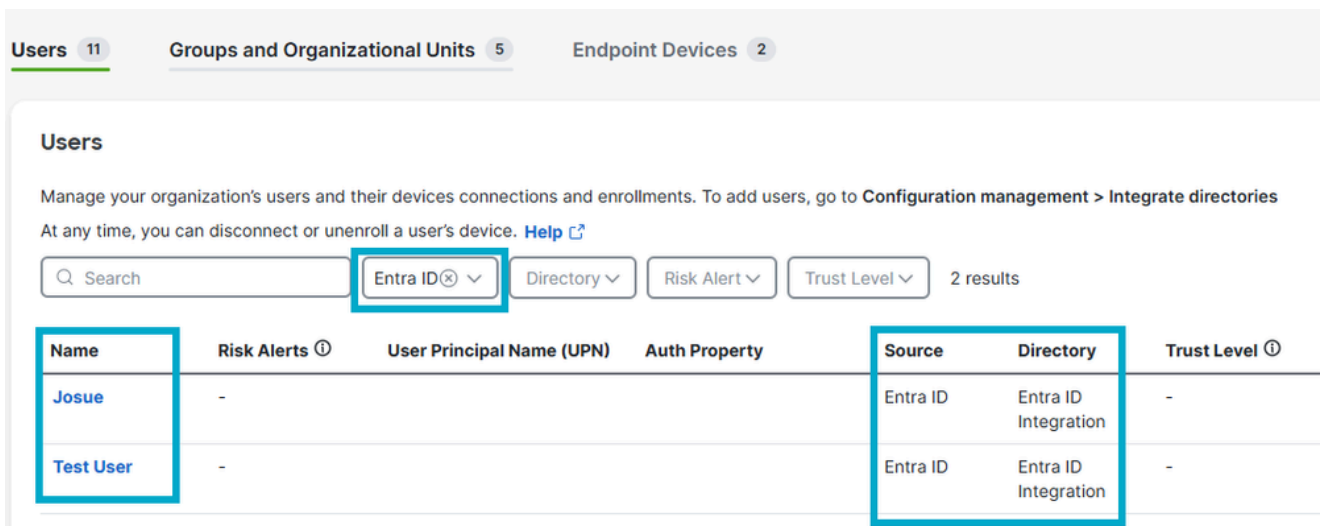
Versie in Cisco Secure Access

- Navigeer naar Verbinden > Gebruikers, Groepen en Eindpuntapparaten.



Users and Groups in CSA

- Klik op Gebruikers.



Gebruikers verifiëren in CSA

- Klik op Groepen en organisatie-eenheden.

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
IT-Admins	Groups	Entra ID	Entra ID Integration
IT-Cloud-Admins	Groups	Entra ID	Entra ID Integration

Verify Groups in CSA

Verifiëren in Entra ID

- Navigeer naar Enterprise Apps en klik op 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 organization.

Search: cisco user management

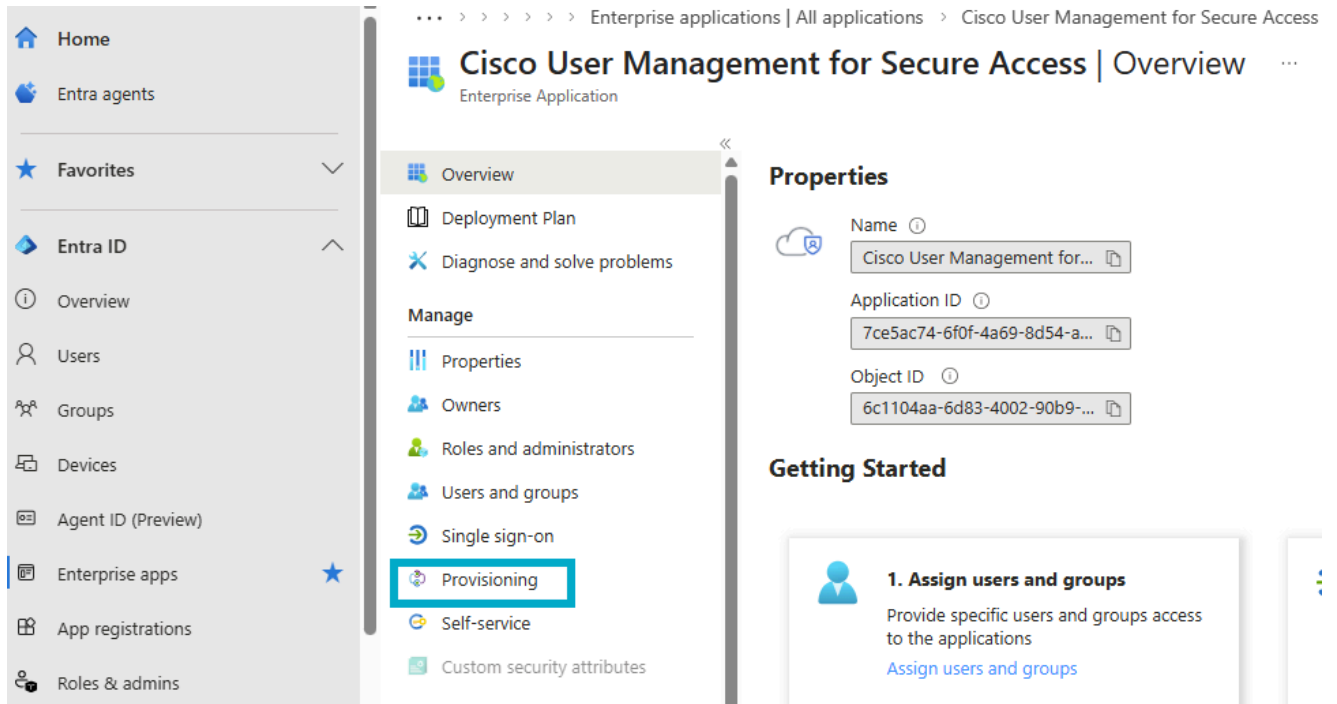
1 application found

Name

- Cisco User Management for Secure Access**

Controleren in Entra

- Klik op Provisioning.



Verify in Entra ID

- Klik op Overzicht.

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

- Klik op Provisioning-logs.

Cisco User Management for Secure Access | Provisioning logs

Download | Refresh | Manage view | Got feedback?

Search Identity Add filter

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

Gerelateerde informatie

[Identiteitsproviders configureren](#)

[Gebruikers en groepen van Microsoft Entra ID voorzien](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.