bitwarden | Help Center Article

ADMIN CONSOLE > MANAGE MEMBERS > SCIM

Microsoft Entra ID SCIM

View in the help center:
https://bitwarden.com/help/microsoft-entra-id-scim-integration/

Microsoft Entra ID SCIM

System for cross-domain identity management (SCIM) can be used to automatically provision and de-provision members and groups in your Bitwarden organization.

> **Note**
>
> SCIM integrations are available for **Teams and Enterprise organizations**. Customers not using a SCIM-compatible identity provider may consider using Directory Sync as an alternative means of provisioning.

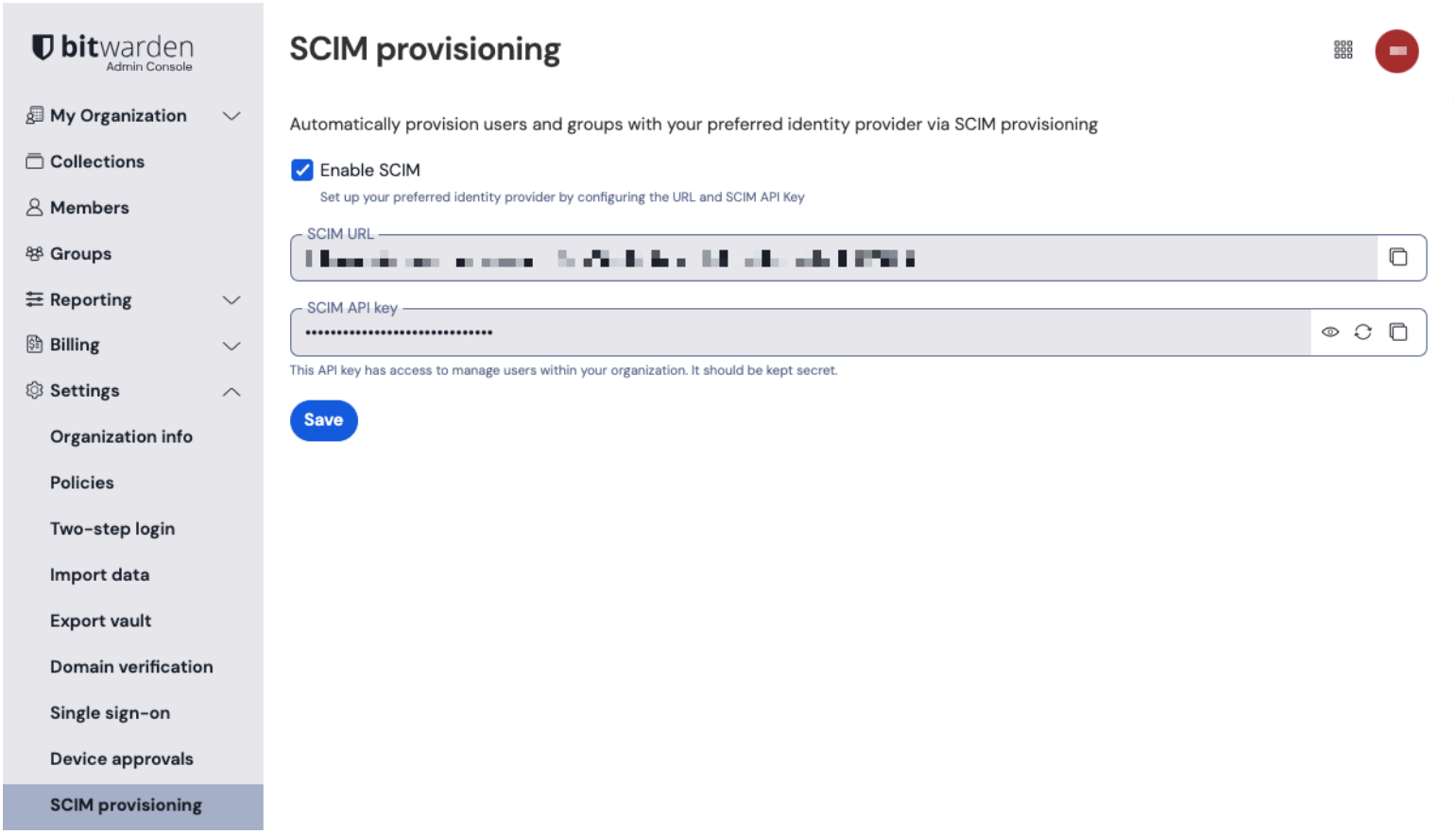
This article will help you configure a SCIM integration with Azure. Configuration involves working simultaneously with the Bitwarden web vault and Azure Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

> **Tip**
>
> **Already an expert?** Skip the instructions in this article and download the quick configuration guide to setup SSO and SCIM with Entra ID.
>
> Quick reference guide

Enable SCIM

> **Note**
>
> **Are you self-hosting Bitwarden?** If so, complete these steps to enable SCIM for your server before proceeding.

To start your SCIM integration, open the Admin Console and navigate to **Settings** → **SCIM provisioning**:



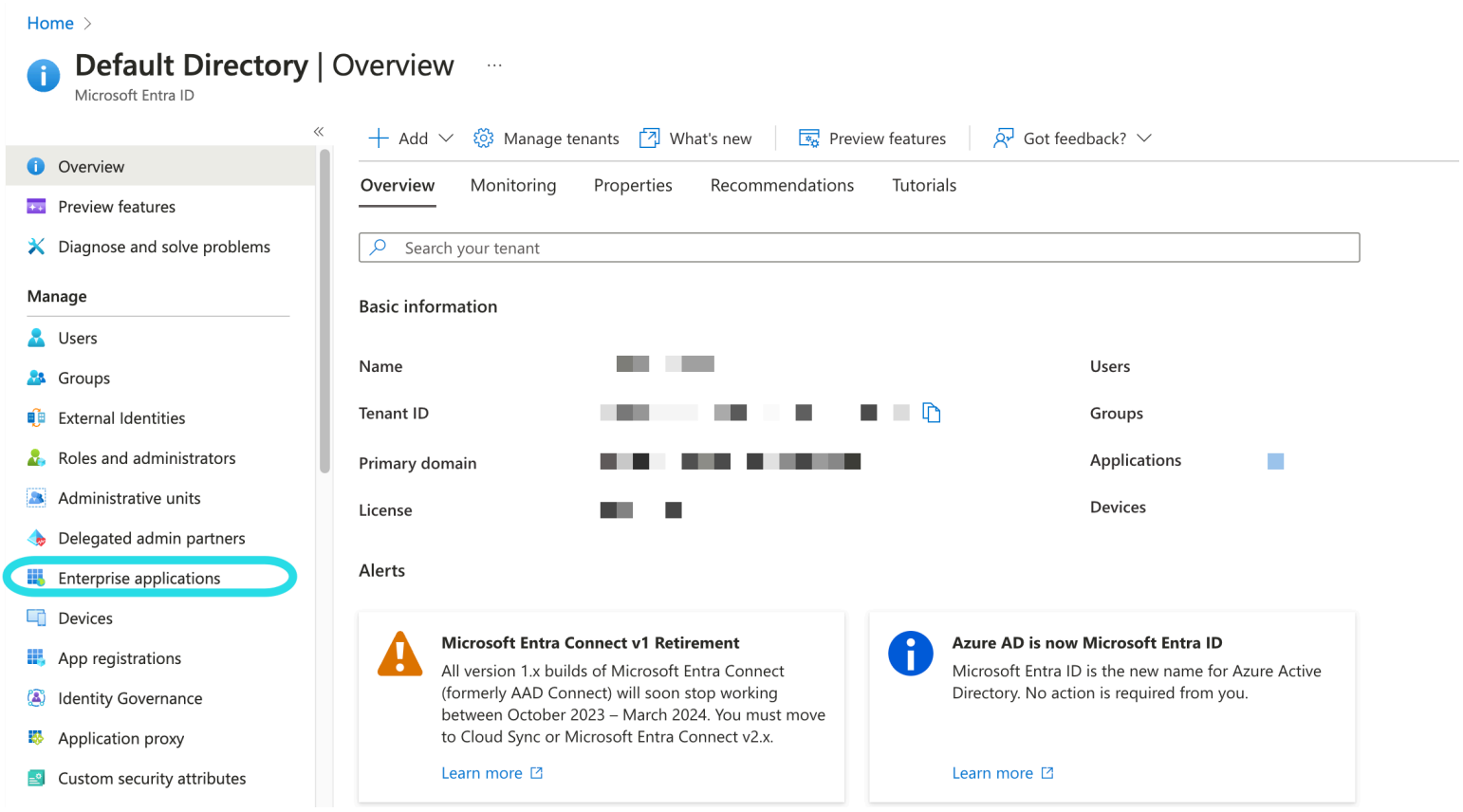
SCIM provisioning

Select the **Enable SCIM** checkbox and take note of your **SCIM URL** and **SCIM API Key**. You will need to use both values in a later step.

Create an enterprise application

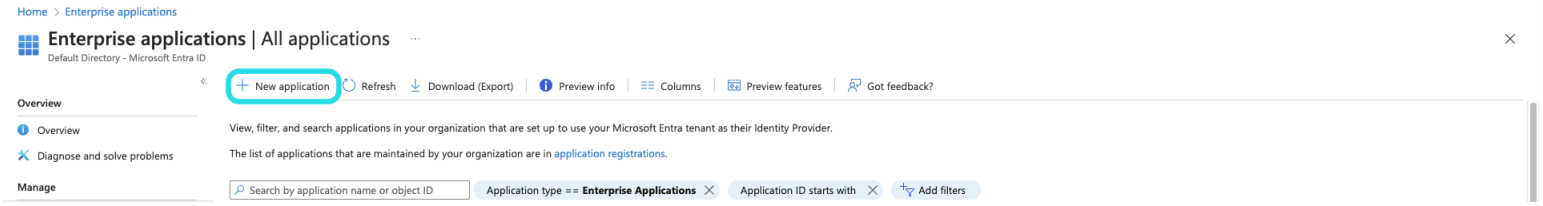
> **Tip**
>
> If you are already using this IdP for Login with SSO, open that existing enterprise application and skip to this step. Otherwise, proceed with this section to create a new application

In the Azure Portal, navigate to **Microsoft Entra ID** and select **Enterprise applications** from the navigation menu:



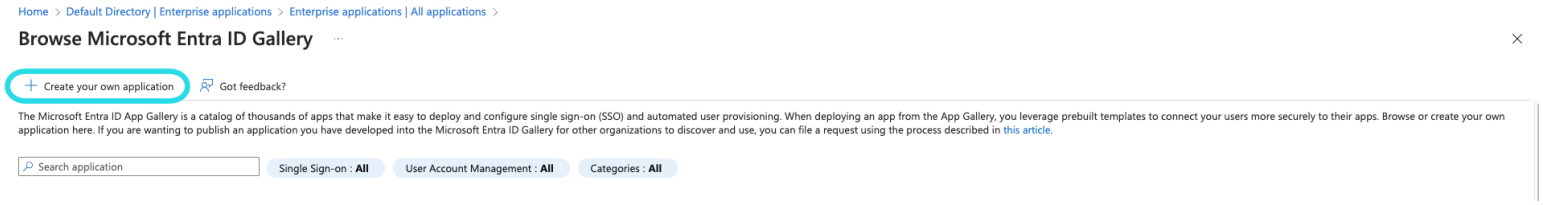
Enterprise applications

Select the ＋ **New application** button:



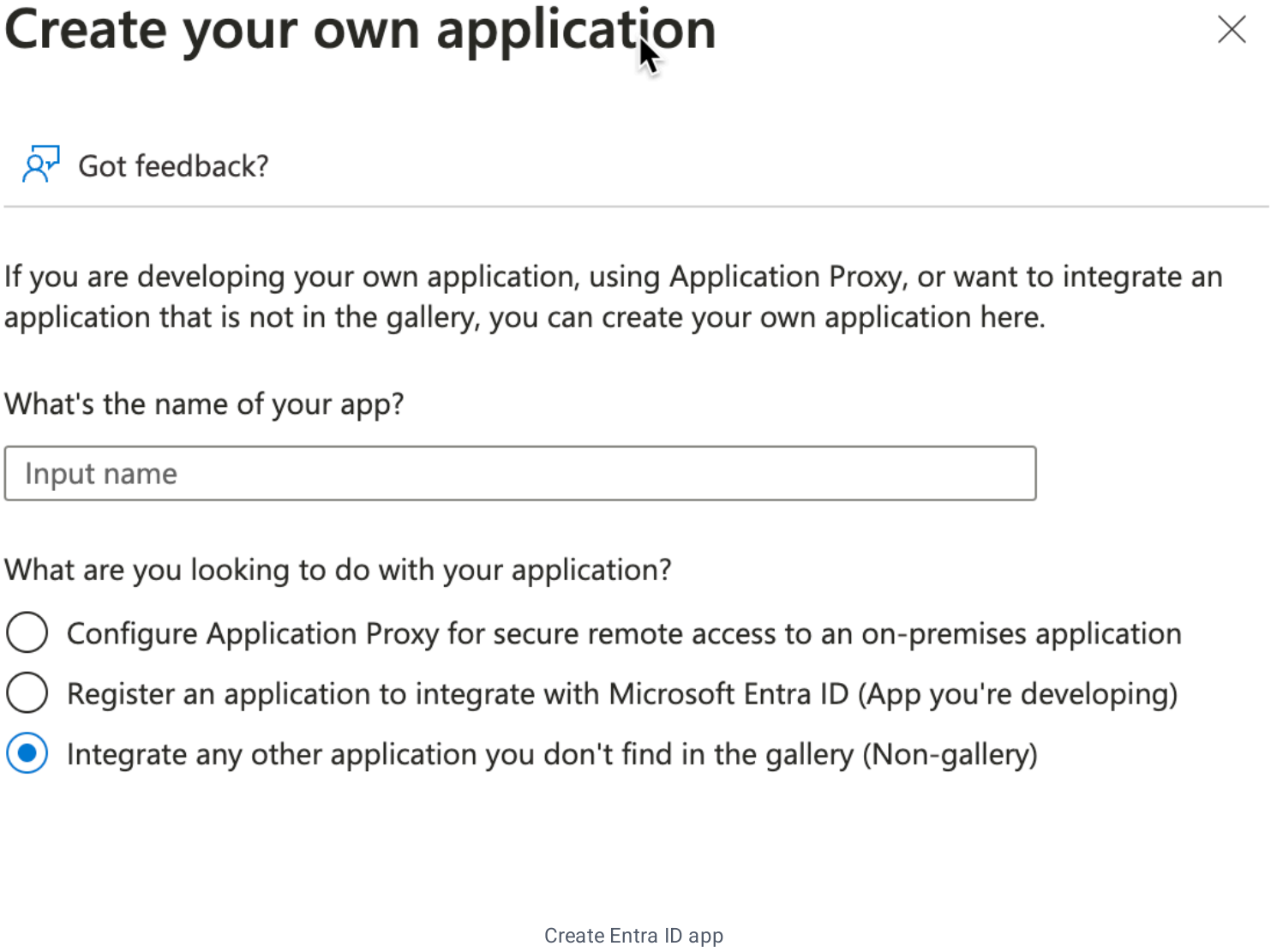
Create new application

On the Browse **Microsoft Entra ID** Gallery screen, select the ＋ **Create your own application** button:



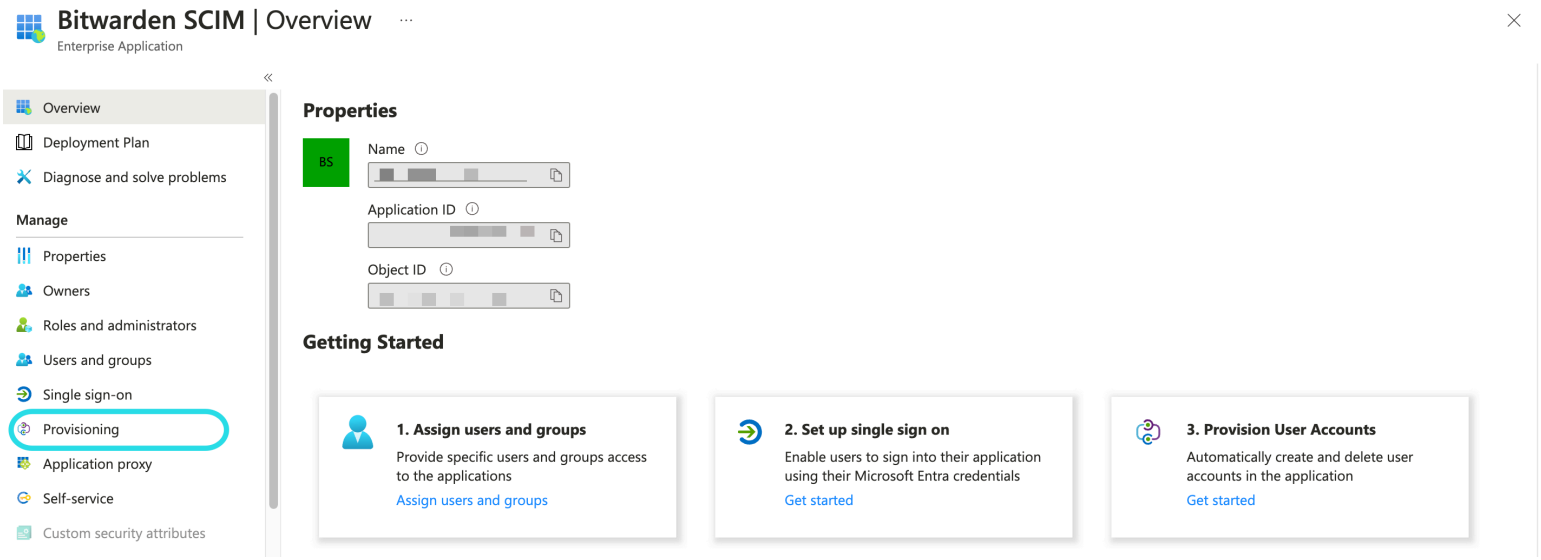
Create your own application

On the Create your own application screen, give the application a unique, Bitwarden-specific name. Choose the **Non-gallery** option and then select the **Create** button.



Enable provisioning

Select **Provisioning** from the navigation and complete the following steps:



Select Provisioning

1. Select the **Get started** button.
2. Select **Automatic** from the **Provisioning Mode** dropdown menu.
3. Enter your SCIM URL (learn more) in the **Tenant URL** field.
4. Enter your SCIM API Key (learn more) in the **Secret Token** field.
5. Select the **Test Connection** button.
6. If your connection test successfully, select the **Save** button.

Mappings

This screen is available while performing initial setup for the Enterprise Application, or by navigating to the Enterprise Application, and selecting **Provisioning** under the **Manage** section of the left-hand menu, and then selecting **Edit Provisioning** at the top.

Bitwarden uses standard SCIM v2 attribute names, though these may differ from Microsoft Entra ID attribute names. The default mappings will work, but you can use this section to make changes if you wish.

User mapping

If you would like User objects in your directory to synchronize with Bitwarden, you may enable or disable **Provision Microsoft Entra ID Users**. This is enabled by default. Select the **Provision Microsoft Entra ID Users** link to customize the attributes sent to Bitwarden with user objects. The following table describes the default mappings for attributes used by Bitwarden:

Bitwarden attribute	Default AAD attribute
`active`	`Switch([IsSoftDeleted], , "False", "True", "True", "False")`
`emails`[a] or `userName`	`mail` or `userPrincipalName`
`displayName`	`displayName`
`externalId`	`mailNickname`

[a] - Because SCIM allows users to have multiple email addresses expressed as an array of objects, Bitwarden will use the `value` of the object which contains `"primary": true`.

User mapping with object identifiers

User mappings may be more performant if they prioritize mapping on an Entra `objectId` over other attributes. Mapping in this way will preserve the connection to a Bitwarden account if the corresponding Entra ID account's email address changes, for example in the case of a name change. To implement this, make the following changes to your user mapping scheme:

- Map the `externalId` to `objectId` instead of `mailNickname`.
- For the `externalId` to `objectId` mapping, set **Match objects using this attribute** to Yes.
- For the `externalId` to `objectId` mapping, set **Matching precedence** to 1.
- For the `userName` (**customerappsso Attribute**) to `userPrincipalName` or `mail` (**Microsoft Entra ID Attribute**) mapping, set **Matching precedence** to 2.

> **⚠ Warning**
>
> If you're implementing this mapping strategy **after users have already been synced to Bitwarden** using SCIM, note that those already-synced users will not have had external IDs set by an Entra ID object ID. For these users, use the Public API's `/public/members/{id}` endpoint to set their external IDs.

Group mapping

If you would like Group objects in your directory to synchronize with Bitwarden, you may enable or disable **Provision Microsoft Entra ID Groups**. This option is enabled by default. Select the **Provision Microsoft Entra ID Groups** link to customize the attributes sent to Bitwarden

with the groups objects if you wish to make changes according to the following table:

Bitwarden attribute	Default AAD attribute
`displayName`	`displayName`
`members`	`members`
`externalId`	`objectId`

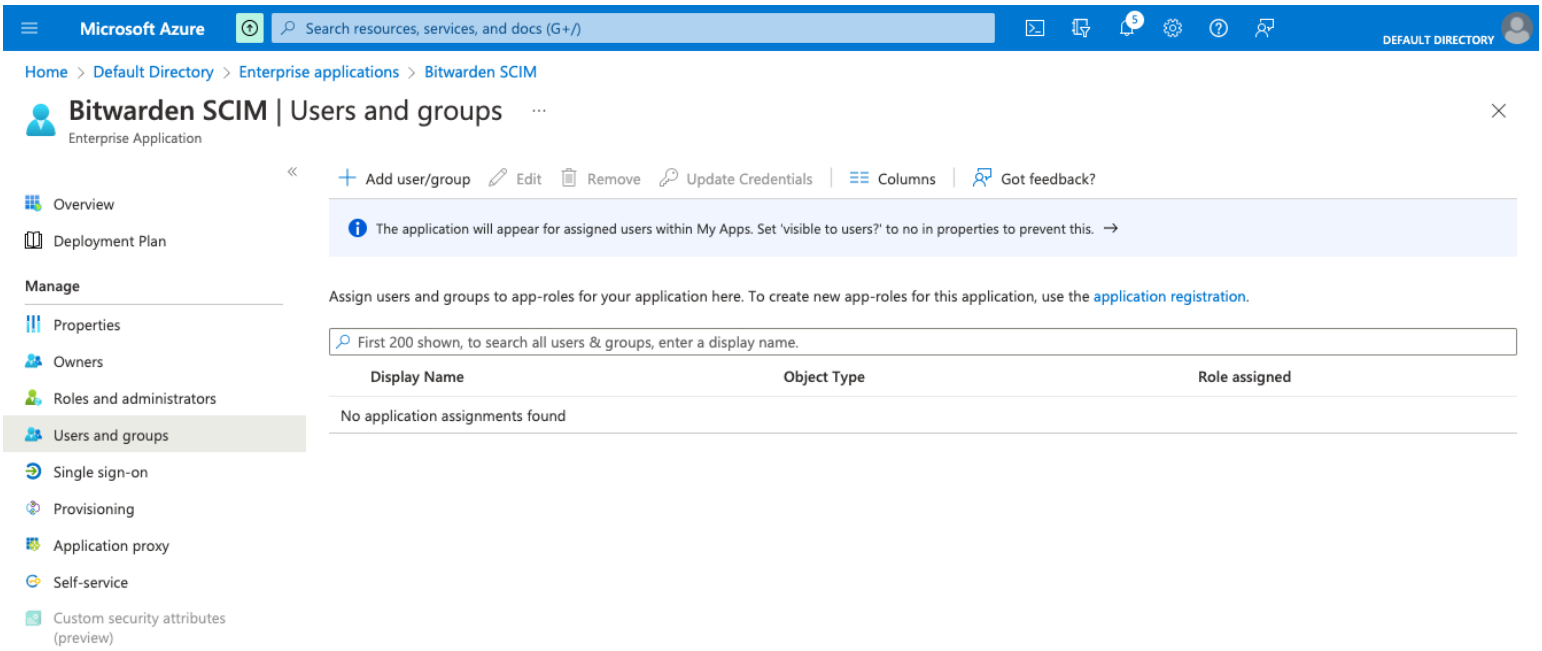
Settings

Under the **Settings** dropdown, choose:

- Whether to send an email notification when failure occurs, and if so, what address to send it to (recommended).
- Whether to **sync only assigned users and groups** or **sync all users and groups**. This setting is modified based your Mapping configuration. For example, if Group mapping is disabled, Groups added to the Enterprise Application will synchronize only the User objects who are members of the Group, and not create the Group in Bitwarden itself. If you choose to sync all users and groups, skip the next step, as your entire directory will be synchronized, depending on your Mapping settings.

Assign users and groups

Complete this step if you have selected to **sync only assigned users and groups** from the provisioning settings. Select **Users and groups** from the navigation:



Enterprise application users and groups

Select the ＋ **Add user/group** button to assign access to the SCIM application on a user or group level. The following sections describe how modifying users and groups in Azure will impact their counterparts in Bitwarden:

Users

If **Provision Microsoft Entra ID Users** has been enabled in your Mappings, the following actions are taken:

- When a new user is assigned in Azure, the user is invited to your Bitwarden organization.
- When a user who is already a member of your organization is assigned in Azure, the Bitwarden user is linked to the Azure user through their first available matching precedence attribute.
  - Users linked in this way are still subject to the other workflows in this list, however values like `displayName` and `externalId/mailNickname` are not automatically changed in Bitwarden.
- When an assigned user is disabled via the `accountEnabled` property in Azure, the user has their access to the organization revoked.
- When an assigned user is "soft" deleted in Azure, the user has their access to the organization revoked.
  - When the user is permanently deleted in Azure, the user is removed from the organization.
- When an assigned user is removed from the Enterprise application in Azure, the user has their access to the organization revoked.
- When an assigned user is removed from a group in Azure, the user is removed from that group in Bitwarden but remains a member of the organization.

Groups

If you have **Provision Microsoft Entra ID Groups** enabled in your Mappings, the following actions are taken:

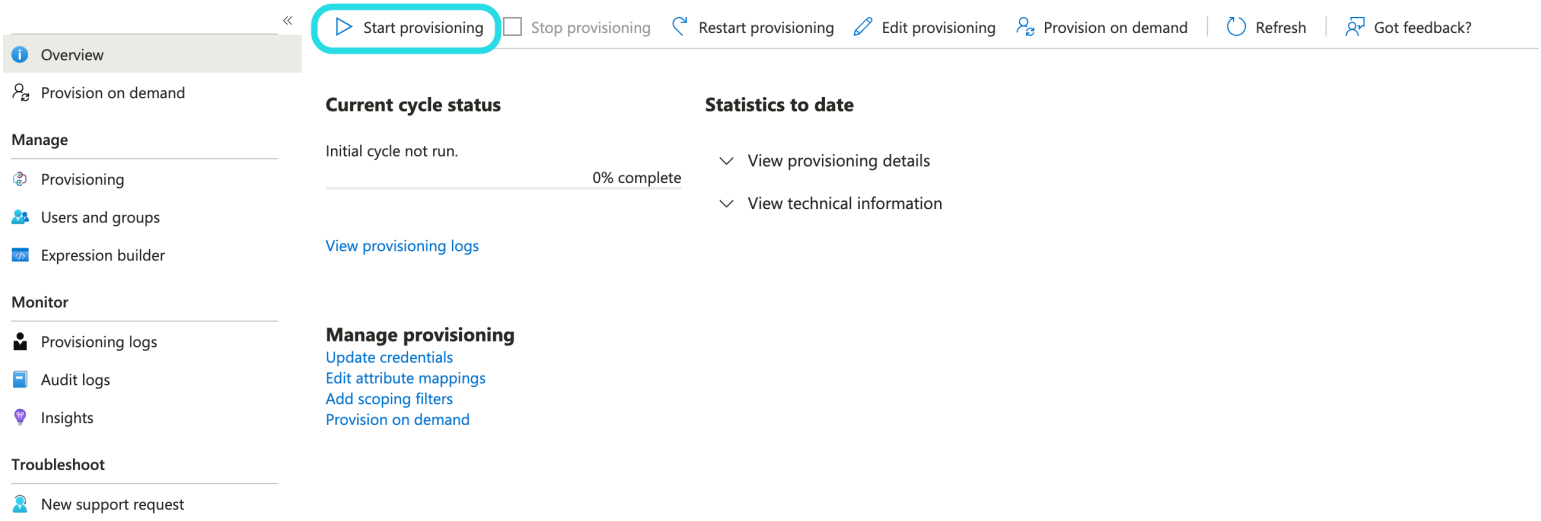
- When a new group is assigned in Azure, the group is created in Bitwarden.
  - Group members who are already members of your Bitwarden organization are added to the group.
  - Group members who are not already members of your Bitwarden organization are invited to join.

- When a group that already exists in your Bitwarden organization is assigned in Azure, the Bitwarden group is linked to Azure through the first available matching precedence attribute.
  - Groups linked in this way will have their members synced from Azure.

- When a group is renamed in Azure, it will be updated in Bitwarden as long as the initial sync has been made.
  - When a group is renamed in Bitwarden, it will be changed back to what it's named in Azure. Always change group names Azure-side.

Start provisioning

Once the application is fully configured, start provisioning by selecting the ▷ **Start provisioning** button on the enterprise application's **Provisioning** page:



Start provisioning

Finish user onboarding

Now that your users have been provisioned, they will receive invitations to join the organization. Instruct your users to accept the invitation and, once they have, confirm them to the organization.

> **Note**
>
> The Invite → Accept → Confirm workflow facilitates the decryption key handshake that allows users to securely access organization vault data.