Connecting and Setting up Microsoft Entra ID

Get your team connected and set up with Microsoft Entra ID in Groopit!

Contents

- Supported features
- Requirements
- Configuration Steps

Supported features

- Single Sign-On via OpenID Connect (OIDC)
- Provisioning users and groups with SCIM (optional)

Requirements

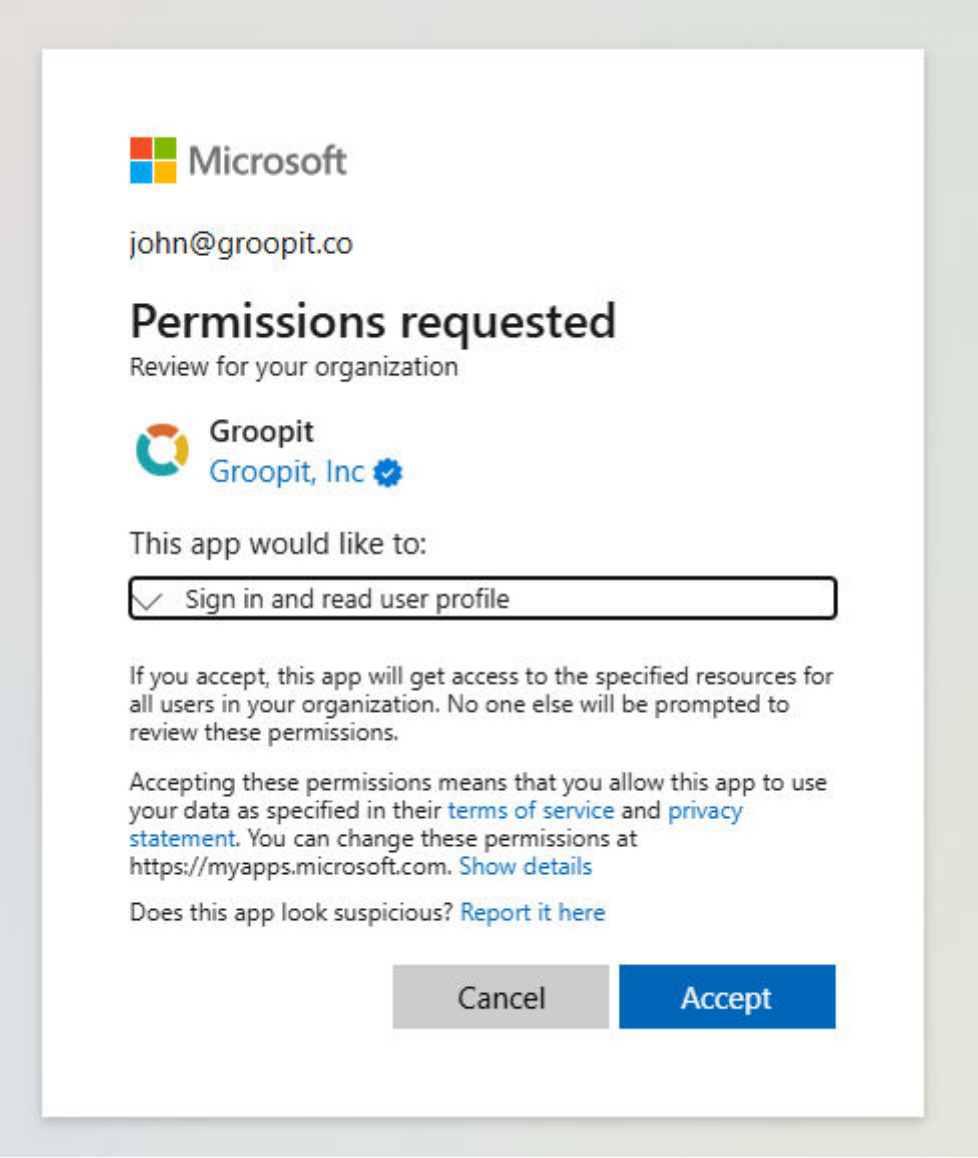
- Your Groopit organization must be part of an organization with an active Groopit Enterprise Subscription
- An Entra user account with one of the following roles: Global Administrator, Cloud Application Administrator, or Application Administrator

SSO Configuration Steps

1. First, install the Groopit application within your Entra tenant. With

   Click on this link:
   https://login.microsoftonline.com/common/adminconsent?client_id=732fe7e0-d0e2-4baf-874a-91fe944f2534&prompt=consent&redirect_uri=https%3A%2F%2Fapp.groopit.co

   If you are logged in with an Entra admin account, you will be presented with the admin consent dialog.



2. After granting the requested permissions, Entra configuration is complete. Contact your Groopit customer support representative to enable SSO for the Groopit application.

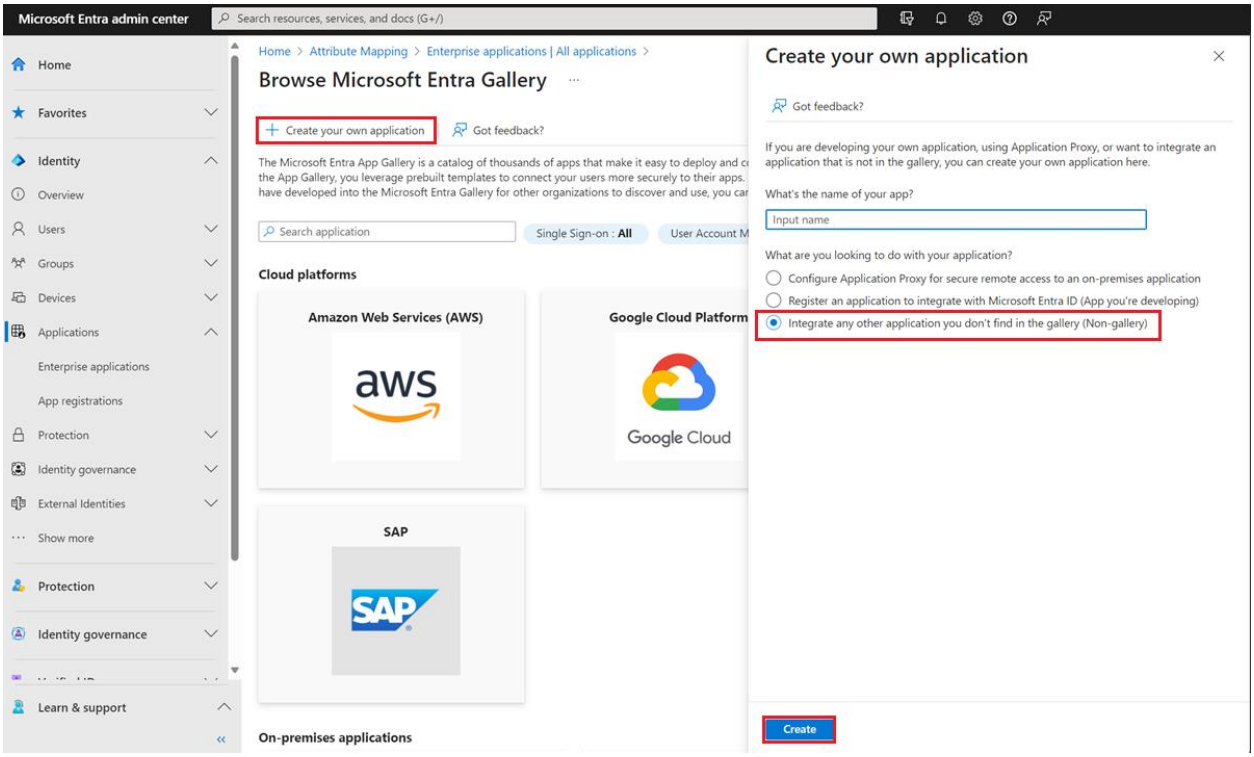
SCIM Configuration Steps

If you are planning to use Entra security groups to control access to Groopit groups, the use of SCIM (System for Cross-domain Identity Management) is recommended. Groopit provides a SCIM-compliant endpoint, but it must be manually added to the Entra tenant to enable SCIM provisioning. The first part of this process must be performed by the tenant administrator in the Groopit application.

1. Go to the Groopit SCIM Integration page at https://app.groopit.co/tenant/ScimSettings
2. Check the “Enable” box.
3. Use the “Copy” buttons to copy the SCIM Endpoint and SCIM Secret into a local document. These values will be needed by the IT administrator to complete the SCIM configuration.

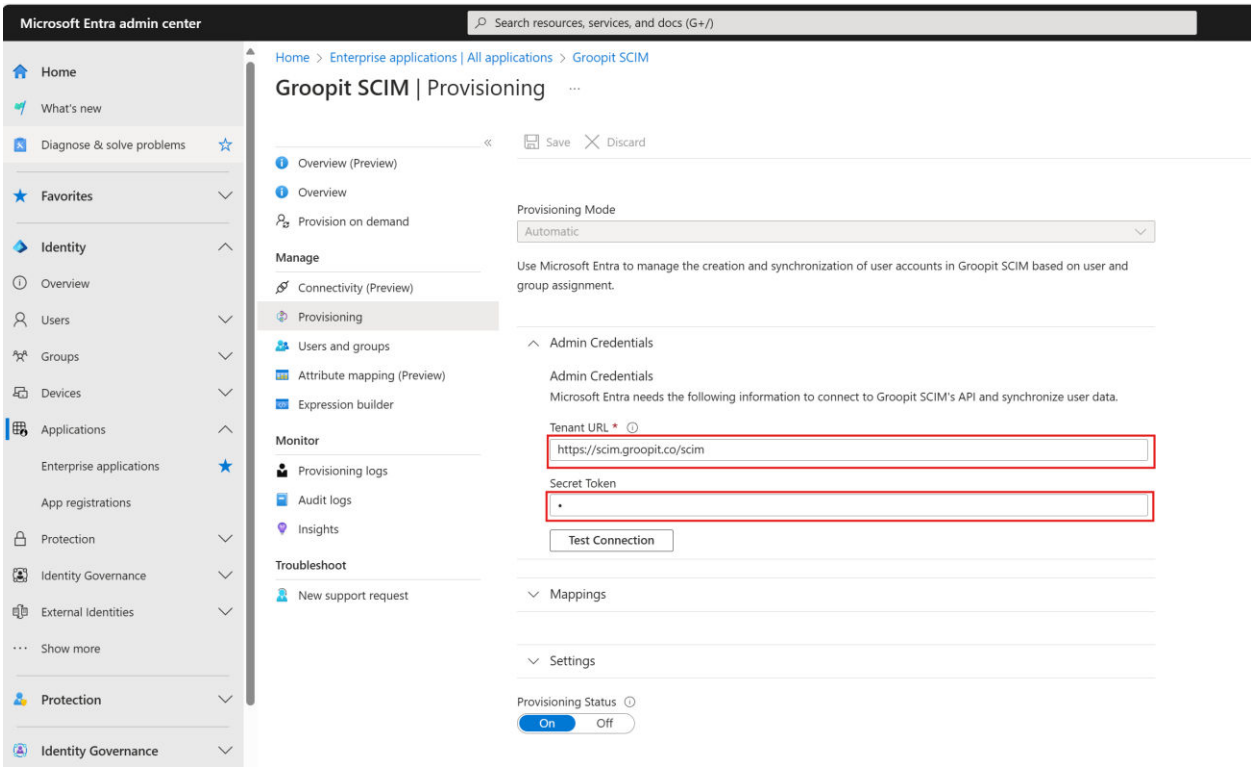
The following steps must be completed by an Entra administrator. More details are provided by Microsoft in the article **Integrate your SCIM endpoint with the Microsoft Entra provisioning service** and the Entra administrator should familiarize themselves with this overview. The Entra administrator will need the SCIM Endpoint and SCIM Secret values obtained by the tenant administrator in the first part of the process.

1. From the Entra Admin Center select Identity->Applications->Enterprise Applications in the left-hand navigation panel.
2. Select “New Application” then “Create your own application” and choose the “Non-gallery” option. Name the application “Groopit SCIM” and Create it.

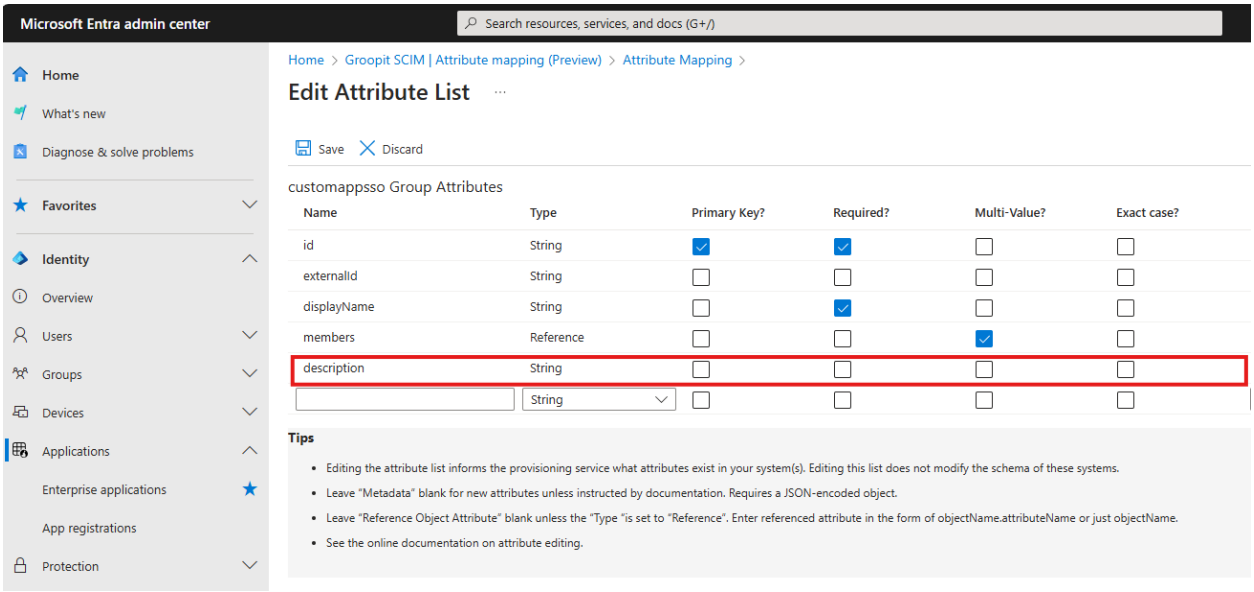


3. Once Entra creates the application, select “Provisioning” from the left navigation panel. Change the provisioning mode to “Automatic” and fill in the “Tenant URL” and “Secret Token” fields

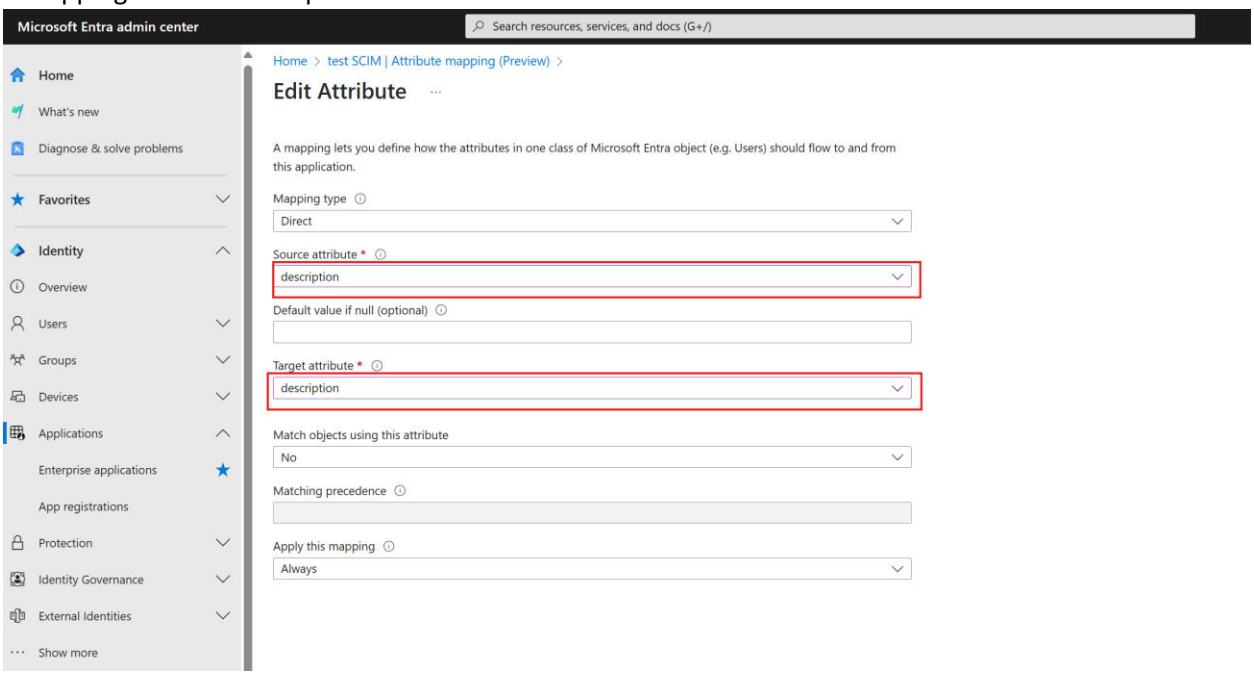
with the values obtained from the Groopit administrator.



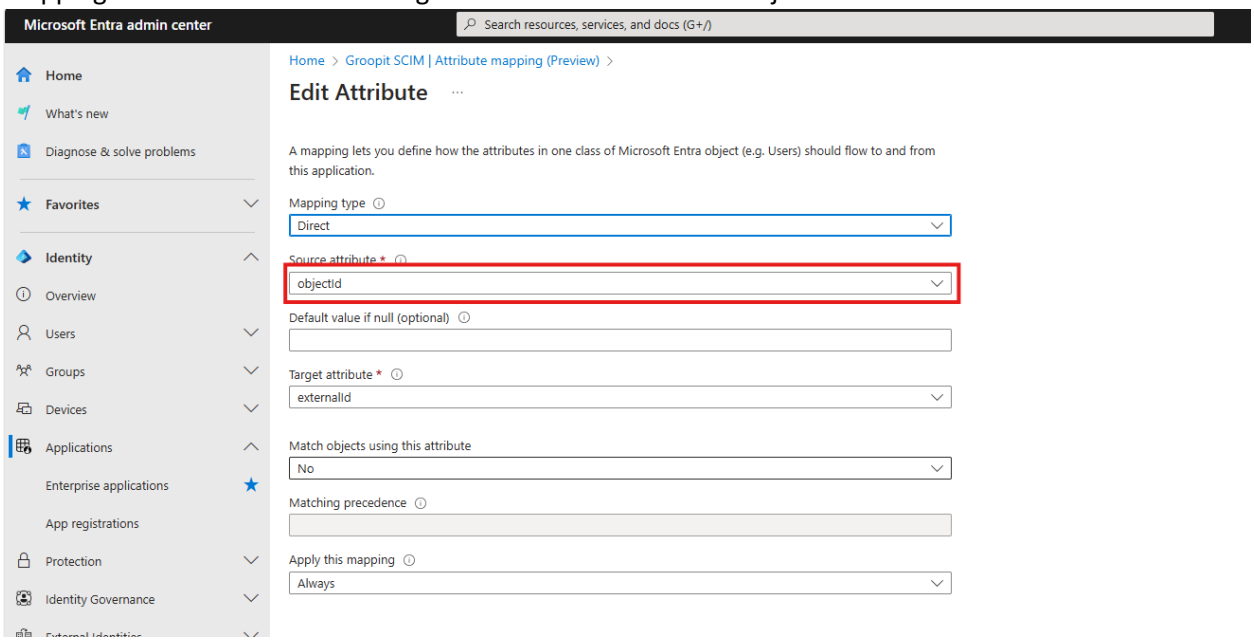
4. Select “Test Connection” and verify that the URL and secret are working correctly, then Save your changes.
5. Select Attribute Mapping and “Provision Microsoft Entra ID Groups”. Under Attribute Mapping, select “Show advanced options” then "Edit attribute list for customappsso". Add a new attribute with the name “description” and type “String”. Save the changes



6. Now you should be back on the Attribute Mapping page. Select “Add New Mapping” and create a mapping for the “description” attribute.



7. Return to the Attribute mapping page and select “Provision Microsoft Entra ID Users”. Edit the mapping for “externalId” and change the source attribute to “objectId”



8. Mapping configuration is now complete. Use the left navigation panel to access “Users and groups” Add all the Entra groups that should be synchronized with Groopit to the list. (Note that nested groups are not supported and this is an Entra limitation)
9. Test your provisioning by navigating to “Provision on demand” and searching for a group that was added in the previous step. Click the Provision button and ensure everything is working correctly.

10. Once you are satisfied that provisioning is working correctly, go to the Overview tab and click “Start Provisioning” This will update the assigned groups and their members on a regular basis. You can also provide an email address to receive notifications if there are any failures during synchronization.