

Assegnare a utenti e gruppi la protezione dell'accesso tramite Entra ID

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione di Cisco Secure Access](#)

[Configura provisioning in Microsoft Entra ID](#)

[Verifica](#)

[Verify in Cisco Secure Access](#)

[Verifica in ID Entra](#)

[Informazioni correlate](#)

Introduzione

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

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Access
- ID entrante

Componenti usati

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

- Accesso amministrativo a Cisco Secure Access Dashboard
- Pannello di controllo Accesso amministrativo a ID di entrata

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 Microsoft Entra ID (in precedenza Azure Active Directory).

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.



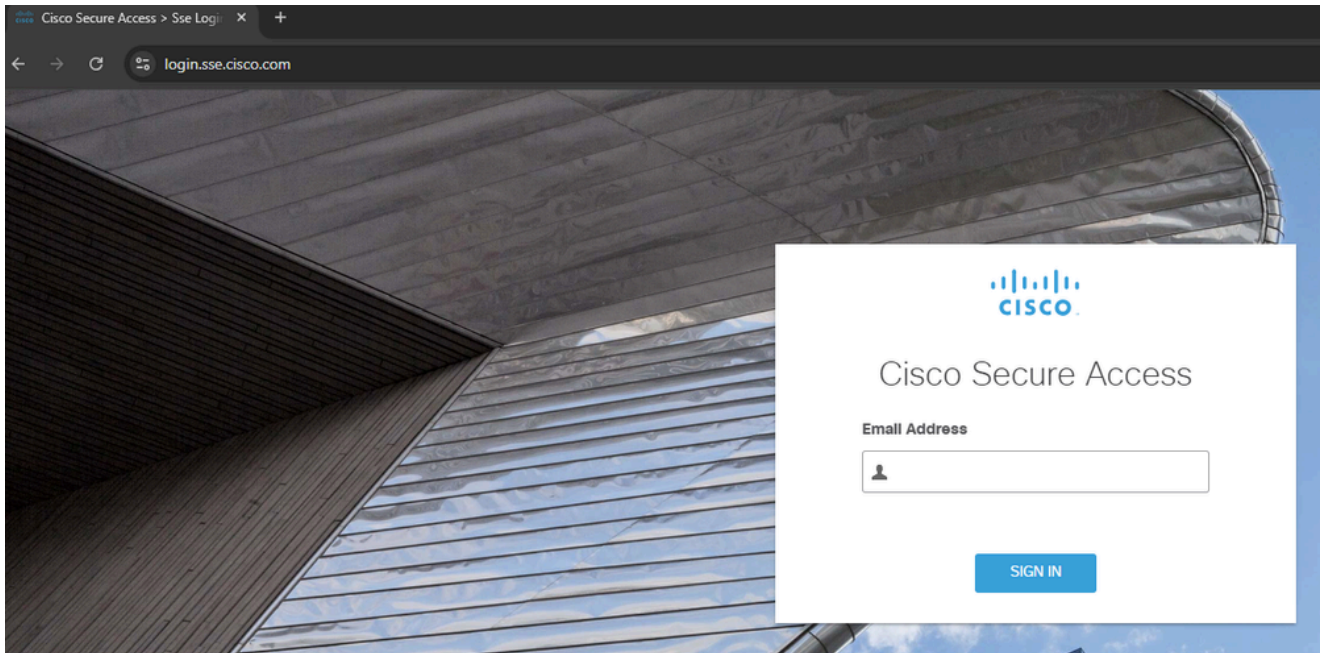
Nota: Questo documento si concentra in modo specifico sul provisioning di utenti e gruppi da Entra ID. La configurazione dell'ID Entra o di altri provider di identità (IdP) per la registrazione ZTA, l'autenticazione VPNaaS o impostazioni di roaming Umbrella specifiche esula dall'ambito di questa guida.

Configurazione

Configurazione di Cisco Secure Access

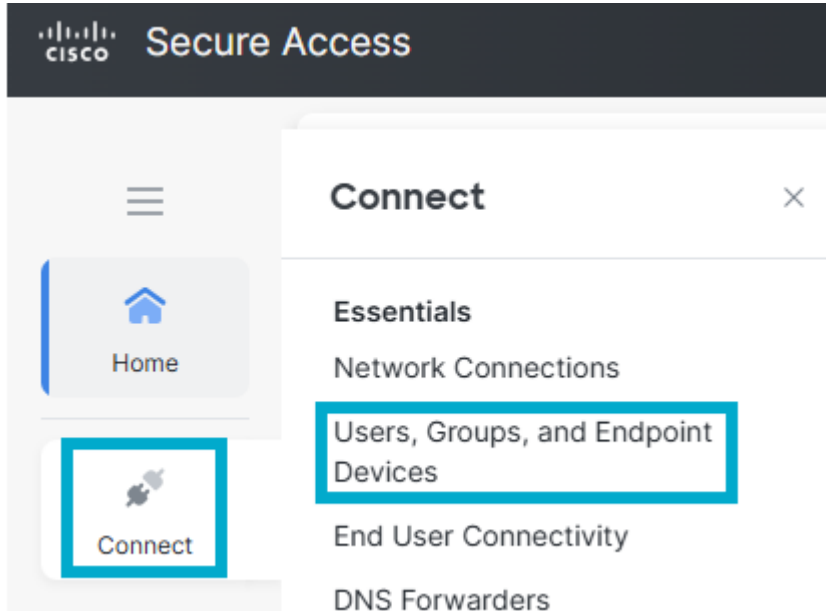
Per avviare il processo di provisioning, è necessario innanzitutto configurare l'integrazione delle directory nel dashboard Cisco Secure Access. Questo passaggio genera le credenziali e i parametri di configurazione necessari per stabilire una connessione protetta con Microsoft Entra ID.

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



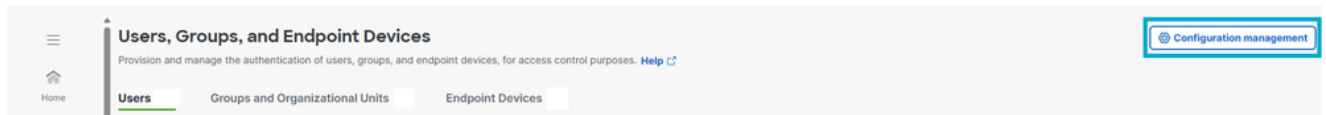
Accedi a CSA

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



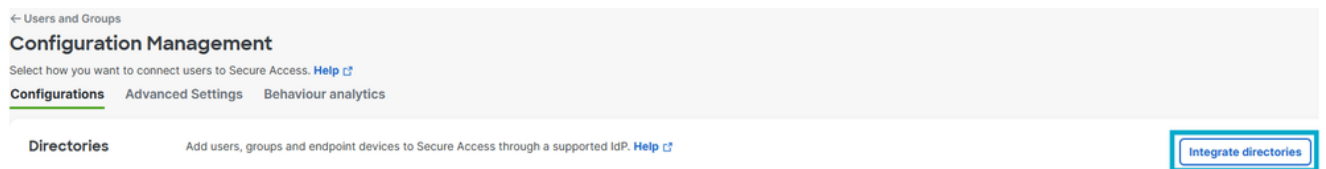
Utenti e gruppi

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



Gestione della configurazione

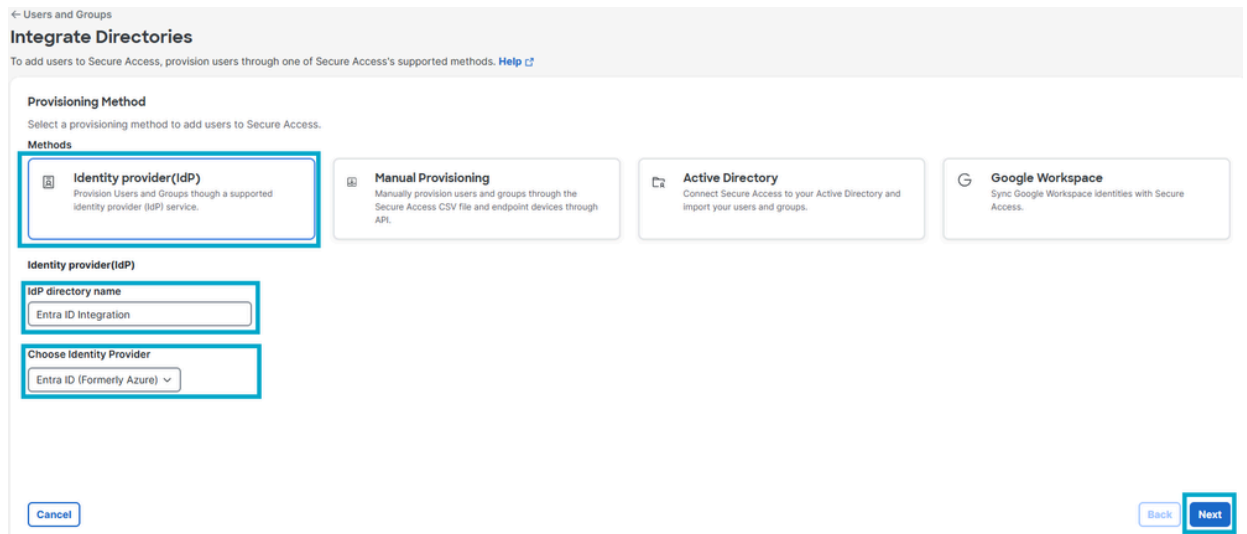
4. Fate clic su **Integra directory (Integrate Directory)**.



Integrate Directory

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

- **Nome directory IdP: Integrazione Entra ID.**
- **Scegli provider di identità: ID Entra (In Precedenza Azure).**
- 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**.

[← 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](#)

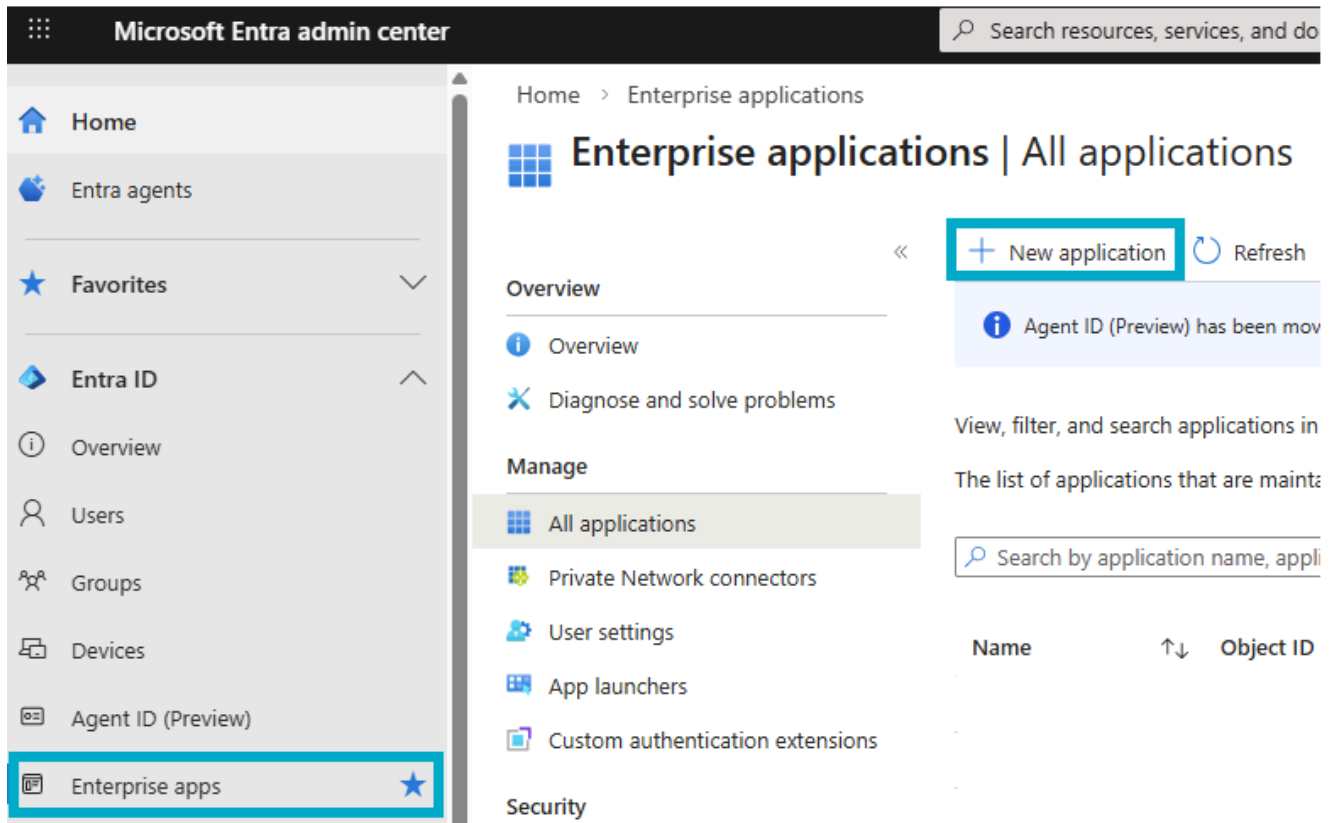
[Cancel](#) [Back](#) [Done](#)

Genera token

Configura provisioning in Microsoft Entra ID

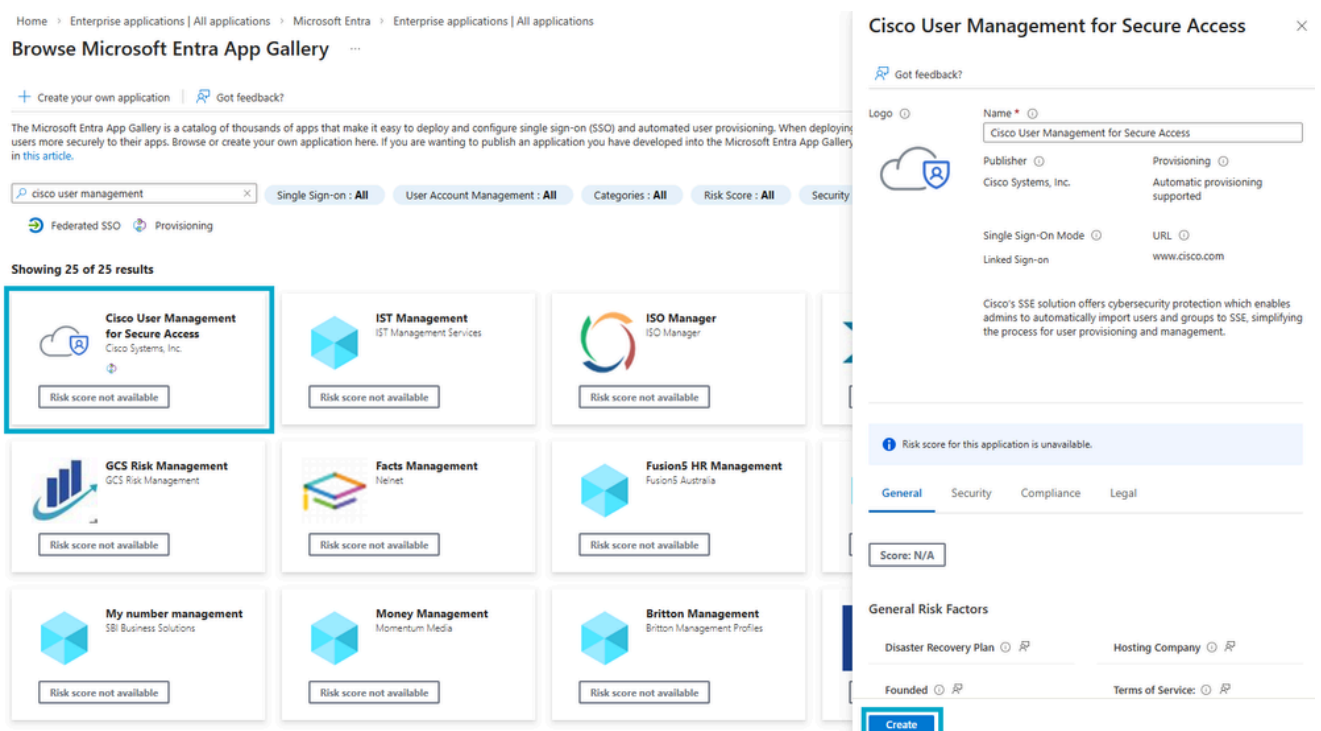
Dopo aver generato le credenziali nel dashboard Cisco Secure Access, è necessario configurare le impostazioni di provisioning nel tenant Microsoft Entra ID per abilitare la sincronizzazione di utenti e gruppi.

1. Accedi a [Entra ID](#).
2. Passare a Enterprise Apps > Nuova applicazione.



Nuova app Enterprise

3. Nella Raccolta app Entra cercare Cisco User Management for Secure Access e fare clic su Crea.



New App

4. Passare a Utenti e gruppi > Aggiungi utente/gruppo.

Cisco User Management for Secure Access | Users and groups
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Users and groups

« + Add user/group Edit assignment Remove assignment

The application will appear for assigned users within My Apps. Set 'visible to us

Assign users and groups to app-roles for your application here. To create new e

First 200 shown, search all users & groups

Display name

No application assignments found

Entra utenti e gruppi

5. Assegnare gli utenti/gruppi a Cisco Secure Access e fare clic su Seleziona (Select), quindi su Assegna (Assign).

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

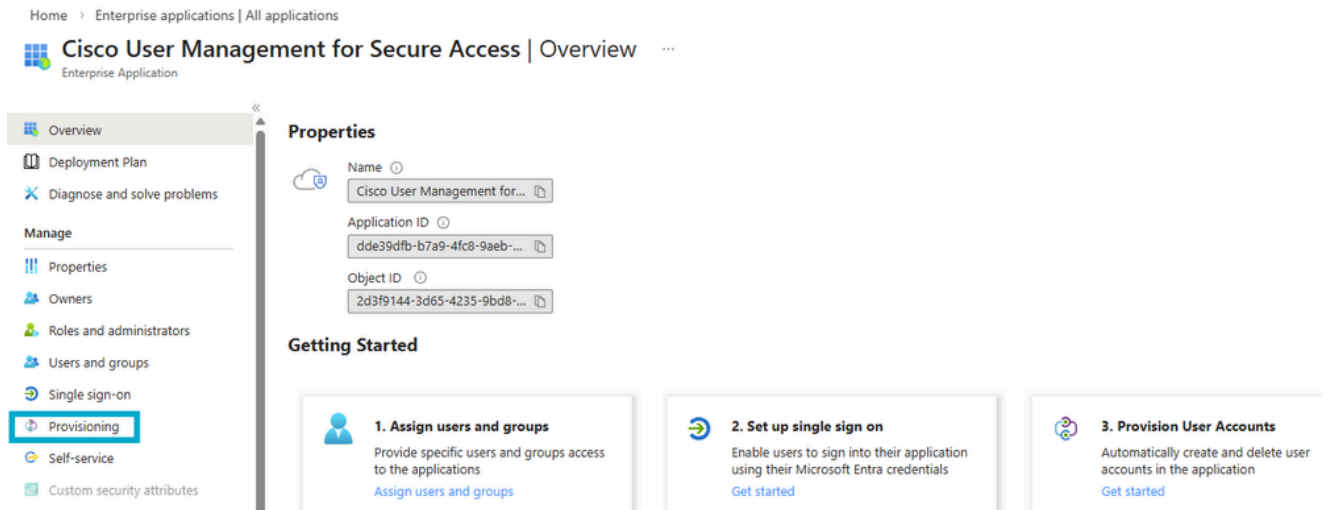
All Users Agent users Groups

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

Select

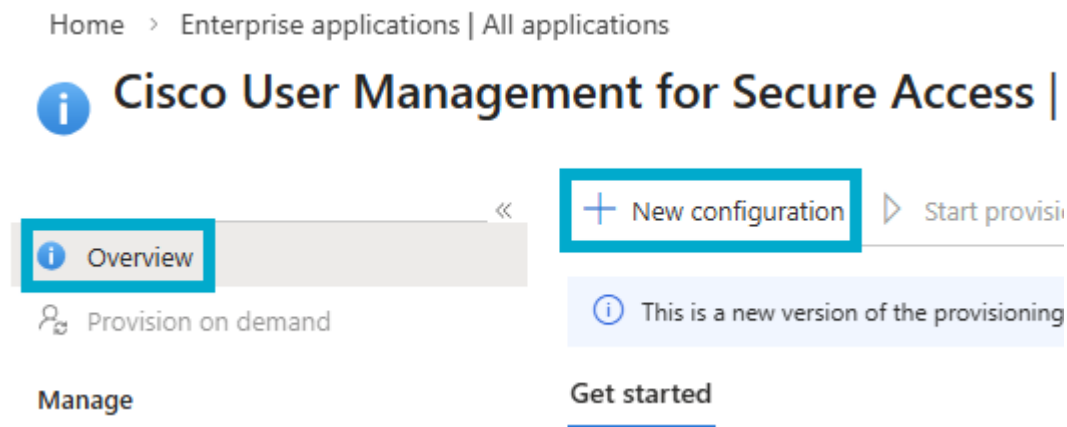
Assign Users and Groups

6. Passare a Provisioning.



Entra ID Provisioning

7. Fare clic su Overview (Panoramica), quindi su New Configuration (Nuova configurazione).



Nuova configurazione

8. Immettere l'URL del tenant e il token segreto salvati dal passaggio n. 6 della configurazione di accesso sicuro. Fare clic su Test configurazione, quindi su Crea.

Dopo aver creato la configurazione, viene visualizzata la pagina dei dettagli di configurazione per gestire le impostazioni avanzate.

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

Test di integrazione

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

9. Passare a Panoramica > Avvia provisioning.

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

Avvia provisioning

Start provisioning
Start in progress

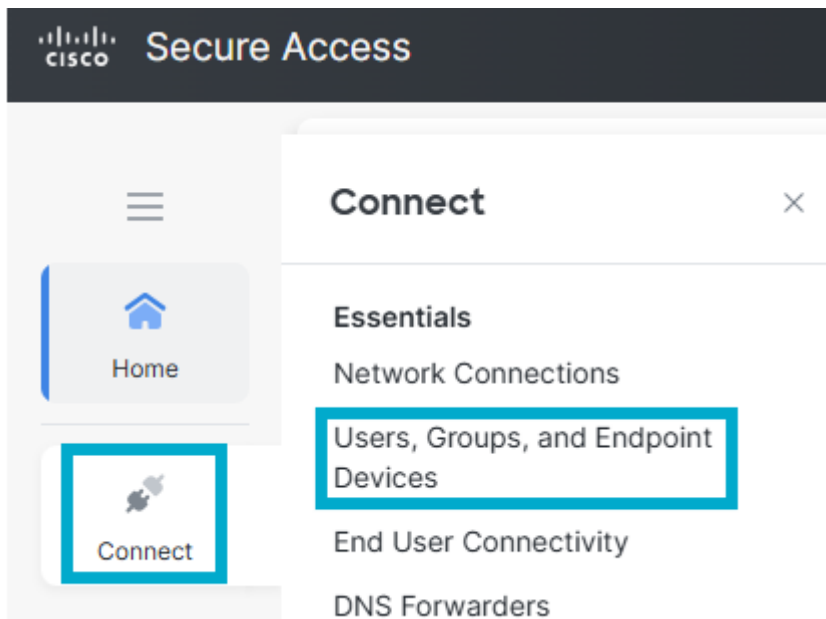


Nota: Se il ciclo di provisioning iniziale non riesce a effettuare il provisioning degli utenti/gruppi, fare clic su **Restart provisioning**. Questa azione forza Entra ID a tentare nuovamente la prima sincronizzazione degli utenti e dei gruppi.

Verifica

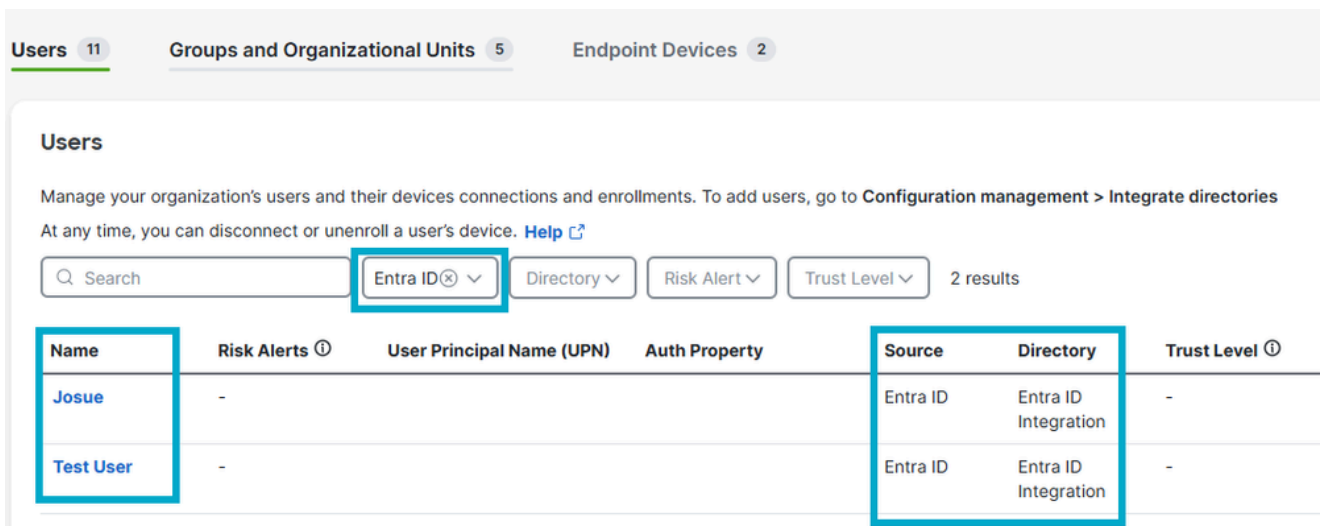
Verity in Cisco Secure Access

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



Users and Groups in CSA

- Fare clic su Utenti.



Verifica degli utenti in CSA

- Fare clic su Gruppi e unità organizzative.

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

Verifica in ID Entra

- Passare a Enterprise Apps e fare clic su 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

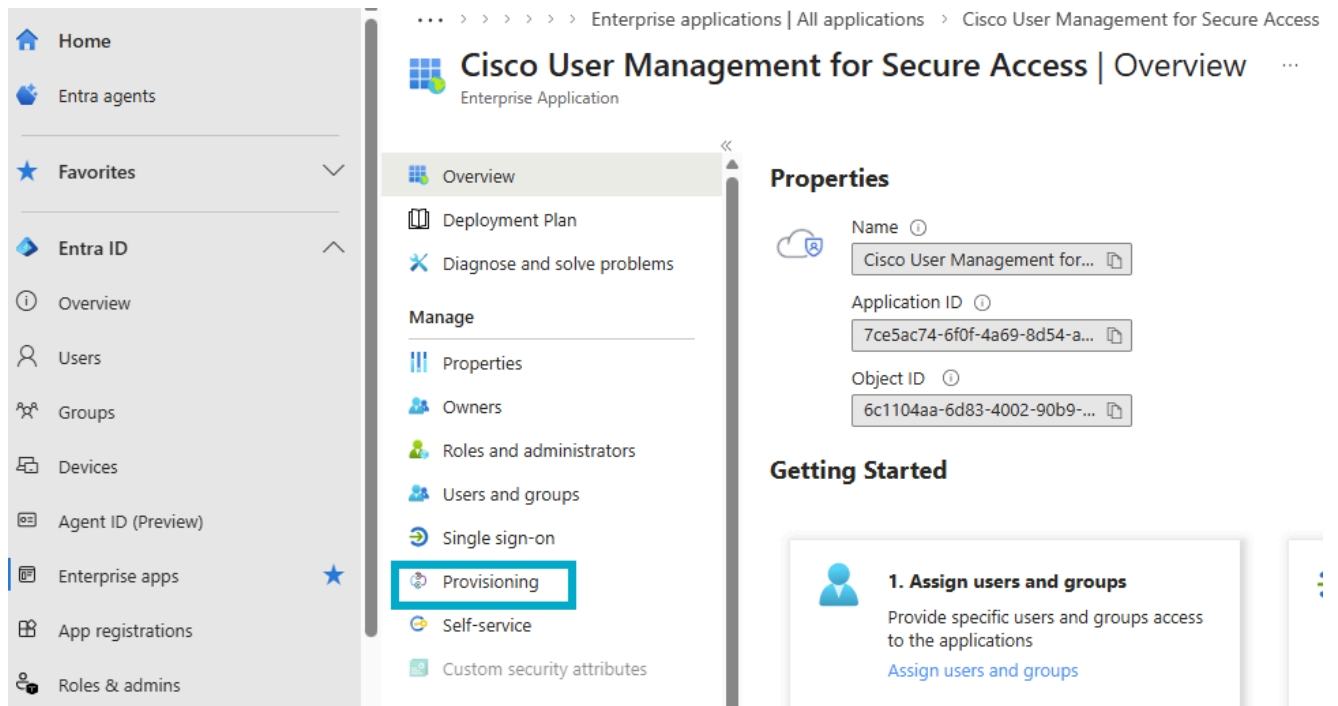
1 application found

Name

Cisco User Management for Secure Access

Verifica in Entra

- Fare clic su Provisioning.



Verify in Entra ID

- Fare clic su Panoramica.

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

- Fare clic su Log di provisioning.

App registrations > Enterprise applications | All applications > Cisco User Management for Secure Access | Overview > App registrations > Enterprise applicat

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	Display 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

Informazioni correlate

[Configura provider di identità](#)

[Assegna ruoli a utenti e gruppi da ID Entra Microsoft](#)

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).