Azure AD SCIM

Integration Guide

Table of Contents

Introduction

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

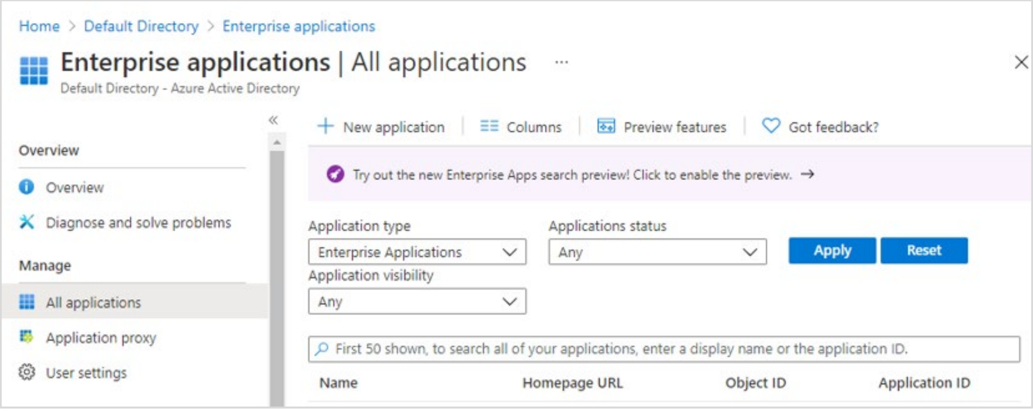
SCIM enables IT departments to automate provisioning and deprovisioning of accounts, which reduces manual redundant processes and increases security.

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**.



Try out the new Enterprise Apps search preview! Click to enable the preview. →

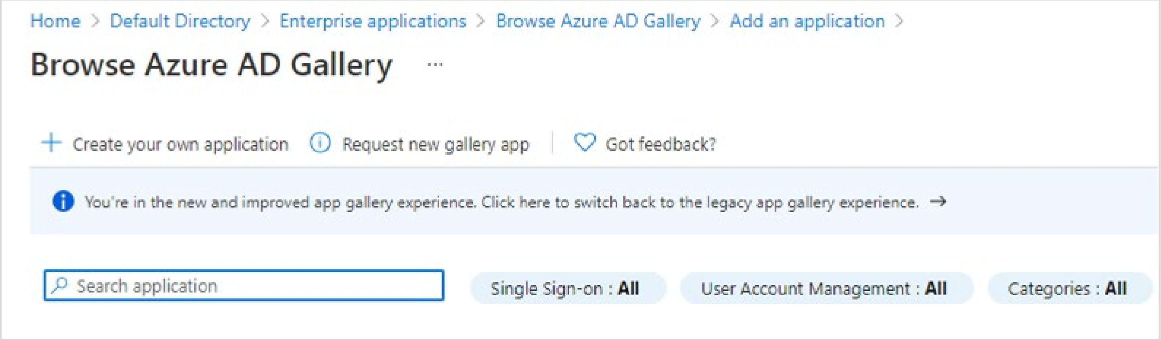
Application type: Enterprise Applications

Applications status: Any

Application visibility: Any

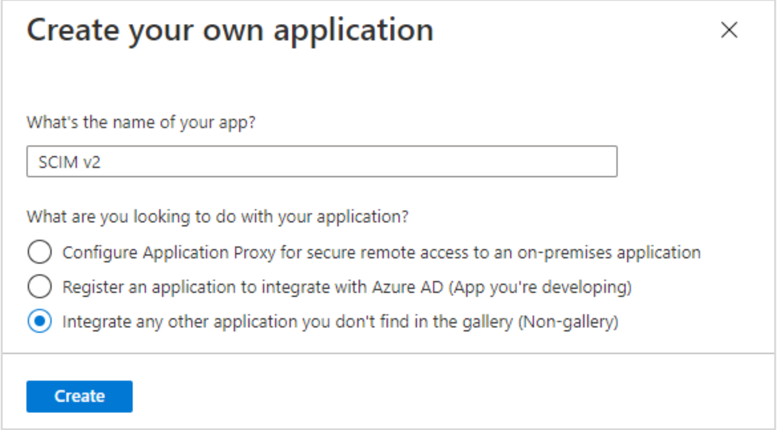
First 50 shown, to search all of your applications, enter a display name or the application ID.

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


Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Add an application >
Browse Azure AD Gallery
+ Create your own application
Request new gallery app
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

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**.



What's the name of your app?

SCIM v2

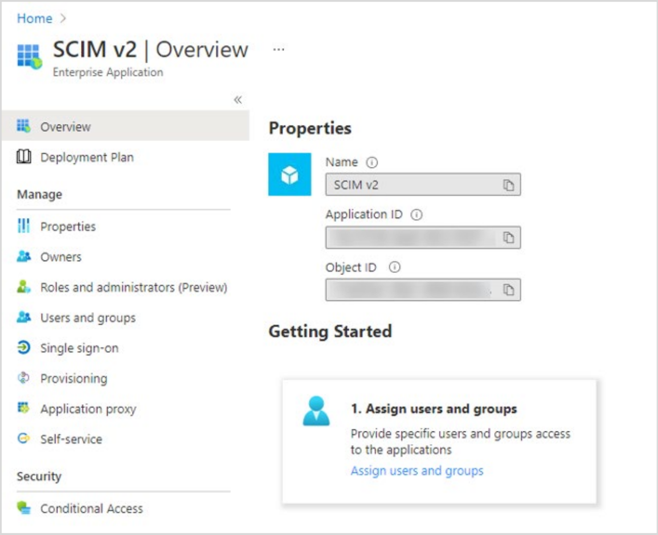
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

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



Home >

SCIM v2 | Overview ···

Enterprise Application

Properties

Name ⓘ
SCIM v2

Application ID ⓘ
[redacted]

Object ID ⓘ
[redacted]

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

Assign users and groups

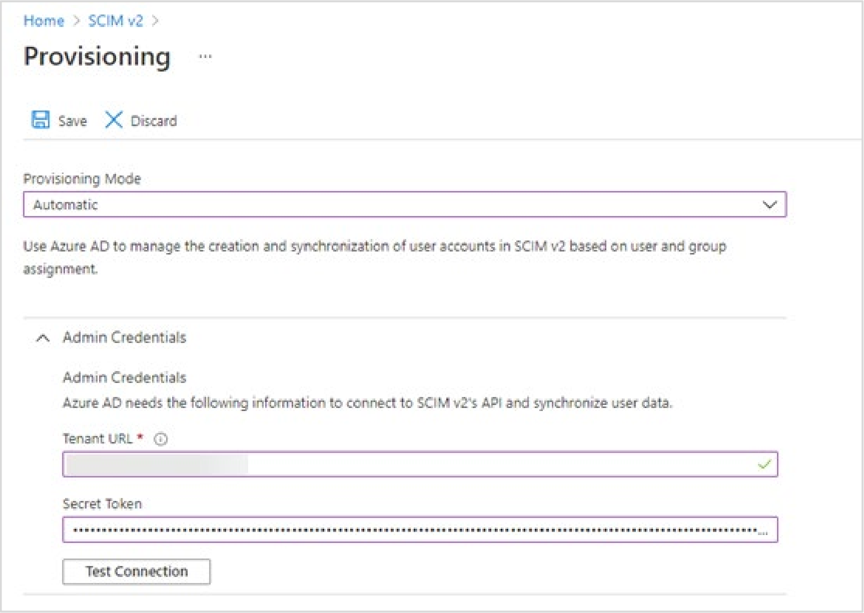
7. On the **Provisioning** page, perform the following steps:

   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.



Home > SCIM v2 >

Provisioning ···

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

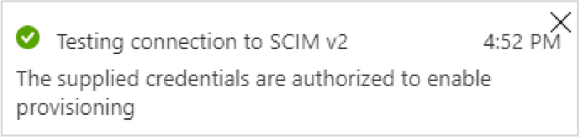
Admin Credentials

Azure AD needs the following information to connect to SCIM v2's API and synchronize user data.

Tenant URL * ⓘ
[redacted]

Secret Token
••...

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



Testing connection to SCIM v2 4:52 PM

The supplied credentials are authorized to enable provisioning

9. Select **Save**.

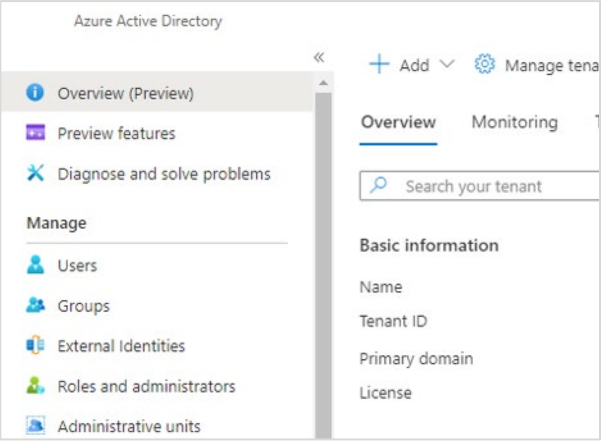
At this point, your configuration is ready for use.

Provisioning

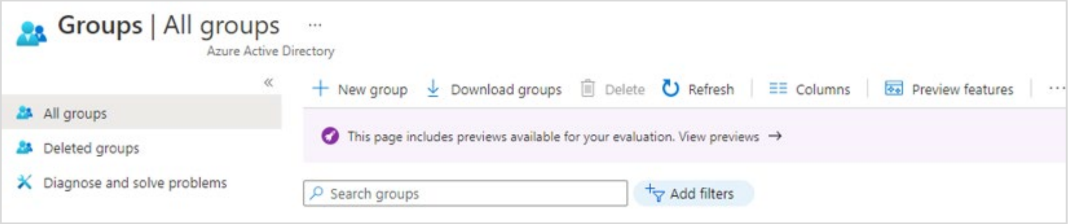
In this section, you will learn how to provision new users and groups.

Group Provisioning

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



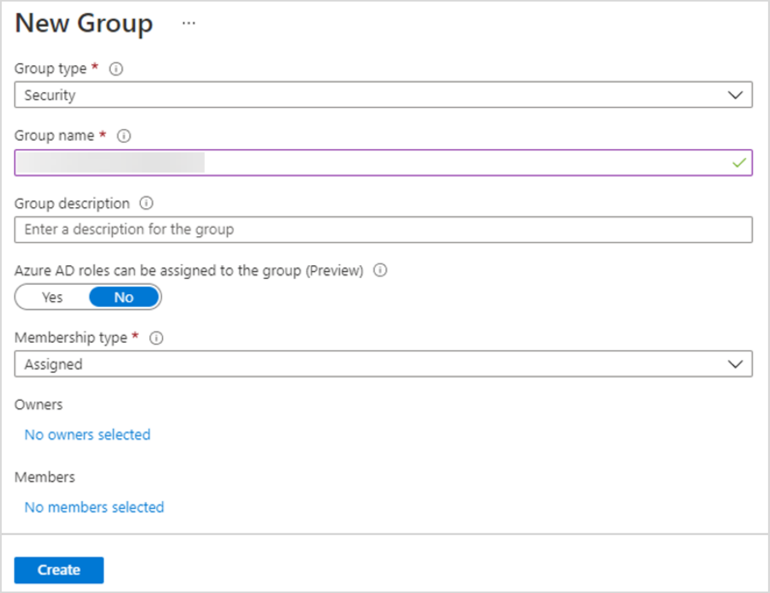
2. On the **Enterprise Applications** page, select **+New group**.



This page includes previews available for your evaluation. View previews →

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**.


New Group ···

Group type * ⓘ
Security

Group name * ⓘ
[redacted]

Group description ⓘ
Enter a description for the group

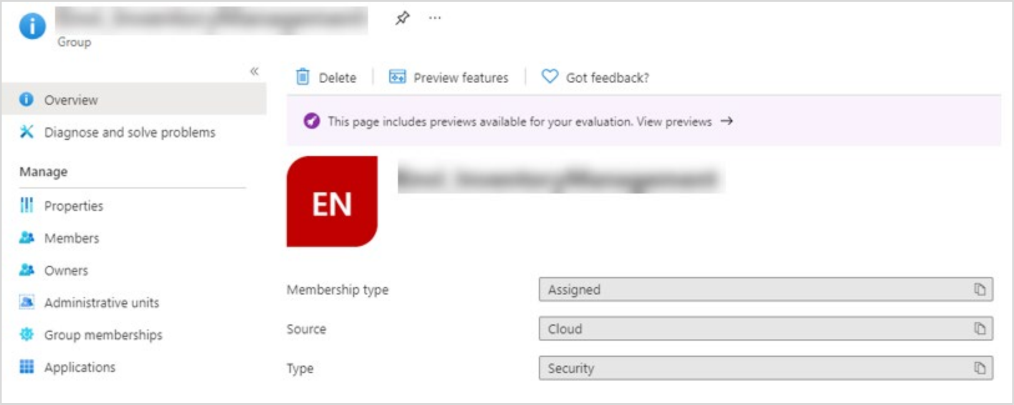
Azure AD roles can be assigned to the group (Preview) ⓘ
Yes [✓ No]

Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

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



This page includes previews available for your evaluation. View previews →

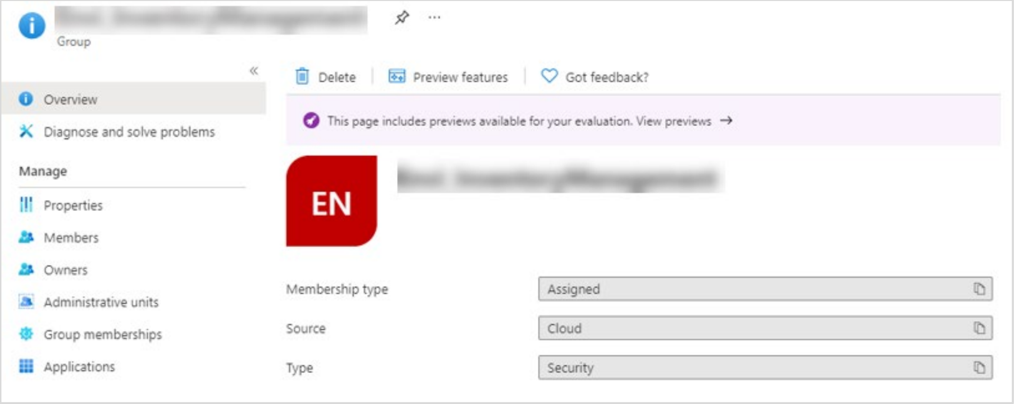
Membership type: Assigned

Source: Cloud

Type: Security

User Provisioning

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



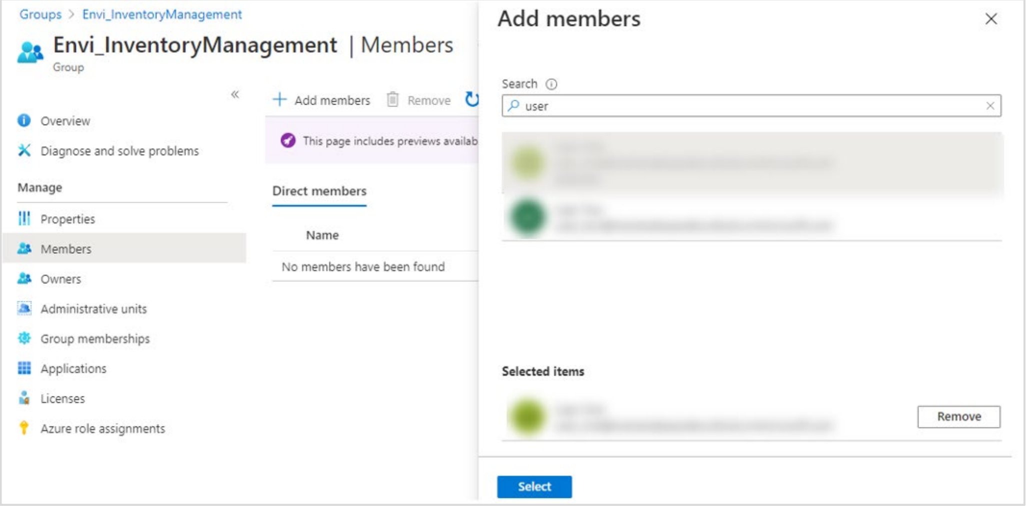
This page includes previews available for your evaluation. View previews →

Membership type: Assigned

Source: Cloud

Type: Security

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.



This page includes previews availab

No members have been found

Search: user

[redacted]

[redacted]

[redacted]

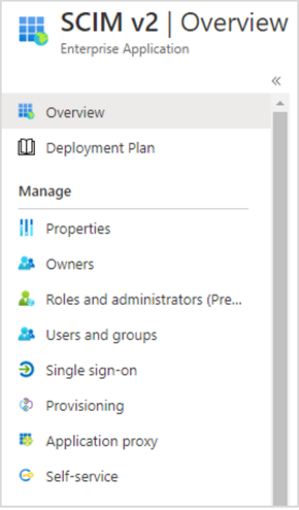
Note: Repeat the process of group creation and user assignment for all other users and groups that you want to add.

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**

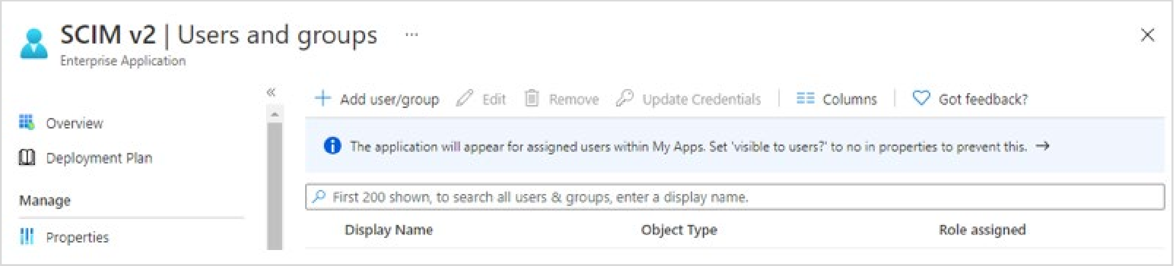
Prefix (Envi_) on the **SCIM Configuration** page (the Envi Configuration section).

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.

3. 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**.



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

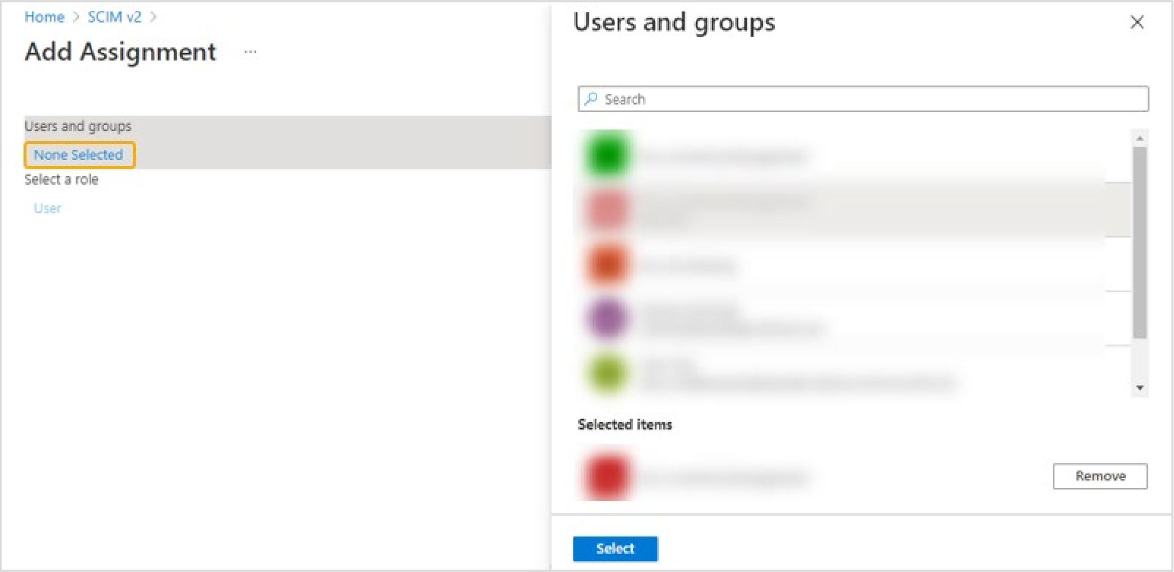


The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

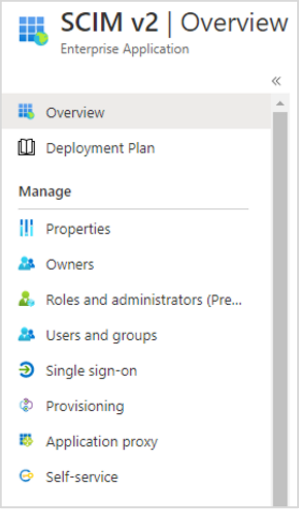
First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned

5. 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.

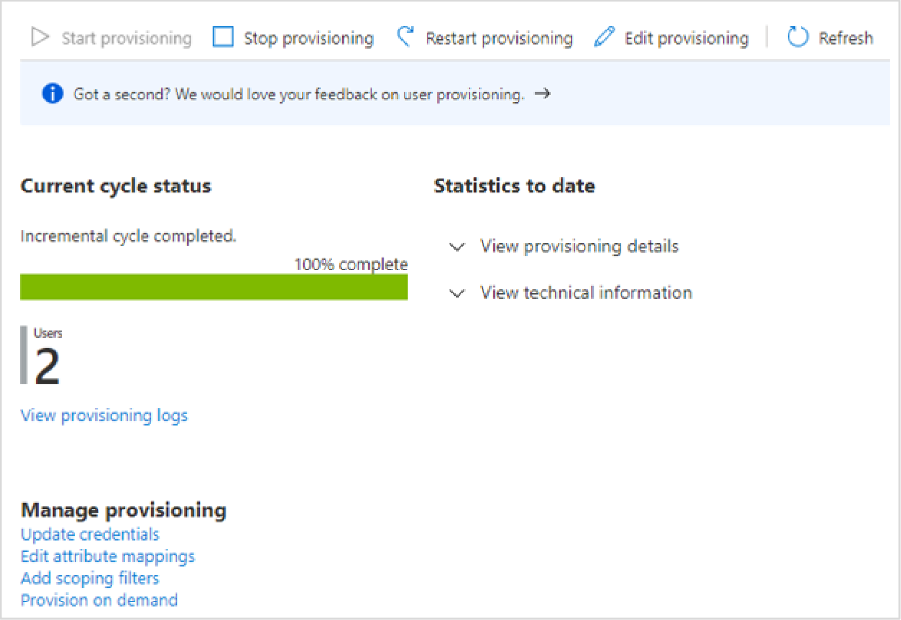


6. Go to the details of your **Azure** application (select **Azure Active Directory** > **Enterprise applications** in the menu and an application in the list), then select **Provisioning**.



SCIM v2 | Overview
Enterprise Application

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



Got a second? We would love your feedback on user provisioning. →

Current cycle status

Incremental cycle completed.

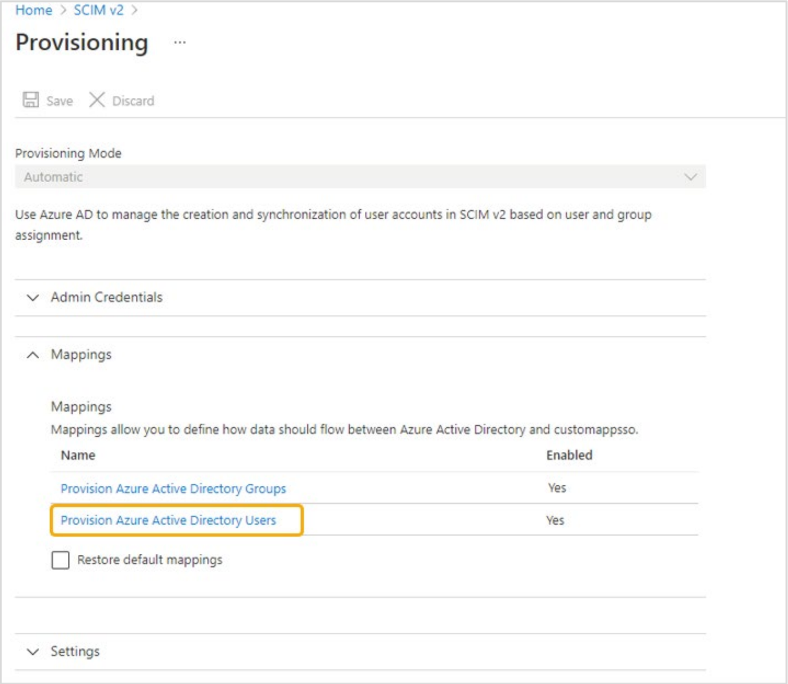
100% complete

Users
2

Statistics to date

Manage provisioning

8. 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

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

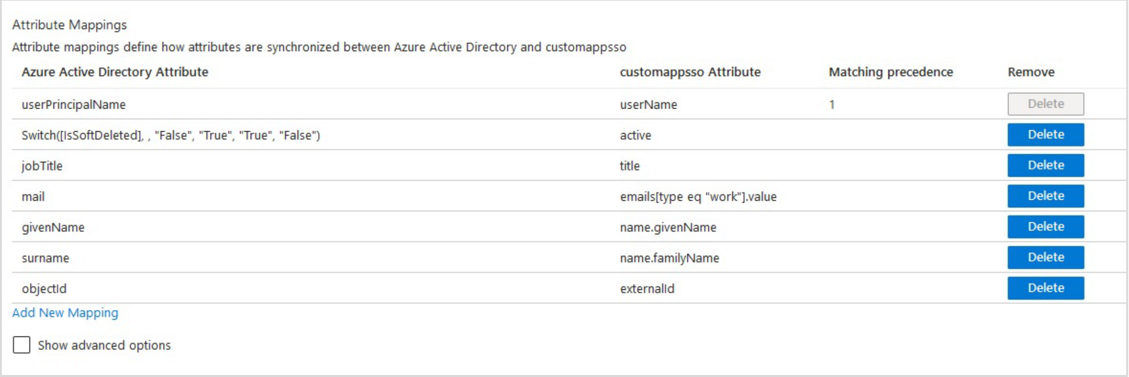
Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

□ Restore default mappings

Settings

9. 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
- title
- emails[type eq "work"].value
- name.givenName
- name.familyName
- externalId



Attribute Mappings

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

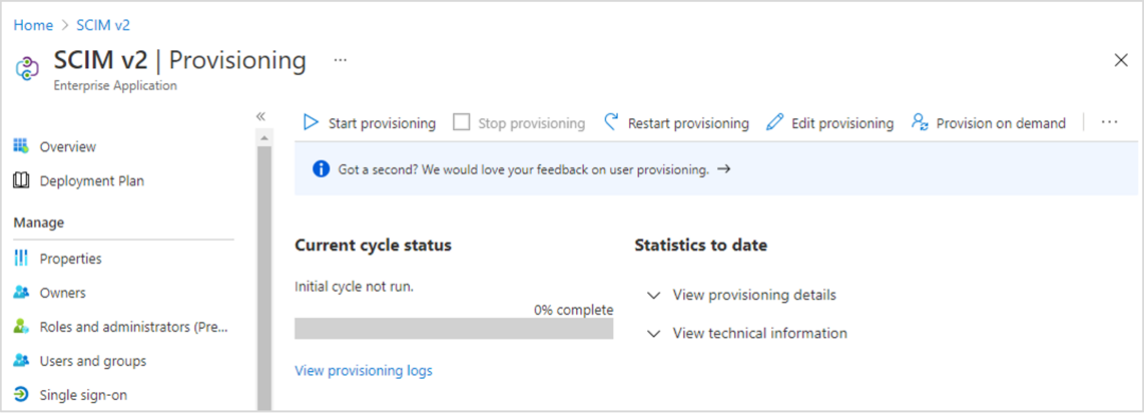
Azure Active Directory Attribute	customappsso Attribute	Matching precedence	Remove
userPrincipalName	userName	1	Delete
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active		Delete
jobTitle	title		Delete
mail	emails[type eq "work"].value		Delete
givenName	name.givenName		Delete
surname	name.familyName		Delete
objectId	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.



Home > SCIM v2

SCIM v2 | Provisioning

Enterprise Application

Got a second? We would love your feedback on user provisioning. →

Current cycle status

Initial cycle not run.

0% complete

View provisioning logs

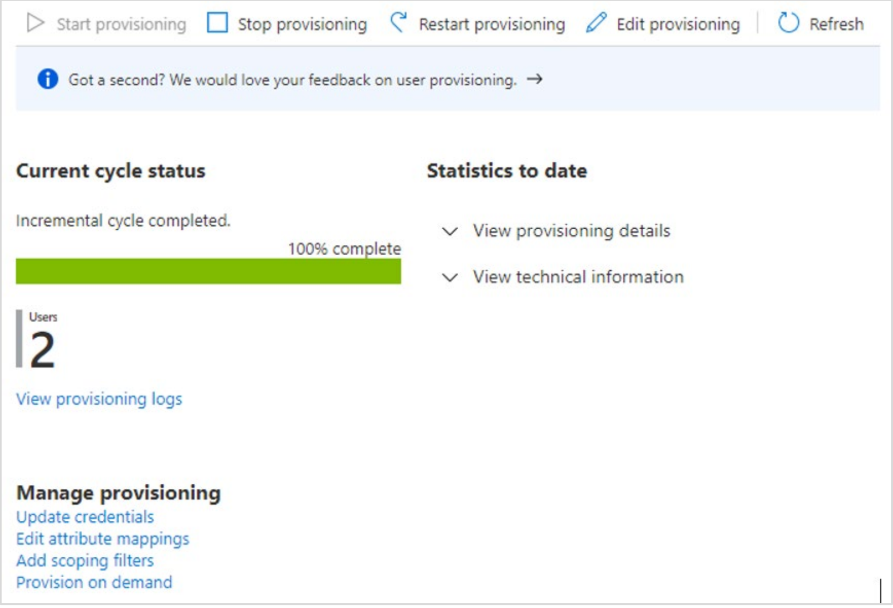
Statistics to date

View provisioning details

View technical information

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.



Got a second? We would love your feedback on user provisioning. →

Current cycle status

Incremental cycle completed.

100% complete

Users

2

View provisioning logs

Statistics to date

View provisioning details

View technical information

Manage provisioning

Update credentials

Edit attribute mappings

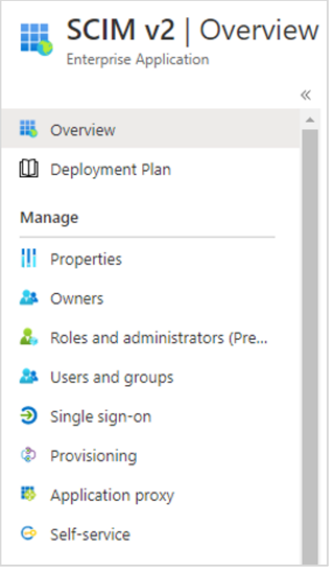
Add scoping filters

Provision on demand

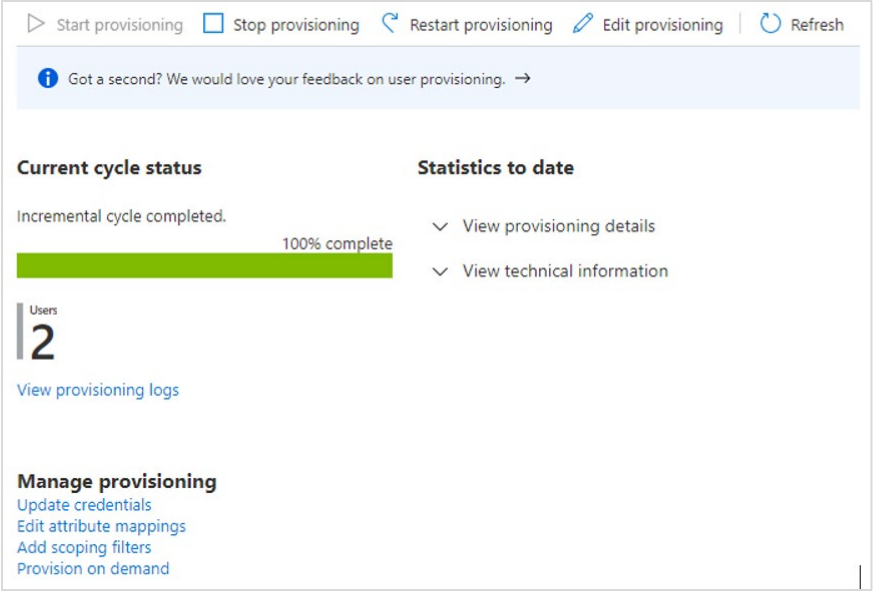
Now, the needed members and groups are added.

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.

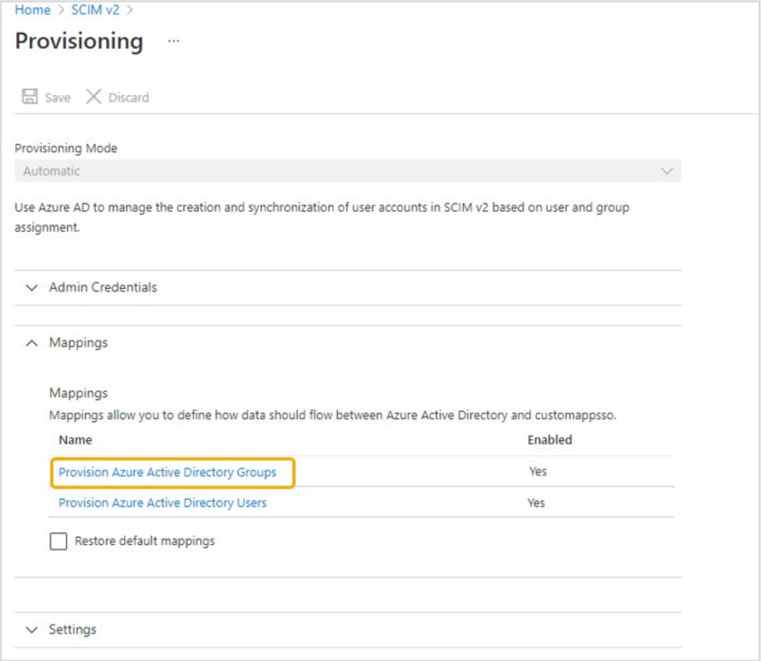


Got a second? We would love your feedback on user provisioning. →

Current cycle status

Incremental cycle completed.

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



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

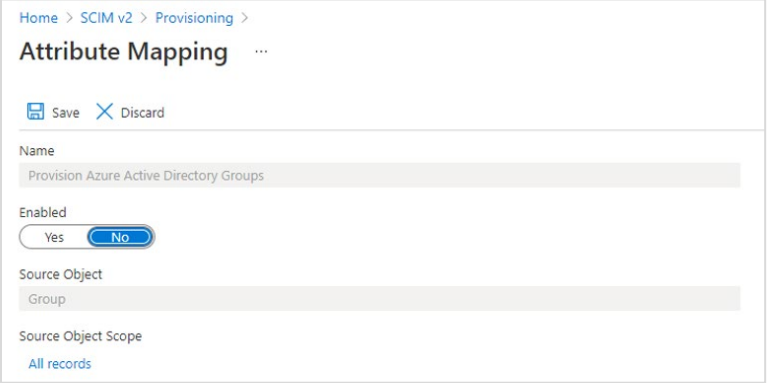
Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

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

□ Restore default mappings

Settings

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



Home > SCIM v2 > Provisioning >

Attribute Mapping ···

Save Discard

Name

Provision Azure Active Directory Groups

Enabled

Yes [✓ No]

Source Object

Group

Source Object Scope

All records

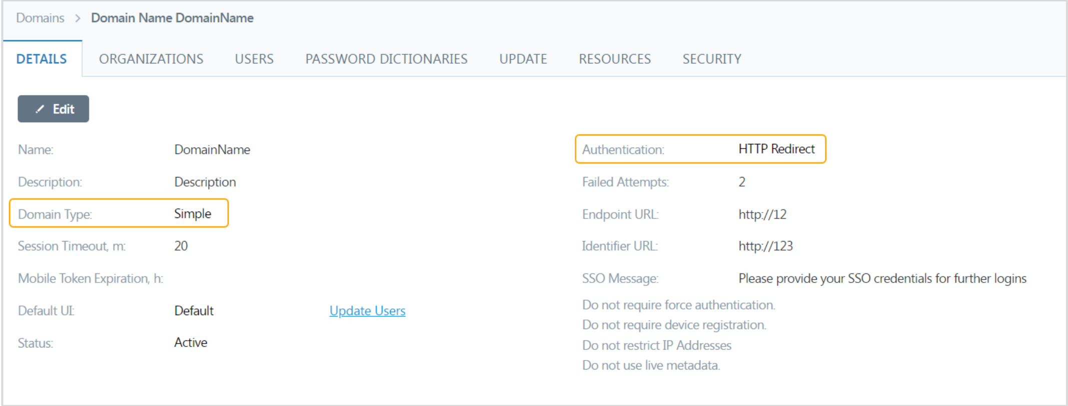
Now, your group provisioning is disabled.

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

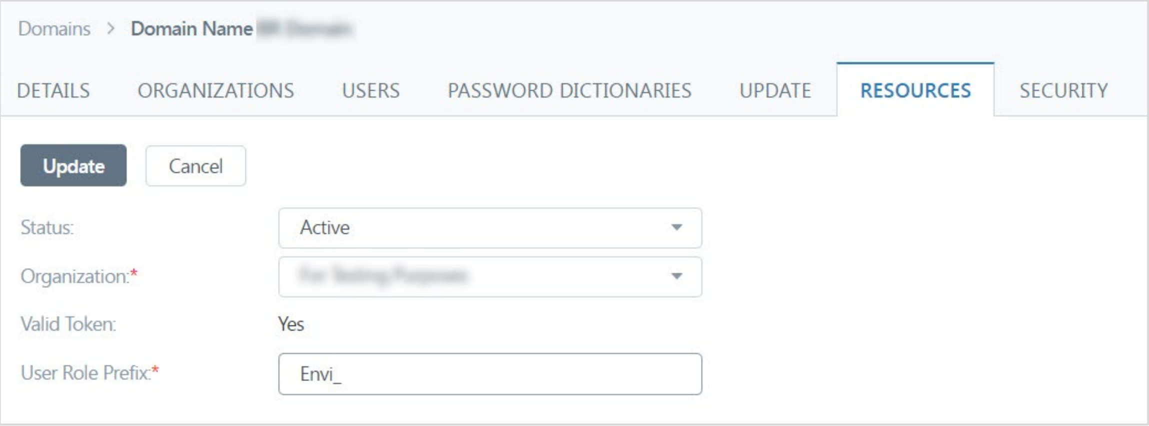
DETAILS | ORGANIZATIONS | USERS | PASSWORD DICTIONARIES | UPDATE | RESOURCES | SECURITY

Edit

Name:	DomainName		Authentication:	HTTP Redirect
Description:	Description		Failed Attempts:	2
Domain Type:	Simple		Endpoint URL:	http://12
Session Timeout, m:	20		Identifier URL:	http://123
Mobile Token Expiration, h:			SSO Message:	Please provide your SSO credentials for further logins
Default UI:	Default	Update Users	Do not require force authentication.	
Status:	Active		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 [redacted]

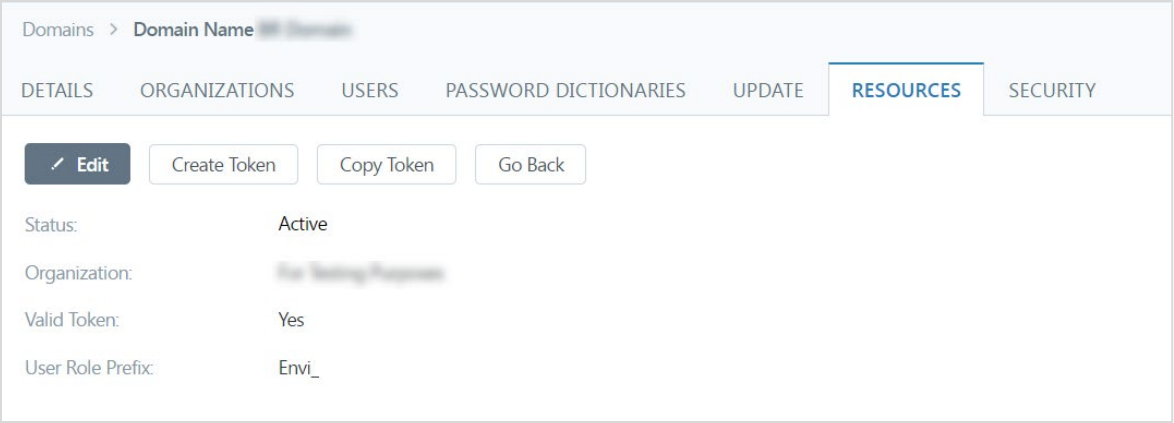
DETAILS | ORGANIZATIONS | USERS | PASSWORD DICTIONARIES | UPDATE | RESOURCES | SECURITY

Update | Cancel

Status:	Active
Organization:*	[redacted]
Valid Token:	Yes
User Role Prefix:*	Envi_

5. 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).



Status: Active

Organization: [redacted]

Valid Token: Yes

User Role Prefix: Envi_

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