Provision Users and Groups to Secure Access via Entra ID

Contents

Introduction

This document describes how to provision users and groups from Entra ID to Cisco Secure Access.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Access
- Entra ID

Components Used

This document is not restricted to specific software and hardware versions.

- Admin Access to Cisco Secure Access Dashboard

- Admin Access to Entra ID dashboard

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco Secure Access supports the provisioning of users and groups from Microsoft Entra ID (formerly Azure Active Directory).

This provisioning enables Secure Access to maintain a directory of users authorized to:

- Enroll in Zero Trust Access (ZTA).
- Connect to VPNaaS.
- Apply identity-based policies to Umbrella Roaming users.

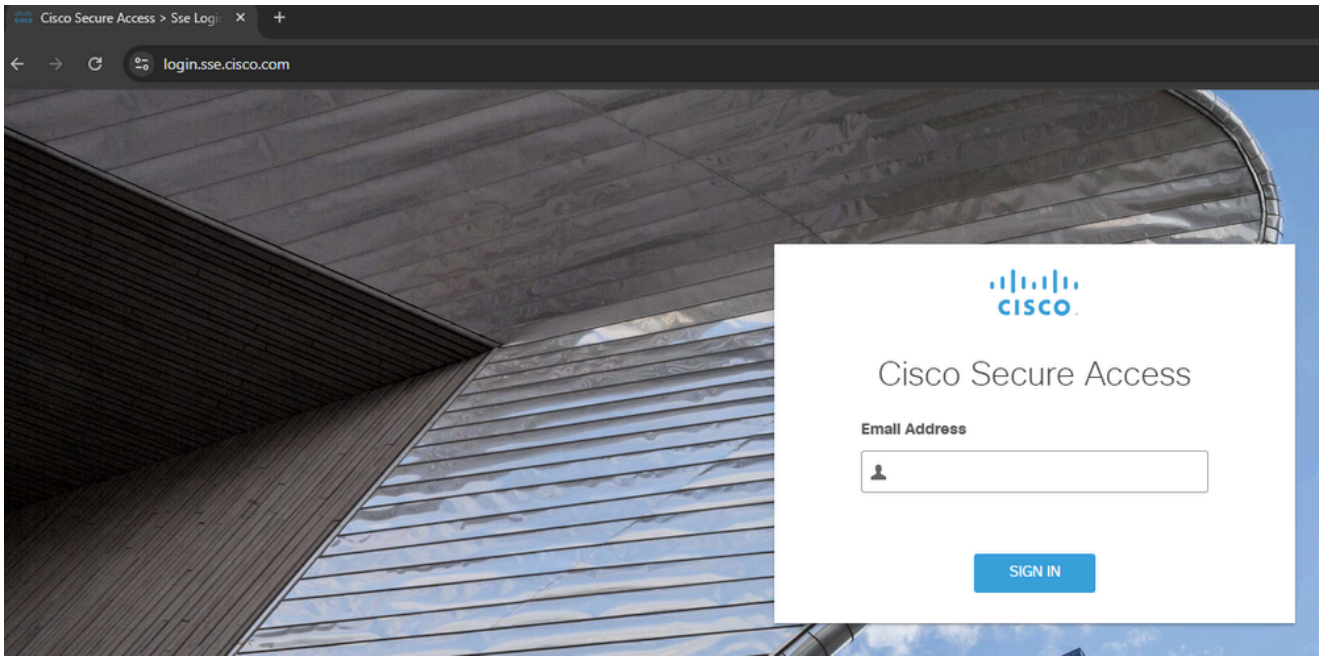
Note: This document focuses specifically on the provisioning of users and groups from Entra ID. The configuration of Entra ID or other Identity Providers (IdP) for ZTA enrollment, VPNaaS authentication, or specific Umbrella Roaming settings is outside the scope of this guide.

Configure

Configure Cisco Secure Access

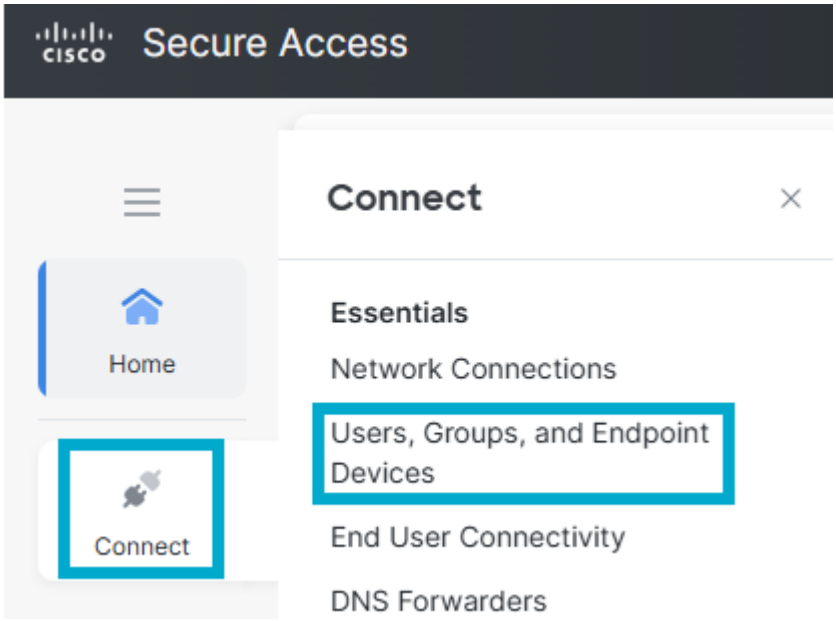
In order to begin the provisioning process, you must first configure the directory integration within the Cisco Secure Access dashboard. This step generates the necessary credentials and configuration parameters required to establish a secure connection with Microsoft Entra ID.

1. Sign in to the **Cisco Secure Access** **Dashboard**.



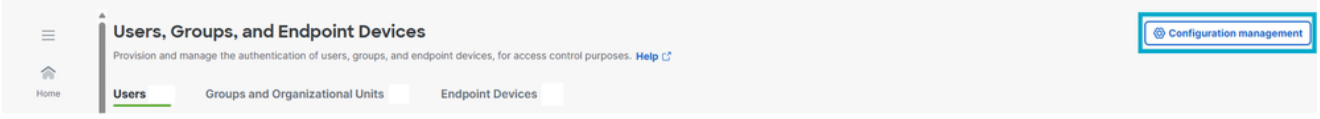
Sign in to CSA

2. Navigate to **Connect > Users, Groups and Endpoint Devices**.

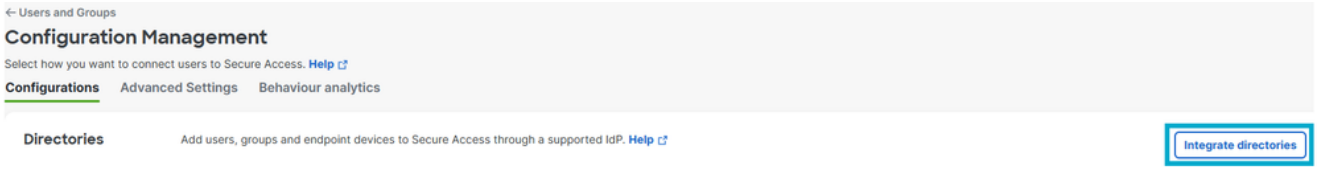


Users and Groups

3. Click **Configuration management**.

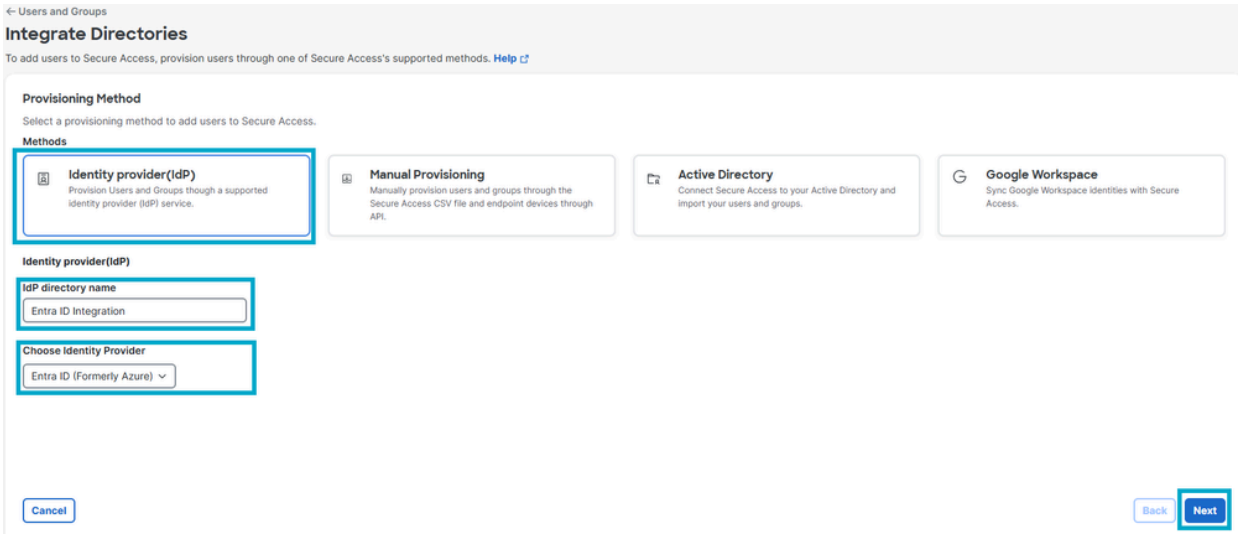


4. Click **Integrate Directory**.



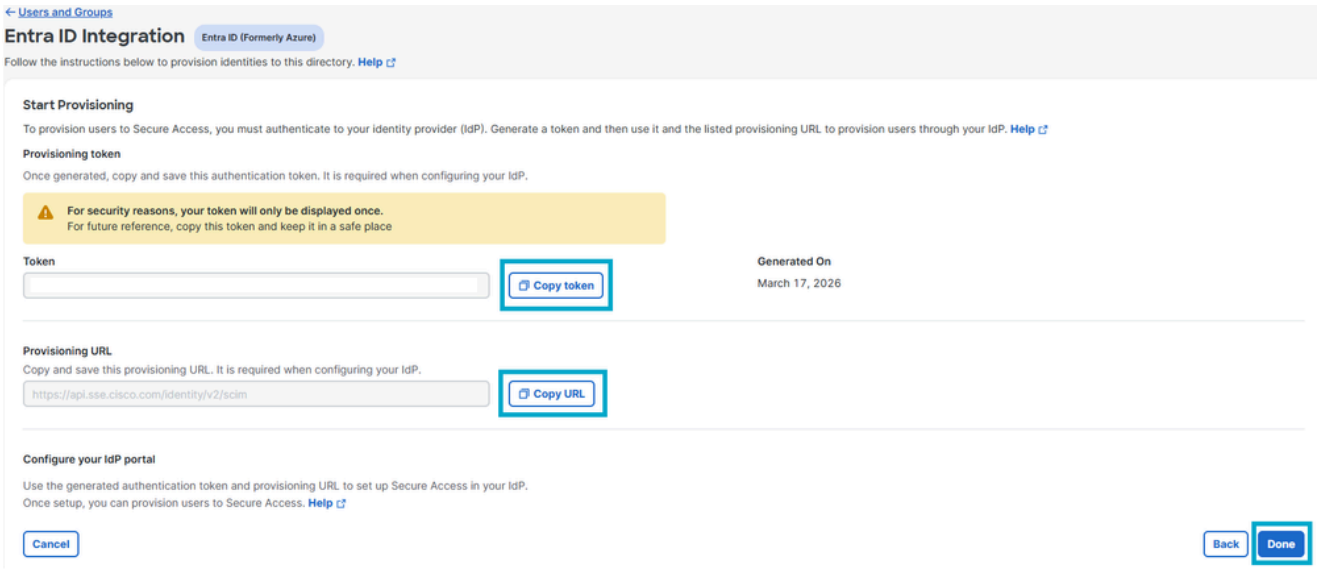
Integrate Directory

5. Under **Provision Method** click **Identity Provider**.
    - **IdP directory name: Entra ID Integration**.
    - **Choose Identity Provider: Entra ID (Formerly Azure)**.
    - Click **Next**.



Directory Configuration

6. Click **Generate token**. Save the **generated token** and the **provisioning URL**, then click **Done**.

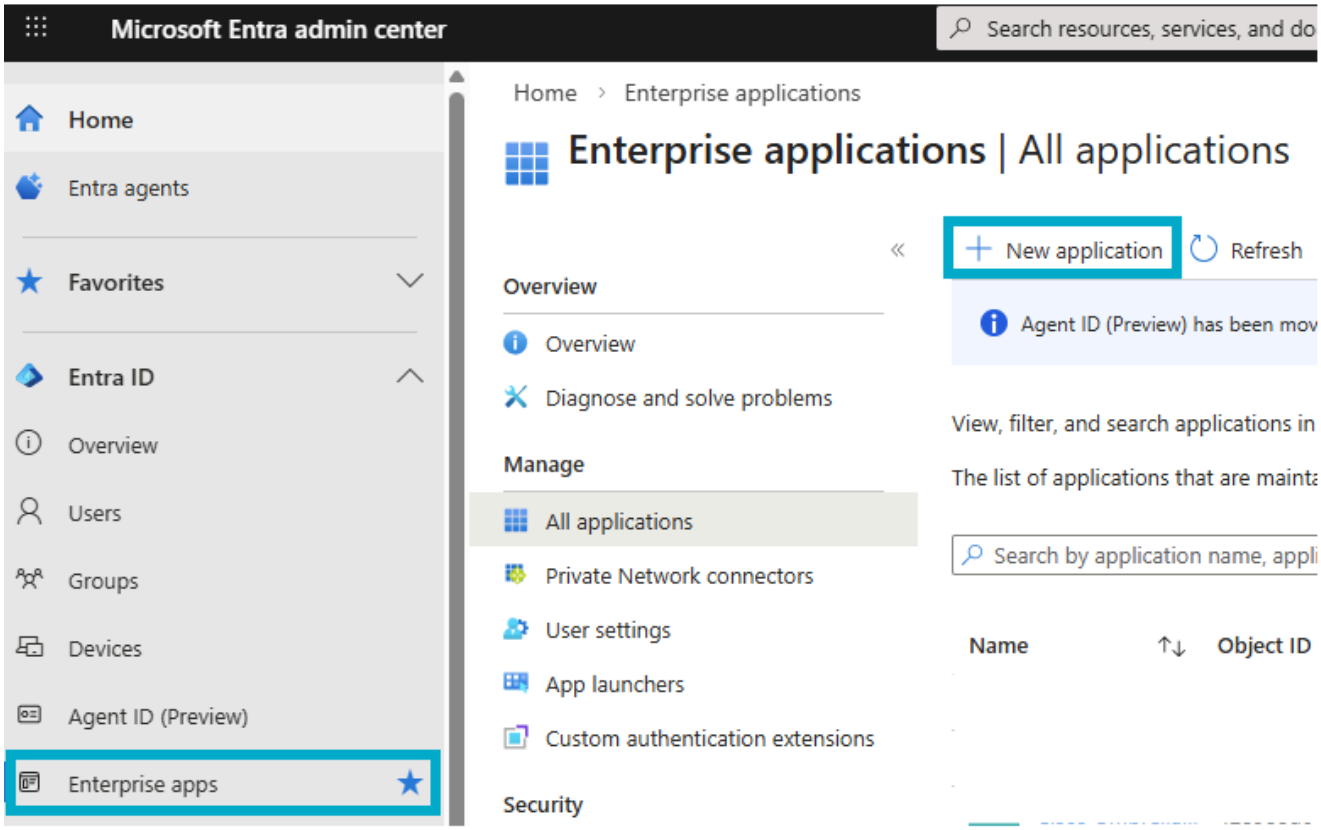


Generate Token

Configure Provisioning in Microsoft Entra ID

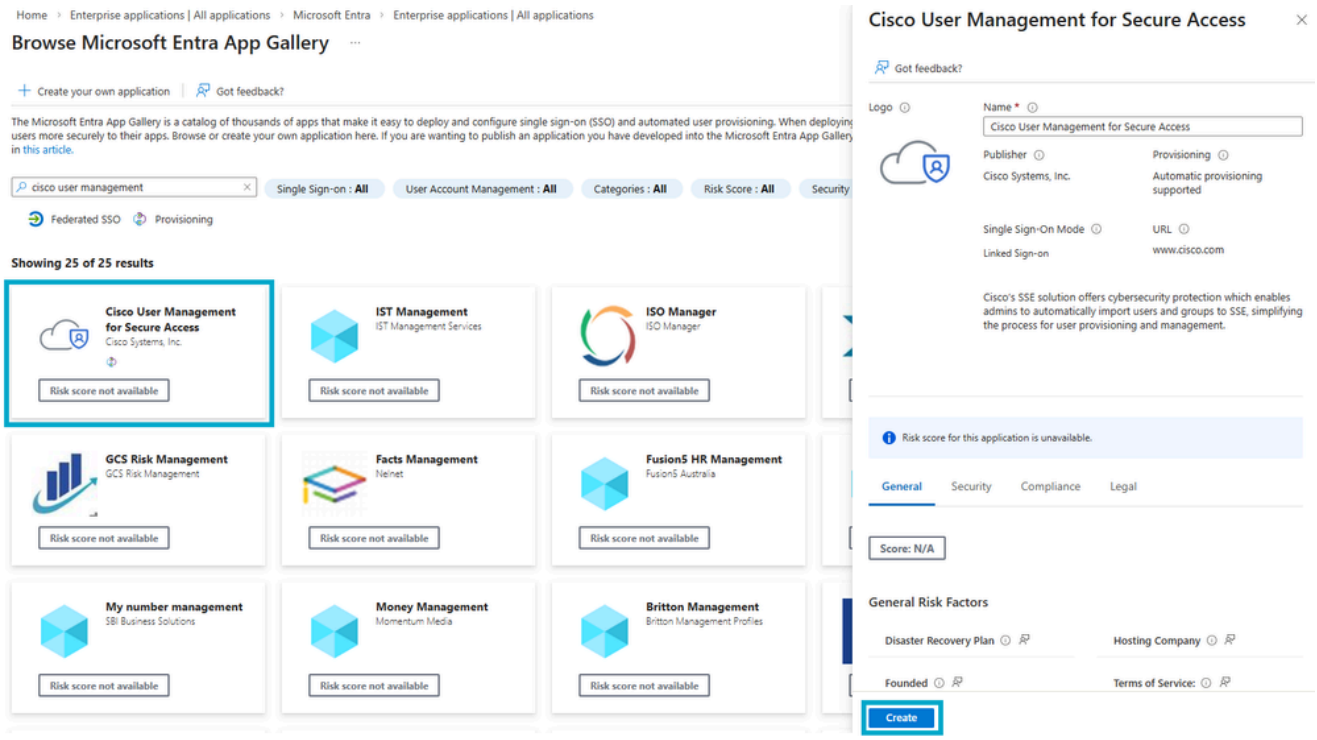
Once you have generated your credentials in the Cisco Secure Access dashboard, you must configure the provisioning settings within your Microsoft Entra ID tenant to enable the synchronization of users and groups.

1. Sign in to **Entra ID**.
2. Navigate to **Enterprise Apps > New Application**.



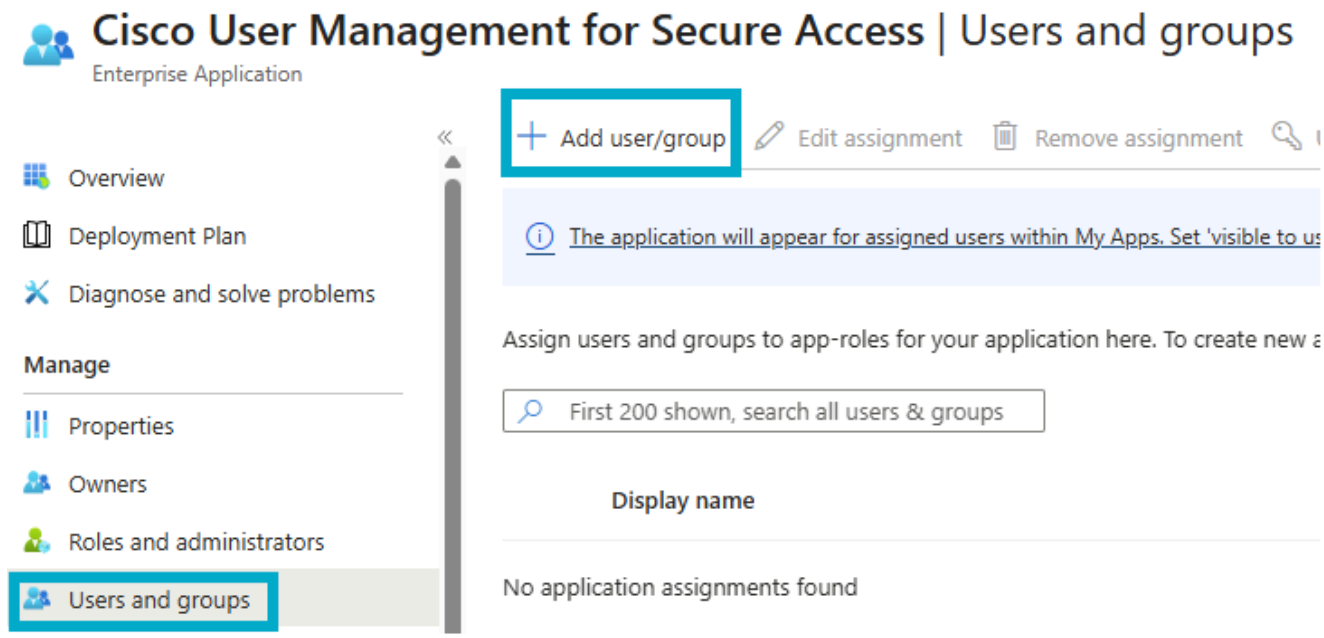
New Enterprise App

3. In the **Entra App Gallery** look for **Cisco User Management for Secure Access** and click **Create**.



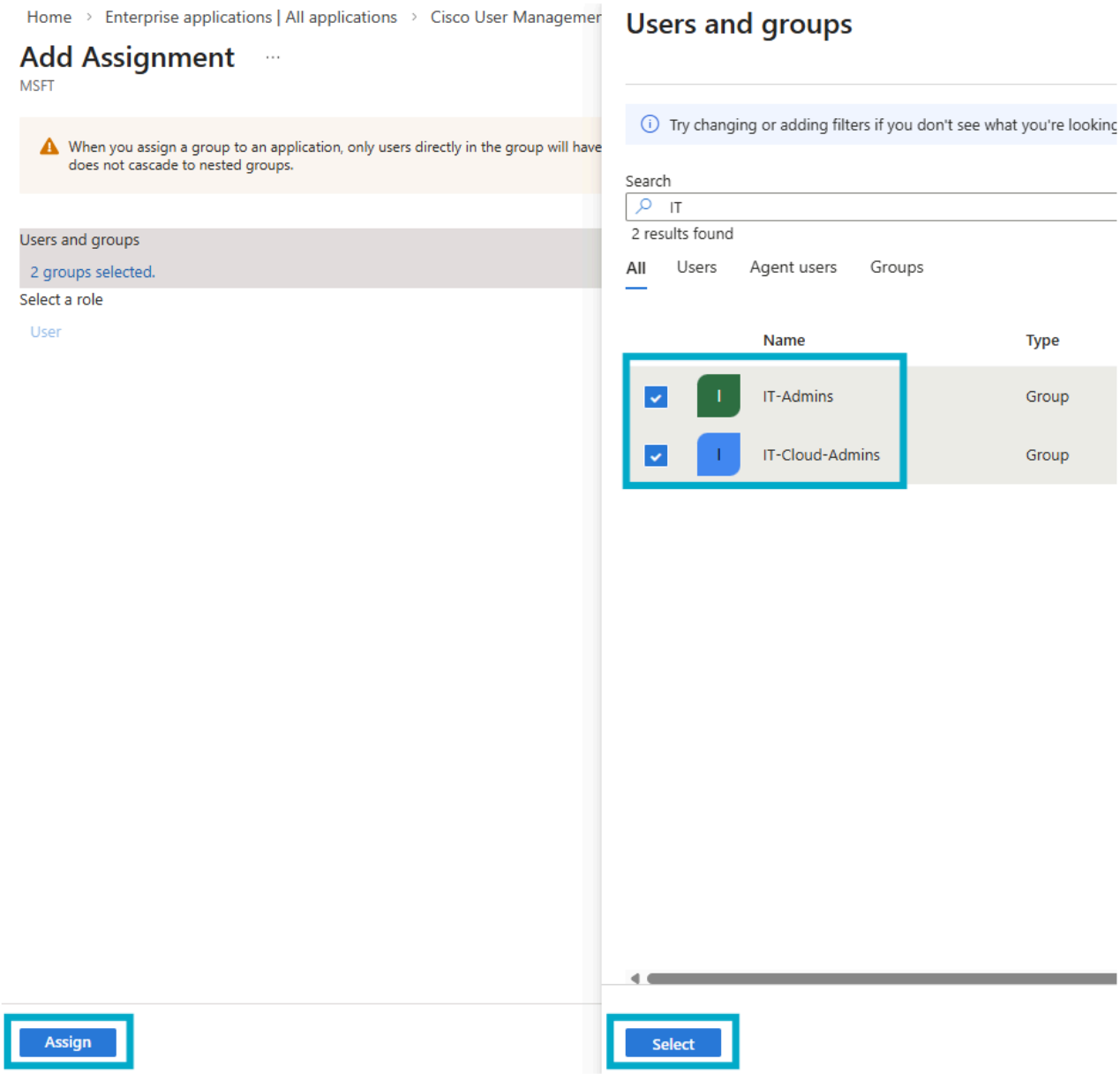
New App

4. Navigate to **Users and Groups > Add user/group**.



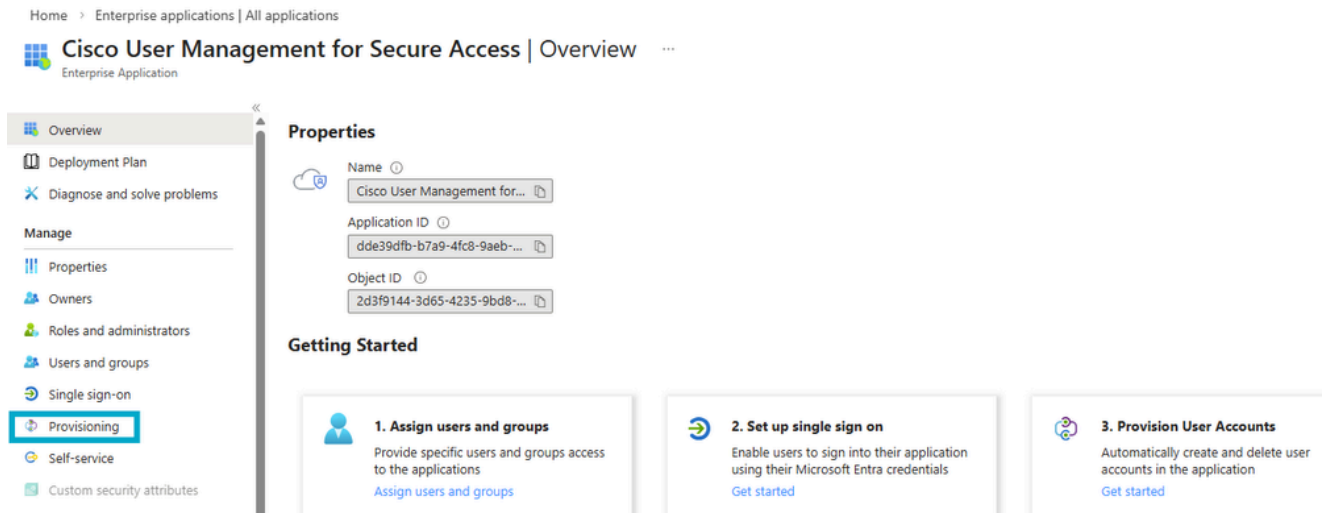
Entra Users and Groups

5. Assign the **users/groups** you want to provision to Cisco Secure Access and click **Select** and then **Assign**.



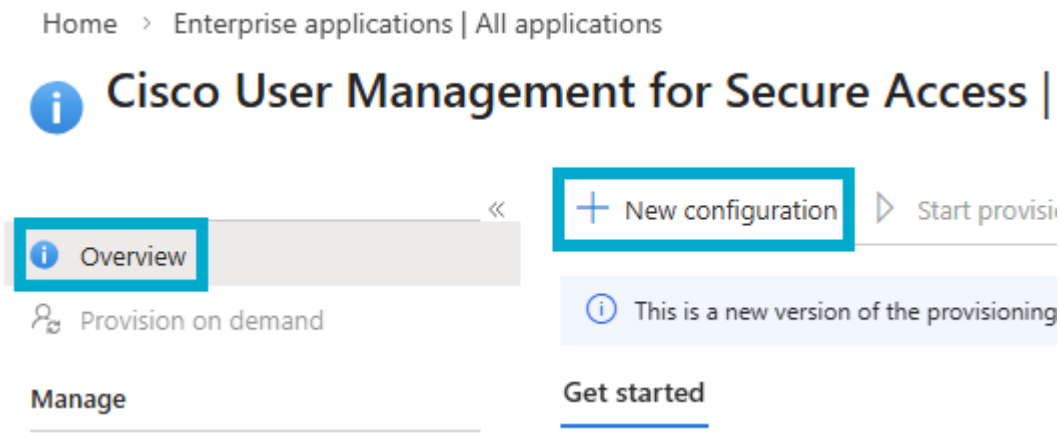
Assign Users and Groups

6. Navigate to **Provisioning**.



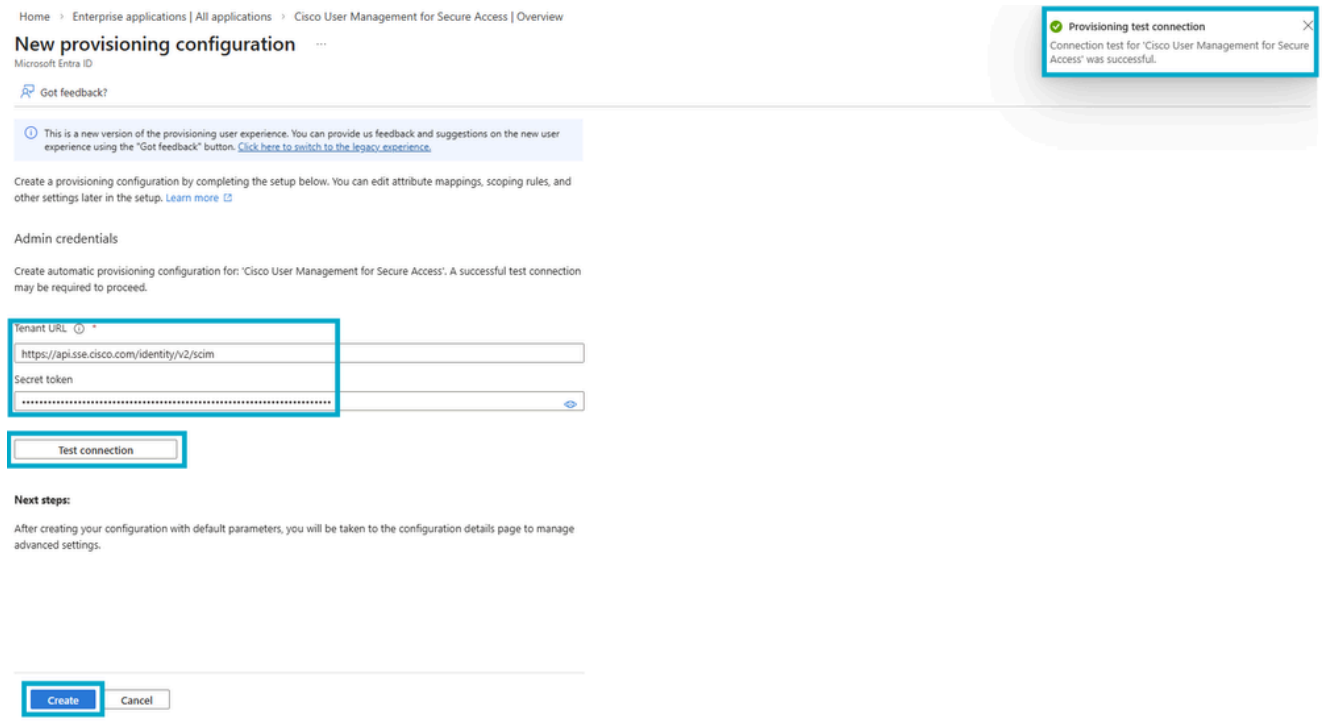
Entra ID Provisioning

7. Click **Overview** and then **New Configuration**.



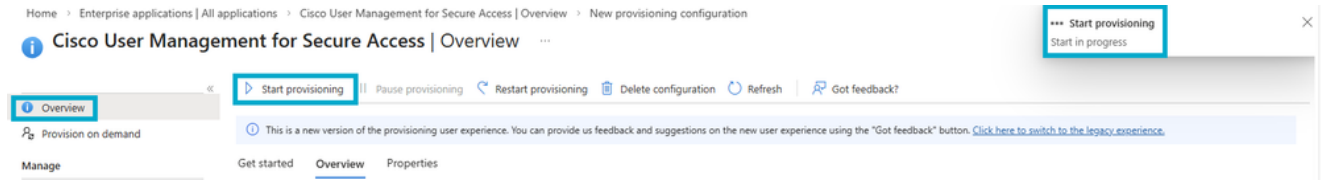
New Configuration

8. Enter the **Tenant URL** and **Secret Token** saved from step #6 of the Secure Access Configuration. Click **Test Configuration** and then **Create**.
   After creating your configuration, you are taken to the configuration details page to manage advanced settings.



Test Integration

9. Navigate to **Overview > Start Provisioning**.



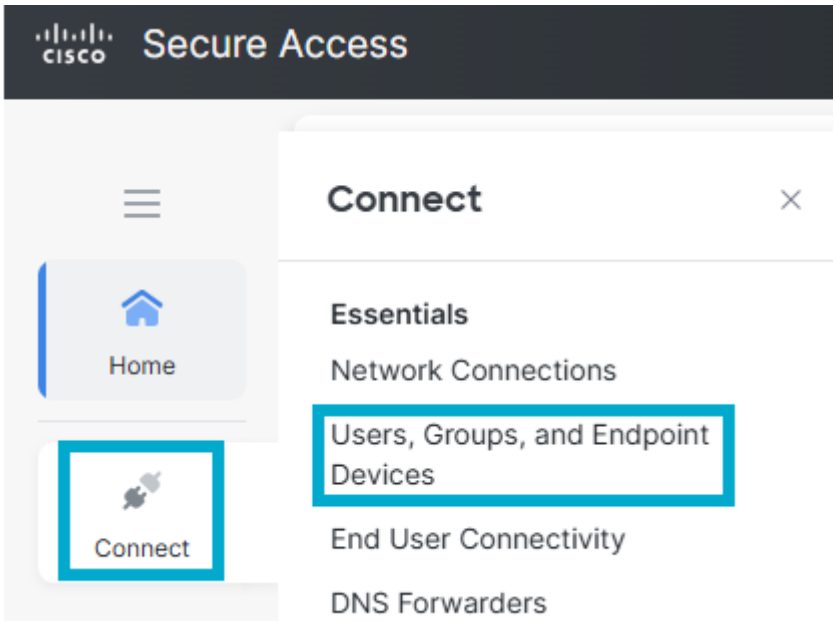
Start Provisioning

Note: If the initial provisioning cycle fails to provision the users/groups, click Restart provisioning. This action forces Entra ID to attempt the the first synchronization again of your users and groups.

Verify

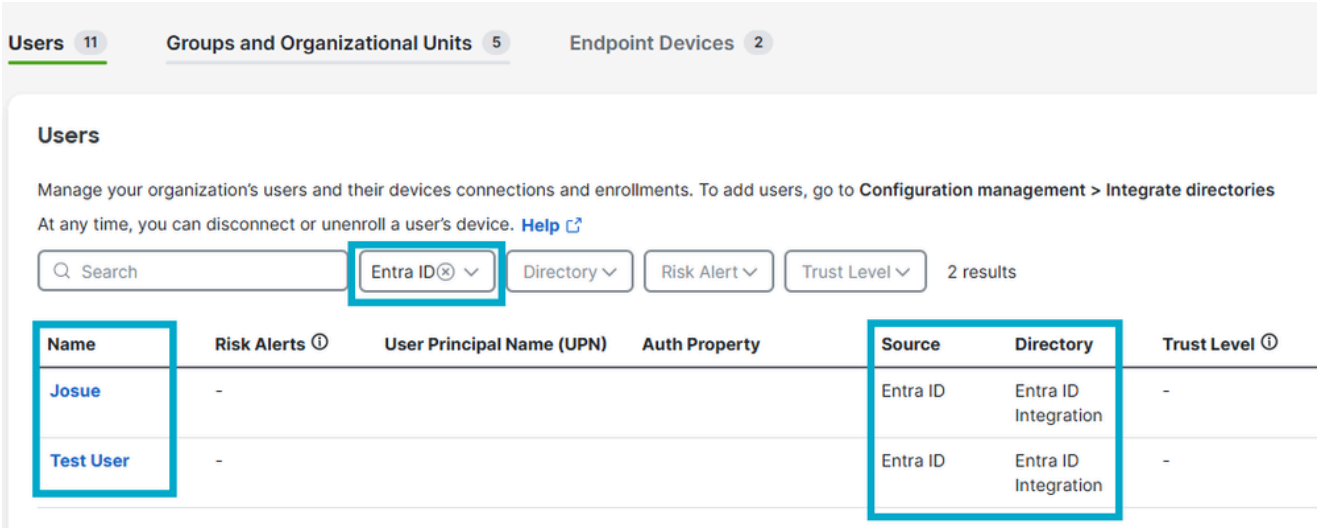
Verity in Cisco Secure Access

- Navigate to **Connect > Users, Groups and Endpoint Devices**.



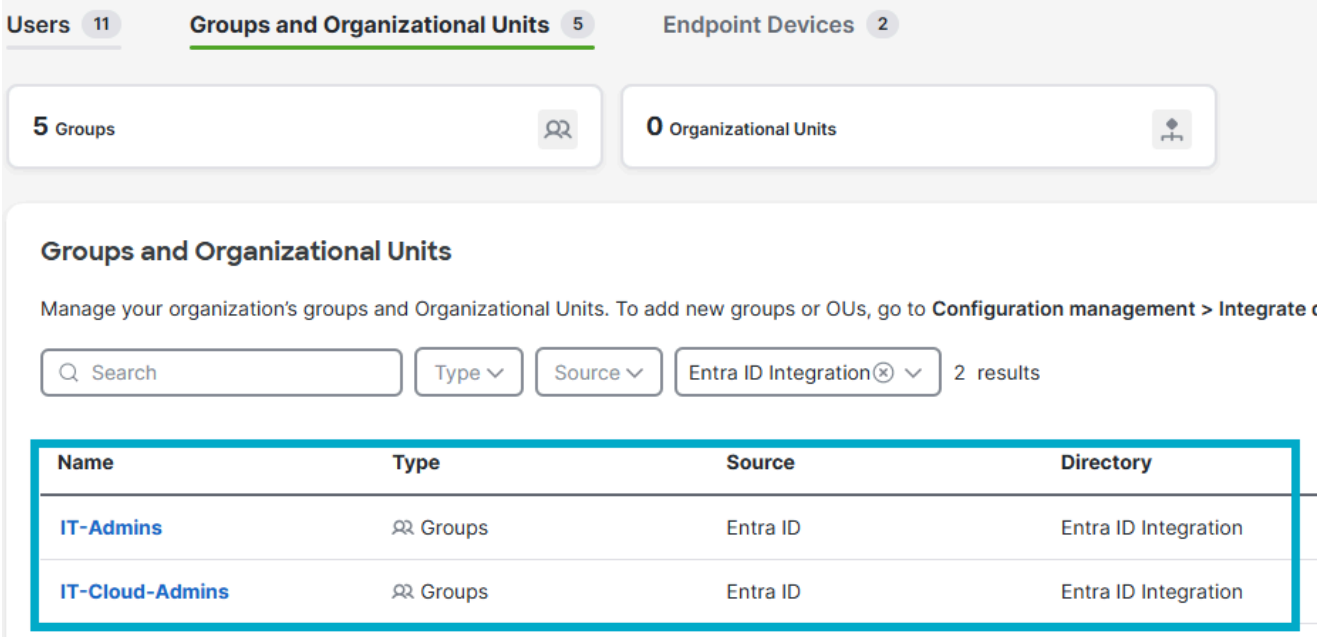
Users and Groups in CSA

- Click **Users**.



Verify Users in CSA

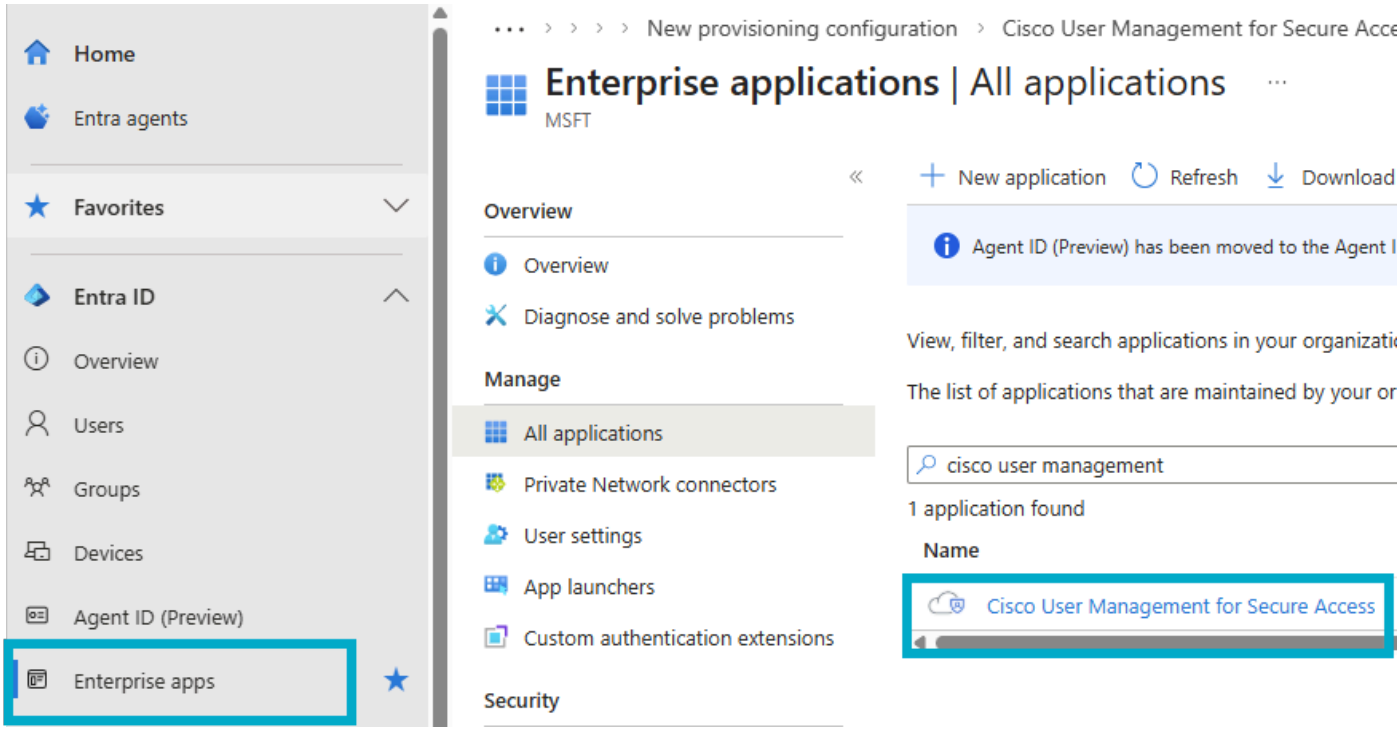
- Click **Groups and Organizational Units**.



Verify Groups in CSA

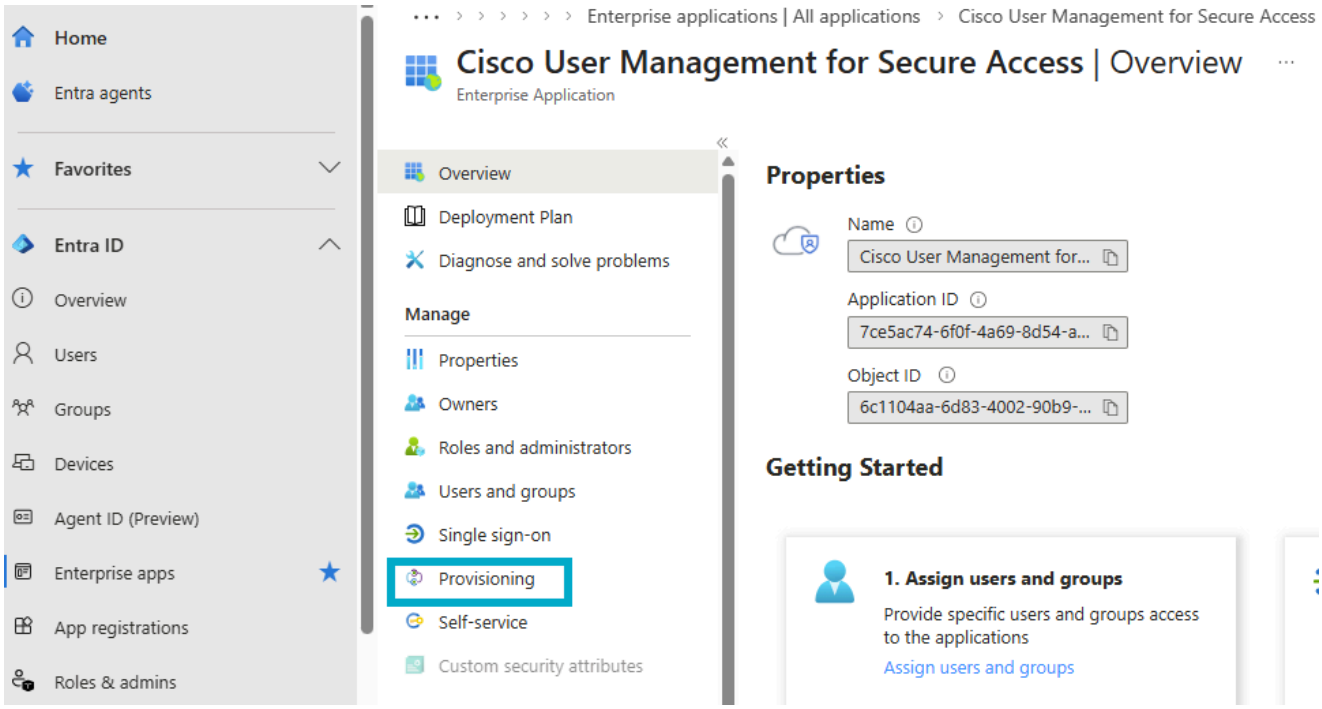
Verify in Entra ID

- Navigate to **Enterprise Apps** and click **Cisco User Management for Secure Access**.



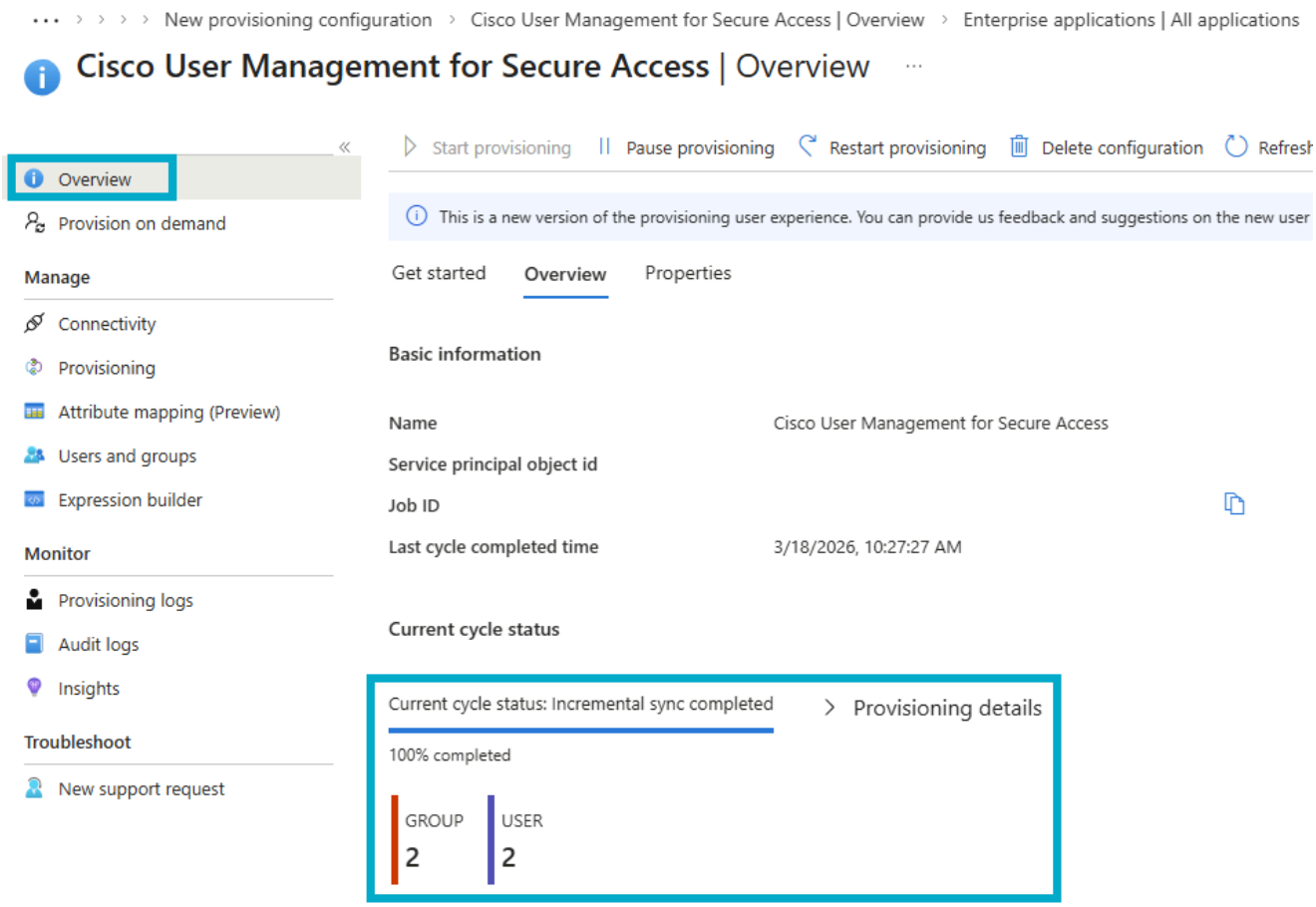
Verify in Entra

- Click **Provisioning**.



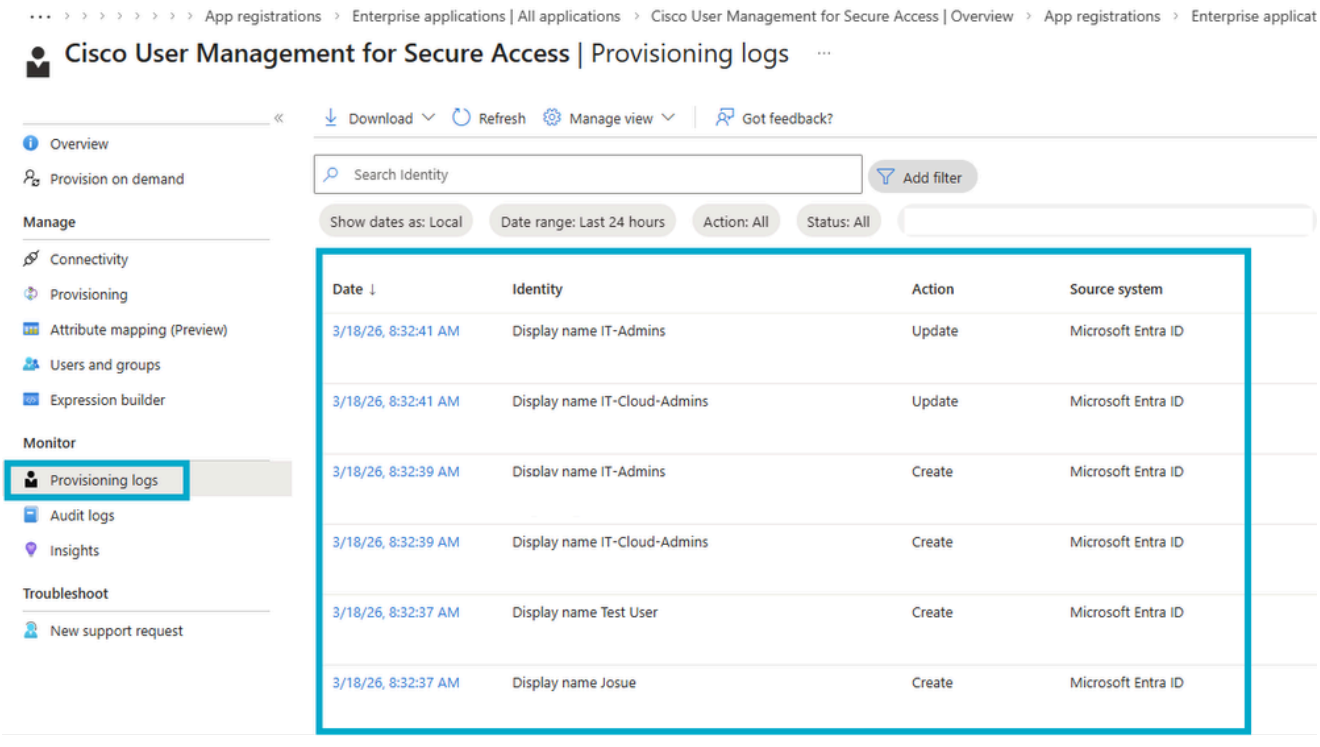
Verify in Entra ID

- Click **Overview**.



Verify Provisioning in Entra

- Click **Provisioning logs**.



Related Information

Configure Identity Providers

Provision Users and Groups from Microsoft Entra ID