



# Azure AD SCIM

## Integration Guide



# Table of Contents

<b>Introduction.....</b>	<b>2</b>
<b>Azure AD Configuration.....</b>	<b>3</b>
<b>Provisioning.....</b>	<b>5</b>
Group Provisioning.....	5
User Provisioning.....	6
Disable Group Provisioning.....	11
<b>Envi Configuration .....</b>	<b>13</b>

# Introduction

**Envi** supports **SCIM 2.0**, enabling user and group provisioning with various identity providers.

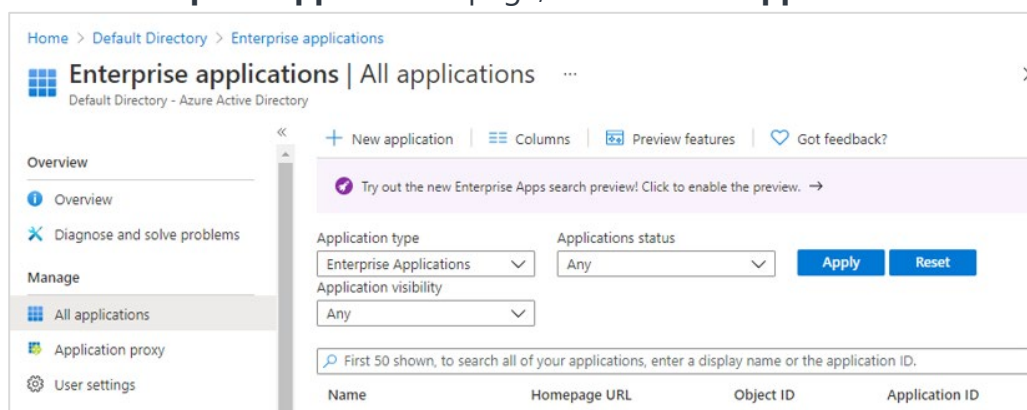
**SCIM** enables IT departments to automate provisioning and deprovisioning of accounts, which reduces manual redundant processes and increases security.

This step-by-step guide explains how to configure **Azure AD SCIM** connection with your **Envi** account.

# Azure AD Configuration

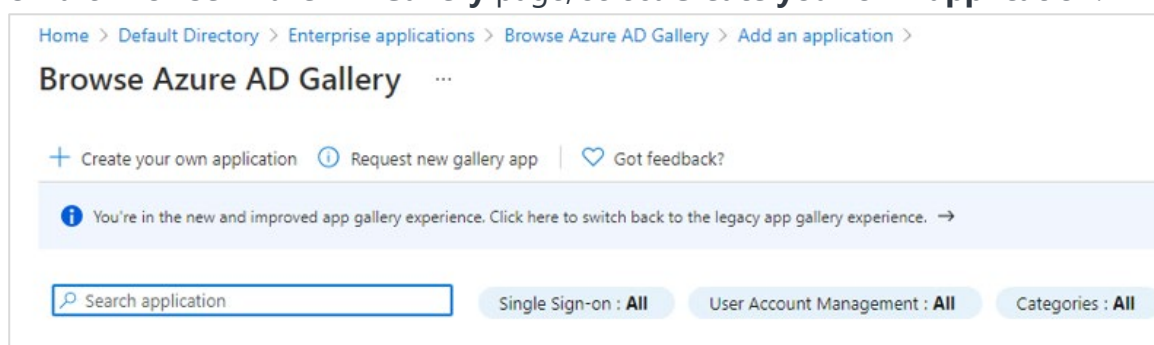
Perform the following steps to implement the **SCIM** provisioning with your **Envi** account.

1. Sign in to the **Microsoft Azure** portal.
2. Select **Azure Active Directory** from the menu and **Enterprise applications** from the **Manage** section.
3. On the **Enterprise Applications** page, select **+New application**.



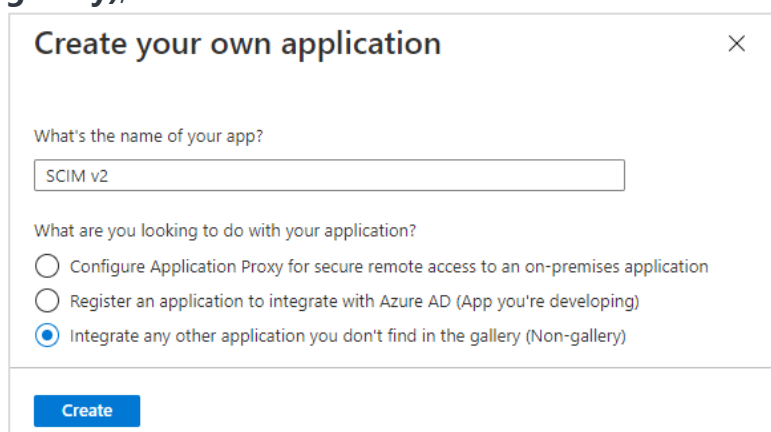
The screenshot shows the 'Enterprise applications | All applications' page in the Azure AD portal. The left sidebar has a 'Manage' section with 'All applications' selected. The main area has a '+ New application' button. Below it, there are filters for 'Application type' (set to 'Enterprise Applications'), 'Applications status' (set to 'Any'), and 'Application visibility' (set to 'Any'). There are 'Apply' and 'Reset' buttons. A search bar is present with the text 'First 50 shown, to search all of your applications, enter a display name or the application ID.' Below the search bar, there are columns for 'Name', 'Homepage URL', 'Object ID', and 'Application ID'.

4. On the **Browse Azure AD Gallery** page, select **Create your own application**.



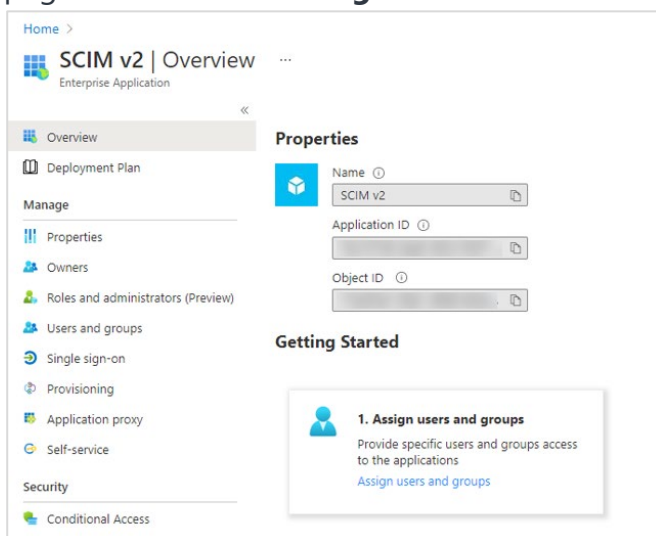
The screenshot shows the 'Browse Azure AD Gallery' page. The breadcrumb trail is 'Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Add an application >'. The main heading is 'Browse Azure AD Gallery'. Below it, there are buttons for '+ Create your own application', 'Request new gallery app', and 'Got feedback?'. A message states: 'You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience.' Below this, there is a search bar labeled 'Search application'. At the bottom, there are filters: 'Single Sign-on : All', 'User Account Management : All', and 'Categories : All'.

5. On the **Create your own application** page, enter a name for the new application, then select **Integrate any other application you don't find in the gallery (Non-gallery)**, and select **Create**.

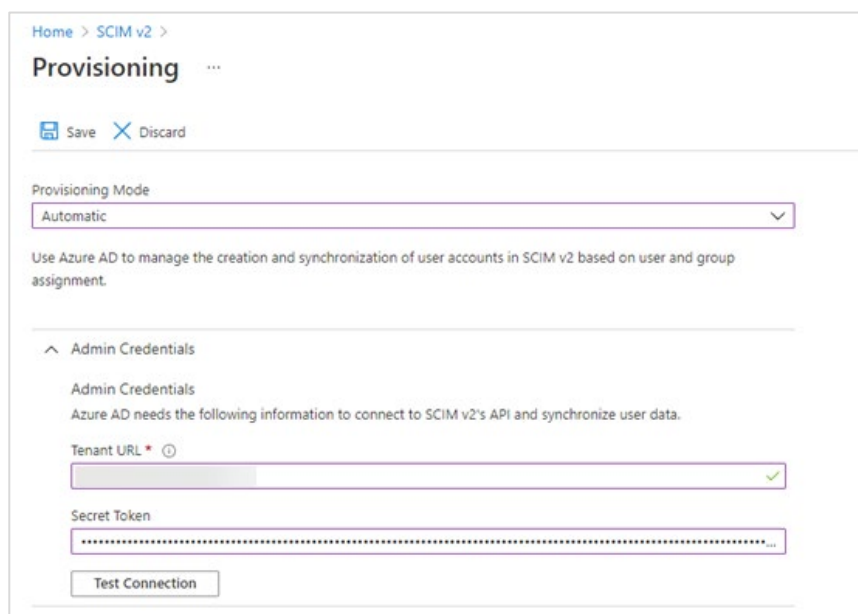


The screenshot shows the 'Create your own application' dialog. It has a title bar with a close button. The first question is 'What's the name of your app?' with a text input field containing 'SCIM v2'. The second question is 'What are you looking to do with your application?' with three radio button options: 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Azure AD (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The third option is selected. At the bottom, there is a blue 'Create' button.

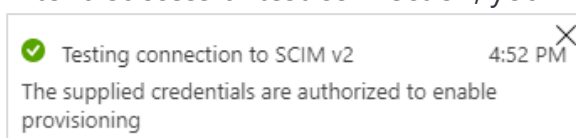
6. After you create the application, you will be redirected to the application details page. Select **Provisioning** in the menu to start provisioning.



7. On the **Provisioning** page, perform the following steps:
  - a. Set **Provisioning Mode** to **Automatic**.
  - b. In the **Tenant URL** box, enter the base URL of the **Envi SCIM** server + **/scim** (for example, https://scim.envi.net/scim).
  - c. In the **Secret Token** box, enter the **SCIM Token** obtained from the **Envi** application (the [Envi Configuration](#) section, step 5).
  - d. Select **Test Connection** which causes a test call from **Azure AD** to **Envi SCIM API** to make sure the entered information is correct.



8. After a successful test connection, you will see the notification:



9. Select **Save**.

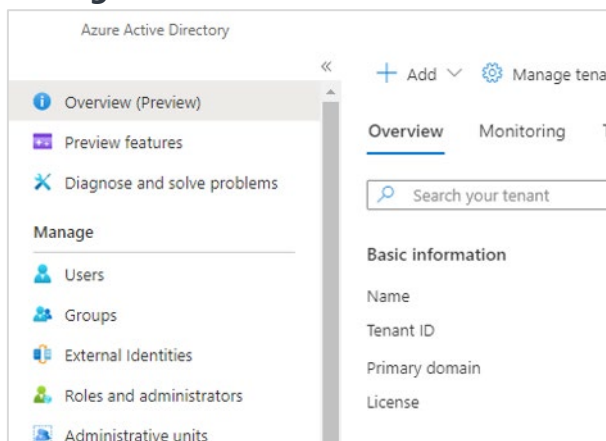
At this point, your configuration is ready for use.

# Provisioning

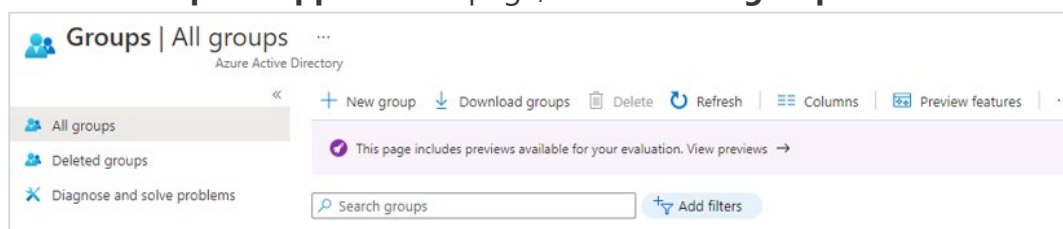
In this section, you will learn how to provision new users and groups.

## Group Provisioning

1. To add a new group, go to **Azure Active directory**, then select **Groups** in the **Manage** menu.

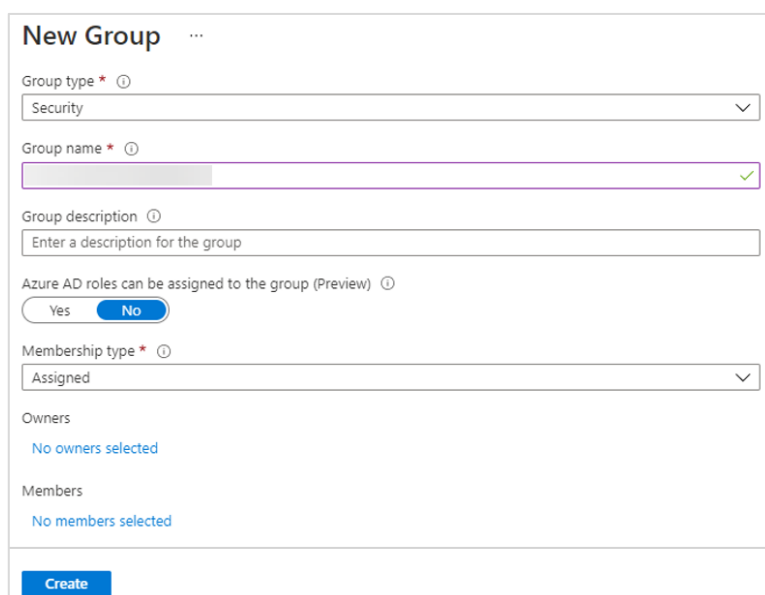


2. On the **Enterprise Applications** page, select **+New group**.

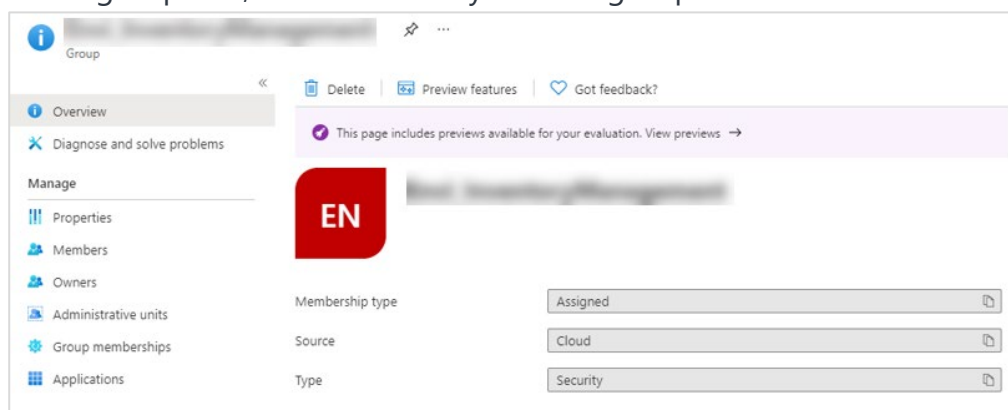


3. On the **New Group** page, perform the following steps:

- a. In **Group Type**, set **Security**.
- b. Enter **Group name** and **Group description**.
- c. In **Membership type**, set **Assigned**.
- d. Select **Create**.

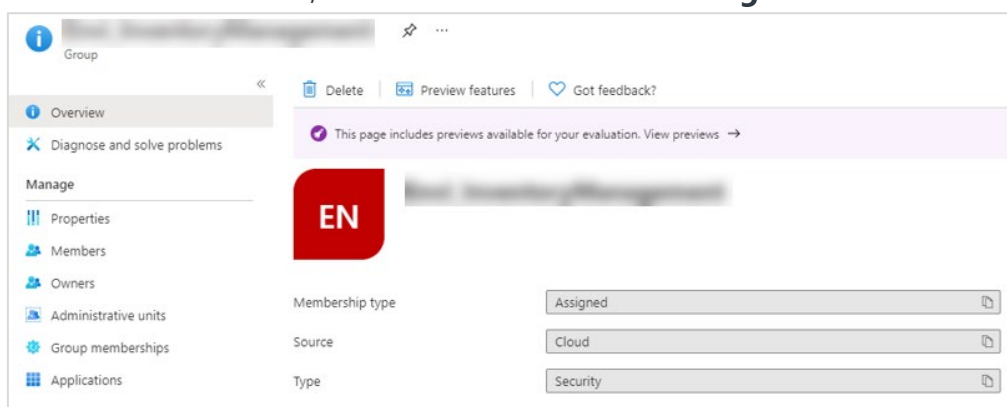


4. In the groups list, select the newly created group to view its details.

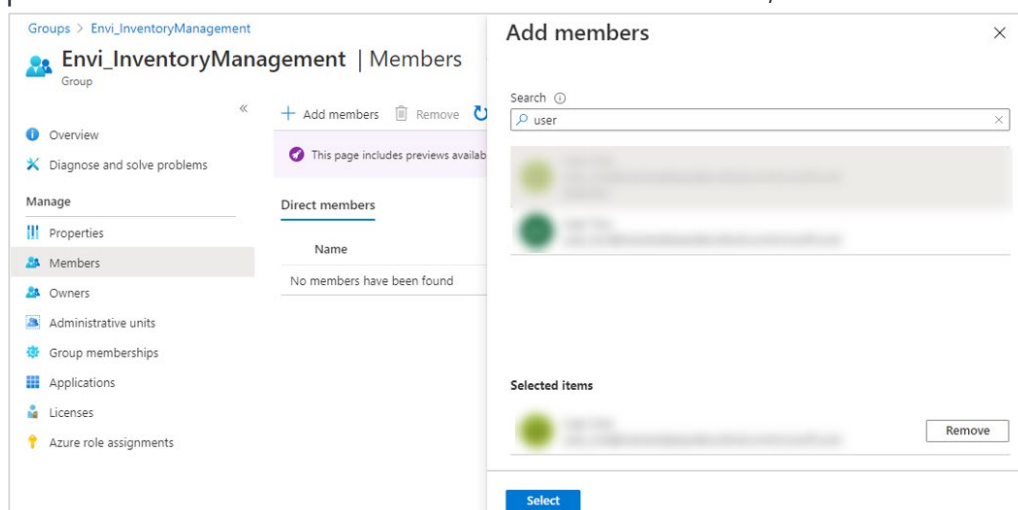


## User Provisioning

1. To add new members, select **Members** in the **Manage** menu.



2. Select **+Add members**, then use the search to select all users that will be provisioned to **Envi**. When all needed users are added, select the **Select** button.



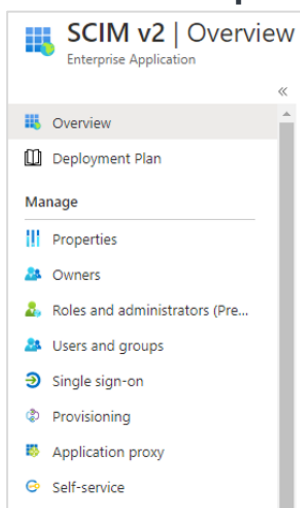
**Note:** Repeat the process of group creation and user assignment for all other users and groups that you want to add.

**Note:** If you are going to use group provisioning from **Azure AD** to **Envi**, you need to create a separate group for each **Envi** role. According to the configurations, your group name should have the same prefix as **User Role**

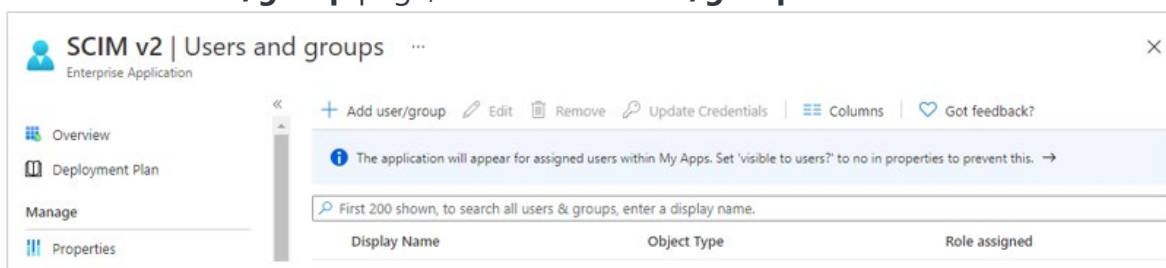
**Prefix** (Envi\_) on the **SCIM Configuration** page (the **Envi Configuration** section).

If you are not going to use automatic user provisioning for groups, it is enough to have only one group, and you are free to set any name for it.

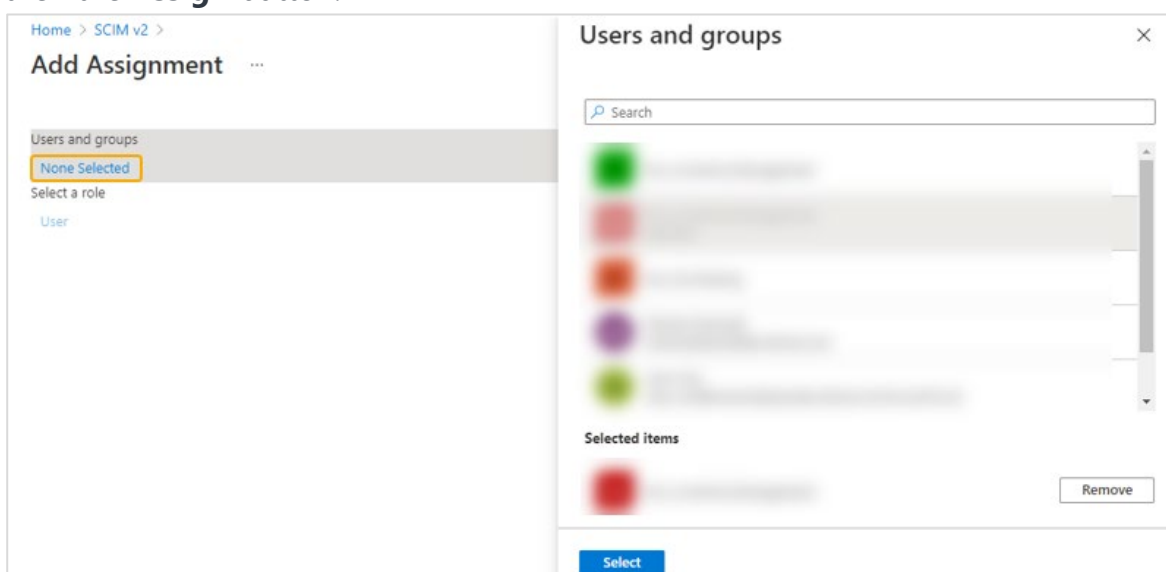
- Go to the details of your **Azure** application (select **Azure Active Directory** > **Enterprise applications** in the menu and an application in the list), then select **Users and Groups**.



- On the **Add user/group** page, select **+Add user/group**.

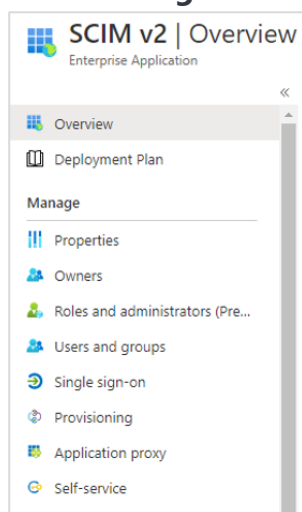


- On the **Add Assignment** page, select **None Selected** and use the search to locate the needed groups. When all needed groups are selected, select the **Select** and then the **Assign** button.

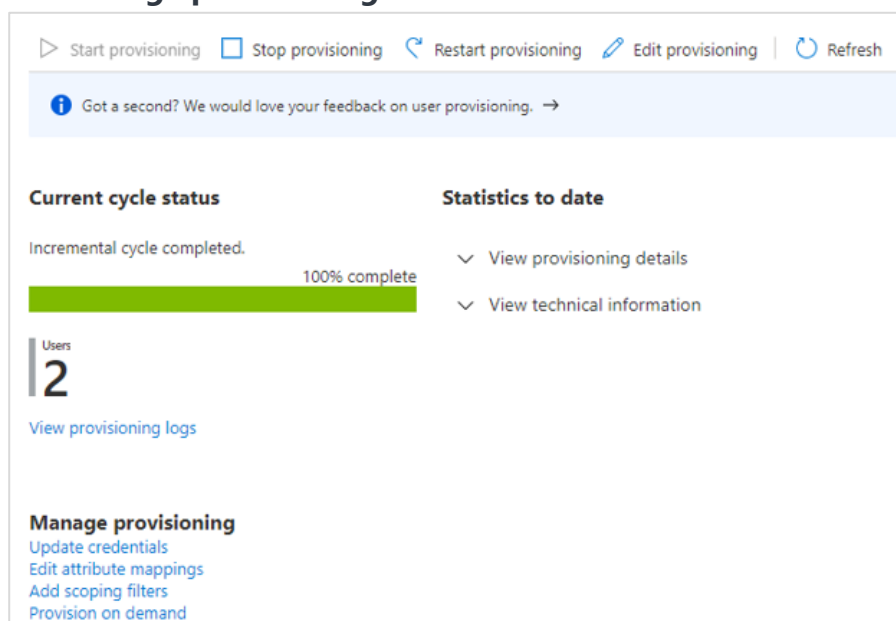




- Go to the details of your **Azure** application (select **Azure Active Directory** > **Enterprise applications** in the menu and an application in the list), then select **Provisioning**.



- On the **Provisioning** page, select **Edit provisioning** or **Edit attributes mapping** in the **Manage provisioning** section.



- On the **Provisioning** page, expand the **Mappings** section, and select **Provision Azure Active Directory Users**.

Home > SCIM v2 > Provisioning

Save Discard

Provisioning Mode  
Automatic

Use Azure AD to manage the creation and synchronization of user accounts in SCIM v2 based on user and group assignment.

Admin Credentials

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

☐ Restore default mappings

Settings

- On the **Attribute Mapping** page, under the **Attribute Mappings** section, delete all the attributes that are not used by **Envi**. **Envi** uses the following attributes for user provisioning (the **Customappsso Attribute** column on the screenshot):

- userName
- active, emails [type eq "work"].value
- name.givenName
- name.familyName
- name.formatted
- externalId

Enterprise applications > SCIM v2 > Provisioning > Attribute Mapping

Save Discard

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

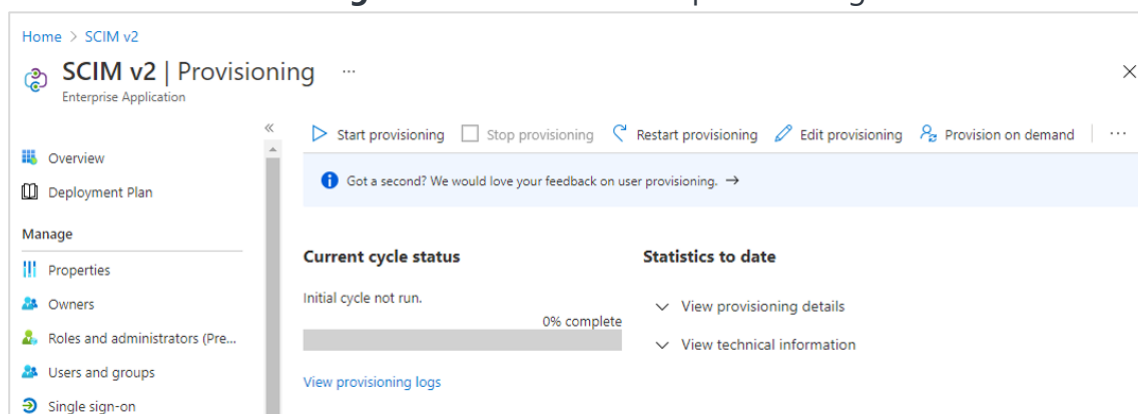
Azure Active Directory Attribute	customappsso Attribute	Matching precedence	Remove
userPrincipalName	userName	1	Delete
Switch([isSoftDeleted], "False", "True", "False")	active		Delete
mail	emails[type eq "work"].value		Delete
givenName	name.givenName		Delete
surname	name.familyName		Delete
Join(" ", [givenName], [surname])	name.formatted		Delete
mailNickname	externalId		Delete

Add New Mapping

☐ Show advanced options

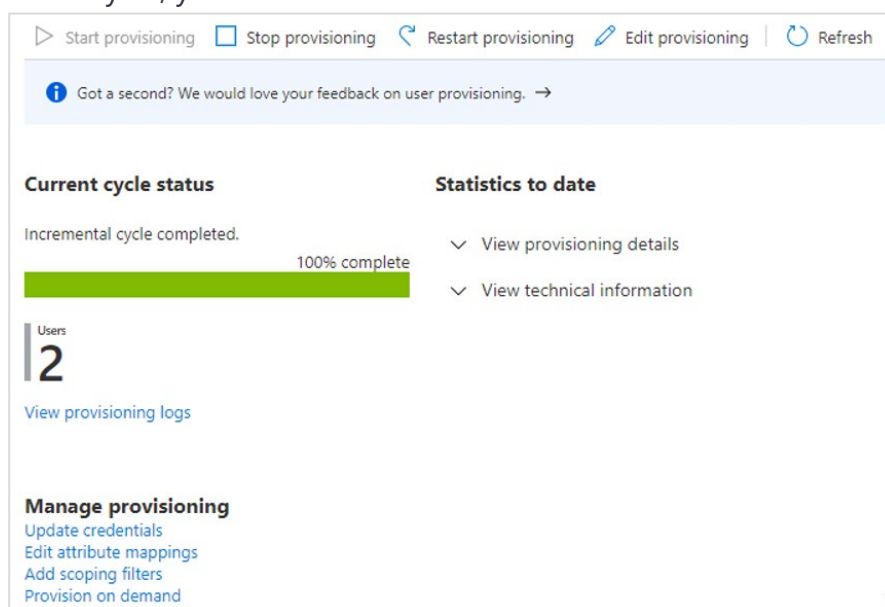
**Note:** Please make sure your configuration does not contain any redundant mappings; otherwise, delete them. If you need to delete an appropriate attribute, select **Delete** and save your changes.

10. Select **Start Provisioning** to start the automatic provisioning.



**Note:** **Azure AD** has both user and group provisioning enabled by default. If you do not need group provisioning, please disable it prior to starting provisioning (the [Disable Groups Provisioning](#) section).

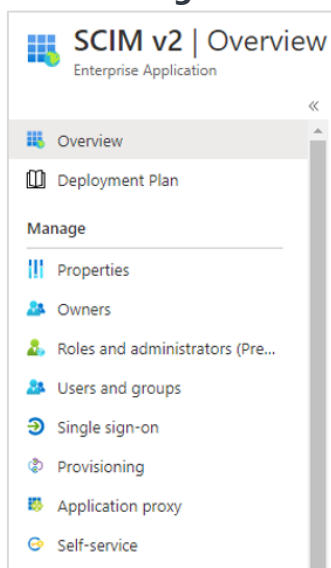
11. Select **Refresh** to refresh information related to provisioning. After completing the initial cycle, you will see the related information.



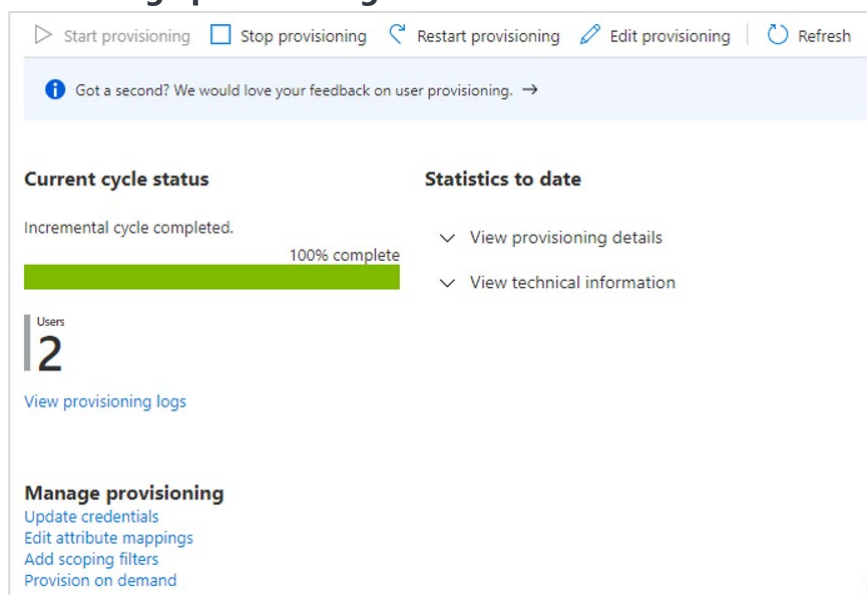
Now, the needed members and groups are added.

## Disable Group Provisioning

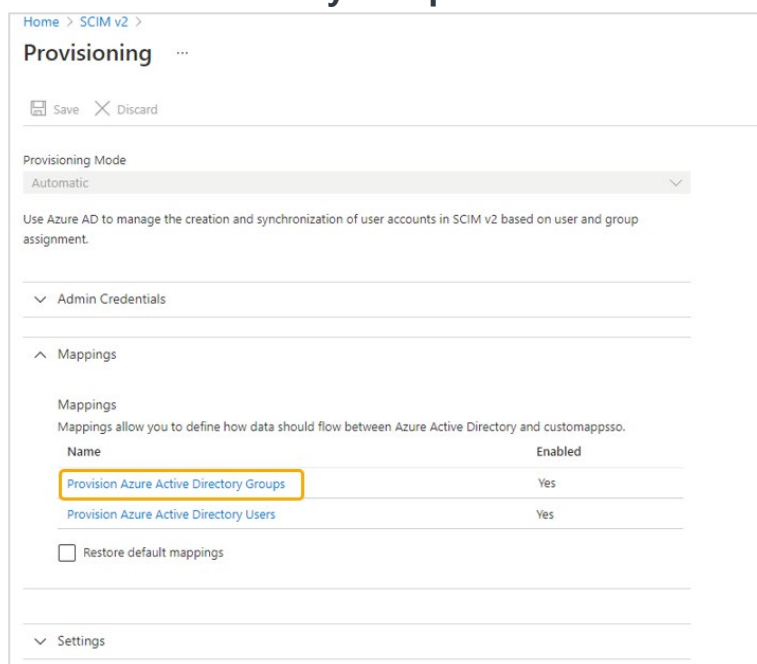
1. Go to the details of your **Azure** application (select **Azure Active Directory** > **Enterprise applications** in the menu and an application in the list), then select **Provisioning**.



2. On the **Provisioning** page, select **Edit provisioning** or **Edit attributes mapping** in the **Manage provisioning** section.



- On the **Provisioning** page, expand the **Mappings** section, and select **Provision Azure Active Directory Groups**.



Home > SCIM v2 > Provisioning

Provisioning ...

Save Discard

Provisioning Mode  
Automatic

Use Azure AD to manage the creation and synchronization of user accounts in SCIM v2 based on user and group assignment.

Admin Credentials

Mappings

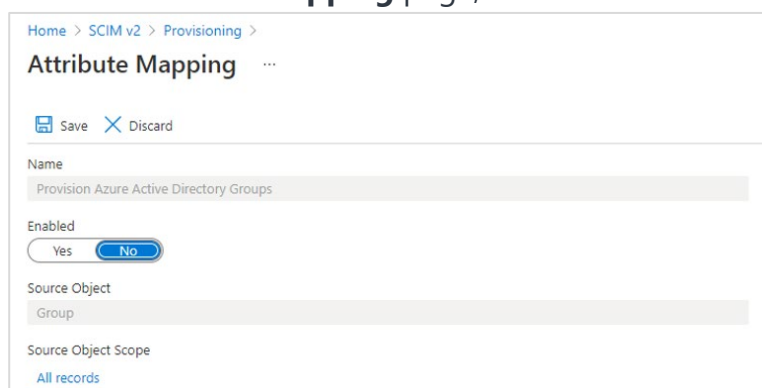
Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

☐ Restore default mappings

Settings

- On the **Attribute Mapping** page, select **No** in **Enabled**, and select **Save**.



Home > SCIM v2 > Provisioning > Attribute Mapping

Attribute Mapping ...

Save Discard

Name  
Provision Azure Active Directory Groups

Enabled  
Yes No

Source Object  
Group

Source Object Scope  
All records

Now, your group provisioning is disabled.

# Envi Configuration

To synchronize **Azure AD** with **Envi** via **SCIM**, perform the following actions:

1. Sign in to the **Envi** application.
2. Go to **My Profile > My Domain > Recourses** tab.
3. On the **Recourses** tab, select the **SCIM Configuration** link.

**Note:** The link is only available for domains with the **Simple** domain type and with the **HTTP Redirect** or **WS Trust** authentication.

Domains > Domain Name DomainName

**DETAILS** ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE RESOURCES SECURITY

[Edit](#)

Name: DomainName

Description: Description

Domain Type: Simple

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect

Failed Attempts: 2

Endpoint URL: http://12

Identifier URL: http://123

SSO Message: Please provide your SSO credentials for further logins

Do not require force authentication.

Do not require device registration.

Do not restrict IP Addresses

Do not use live metadata.

4. On the **SCIM Configuration** page, you will find the domain details of your configuration. By default, a new configuration will be **Inactive** and will contain no organizations. To proceed with further **SCIM** configuration, perform the following steps:
  - a. Select **Edit**.
  - b. In the **Status** dropdown, select **Active**.
  - c. In the **Organization** dropdown, select a needed organization.
  - d. Select **Update**.

Domains > Domain Name **For Testing Purpose**

**DETAILS** ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE **RESOURCES** SECURITY

[Update](#) [Cancel](#)

Status: Active

Organization\*: For Testing Purpose

Valid Token: Yes

User Role Prefix\*: Envi\_

- Once you have updated **SCIM** configurations, select the **Create Token**, then **Copy Token** button.

**Note:** Enter the obtained **SCIM** token in the **Secret Token** box ([Azure AD Configuration](#), step 7).

The screenshot shows a web interface for managing domains. At the top, there's a breadcrumb 'Domains > Domain Name' followed by a blurred domain name. Below this is a horizontal menu with tabs: 'DETAILS', 'ORGANIZATIONS', 'USERS', 'PASSWORD DICTIONARIES', 'UPDATE', 'RESOURCES' (which is active and highlighted in blue), and 'SECURITY'. Under the 'RESOURCES' tab, there are four buttons: 'Edit' (with a pencil icon), 'Create Token', 'Copy Token', and 'Go Back'. Below the buttons, there are four rows of configuration details: 'Status: Active', 'Organization: For Testing Purpose', 'Valid Token: Yes', and 'User Role Prefix: Envi\_'.

Domains > Domain Name <b>[Blurred]</b>	
DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE <b>RESOURCES</b> SECURITY	
<b>Edit</b> Create Token Copy Token Go Back	
Status:	Active
Organization:	For Testing Purpose
Valid Token:	Yes
User Role Prefix:	Envi_

Now, **Azure AD SCIM** is configured and synchronized.