Azure Active Directory Setup in Sendio

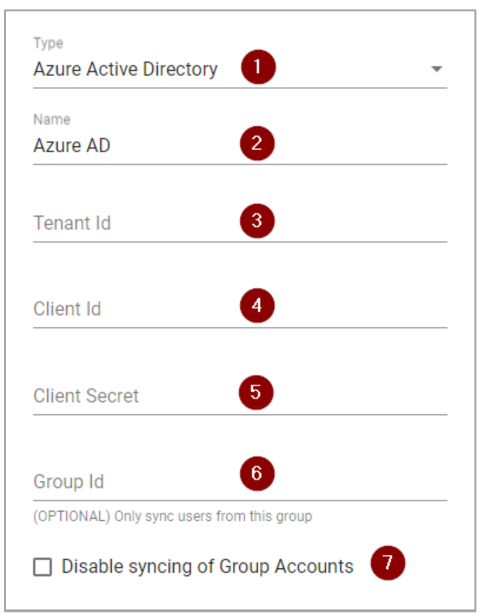
Overview

Sendio will allow you to sync your Azure Active Directory associated with Office 365 to create your Sendio accounts. If you have moved to Azure AD, Sendio can now sync with your cloud-based AD, removing the need to have an on-premises Active Directory server for Sendio account authentication. Integration also allows users to authenticate against Azure AD.

Create new directory in the Sendio admin UI

You will need the following information to complete directory setup, obtained when completing App Registration in Microsoft Azure console

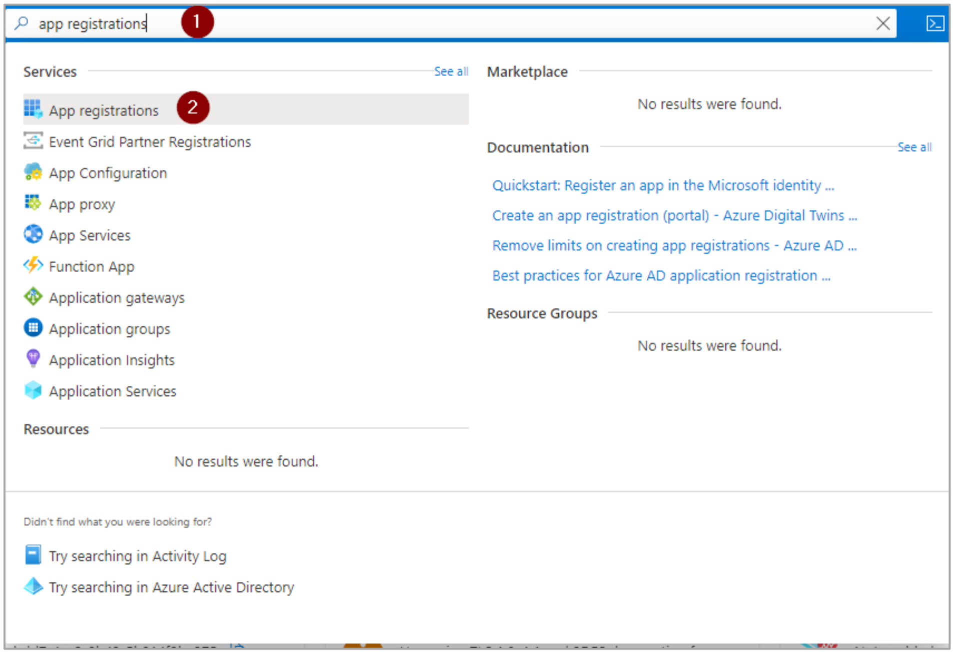
1. Type is Azure Active Directory
2. Name is customer’s choice, an example would be Azure AD
3. Tenant ID
4. Client ID
5. Client Secret
6. Group ID – If used to sync specific group
7. Disable syncing of Group Accounts – client can enable if desired



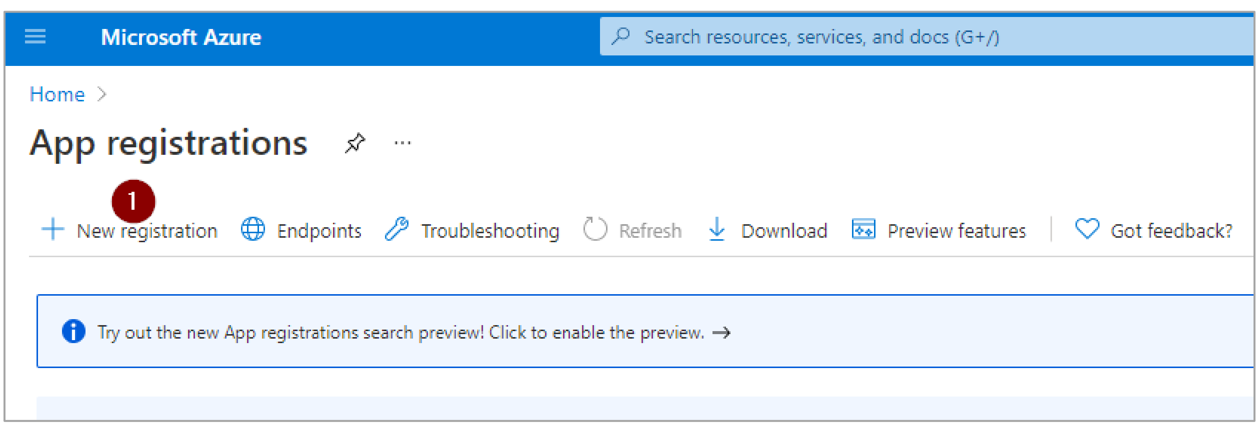
Create App Registration in Microsoft Azure console

Create App Registration

Go to portal.azure.com and login with your credentials. Use the search bar at the top of the screen to search for App Registrations (1) then click on App Registrations under Services (2)

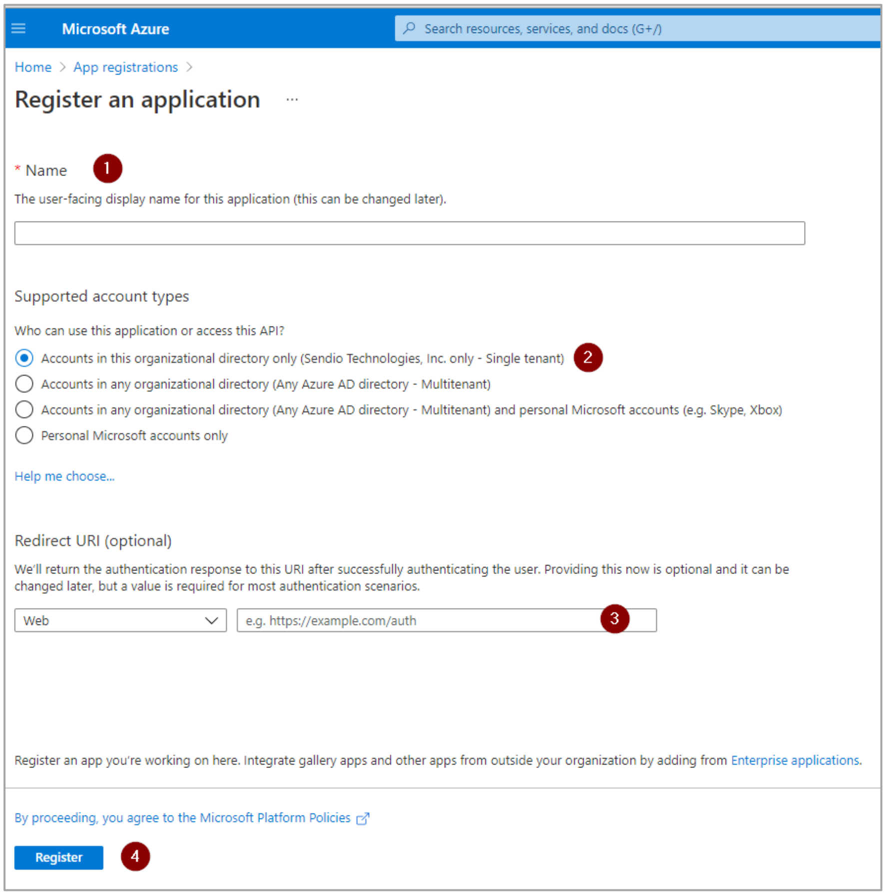


1. Click New Registration in menu bar



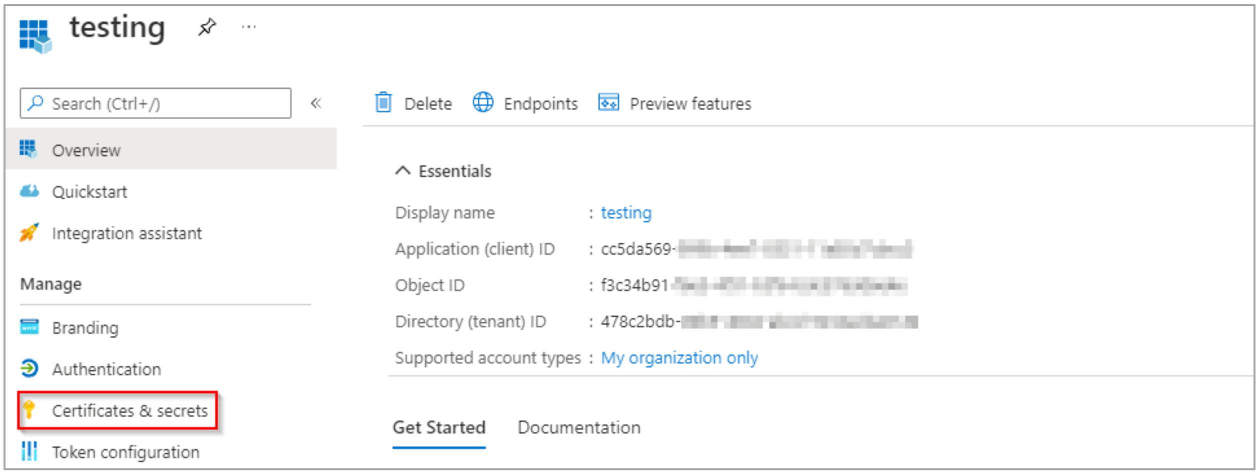
Register an application screen

1. Set name to Sendio
2. Supported Account types is: Accounts in this organization directory only
3. Redirect URL - https://<sendio-hostname>/sendio/ice/cmd/oauth/complete/azuread
4. Click Register

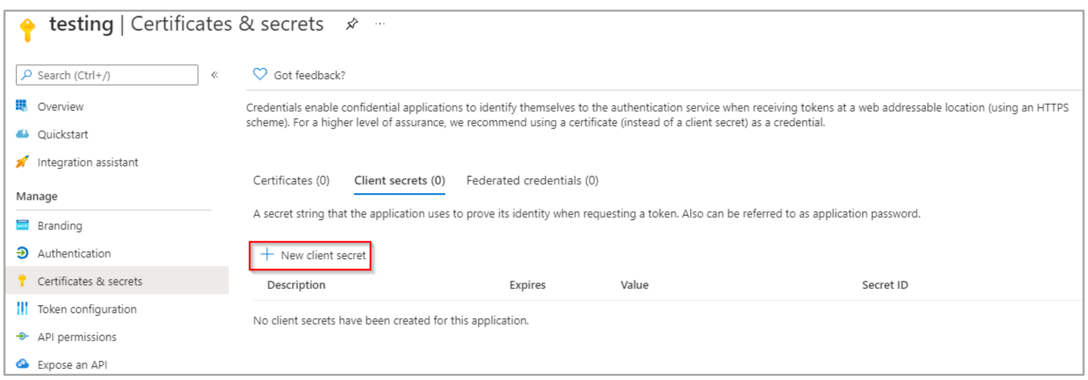


Create a Secret

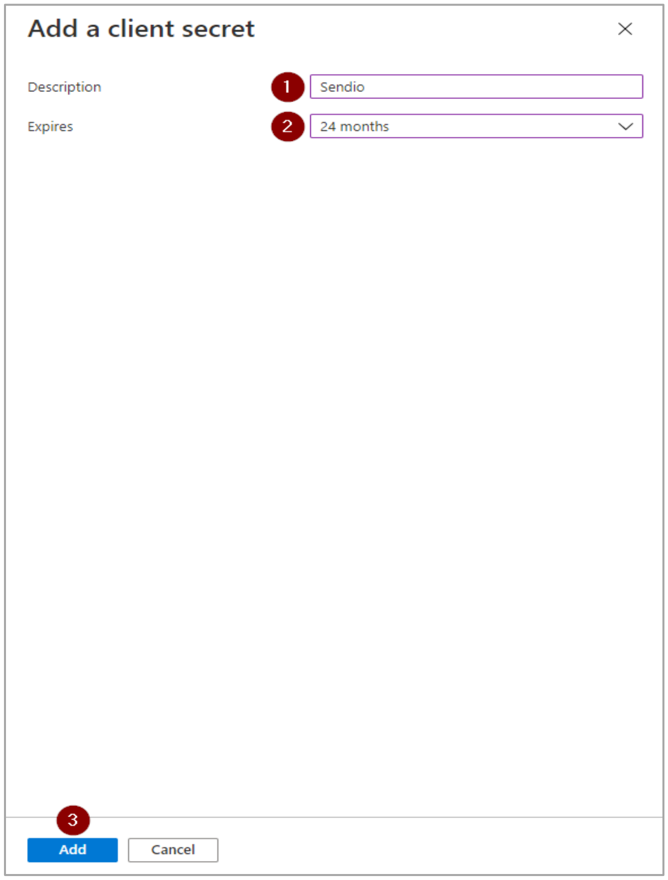
Main menu, click on Certificates & secrets



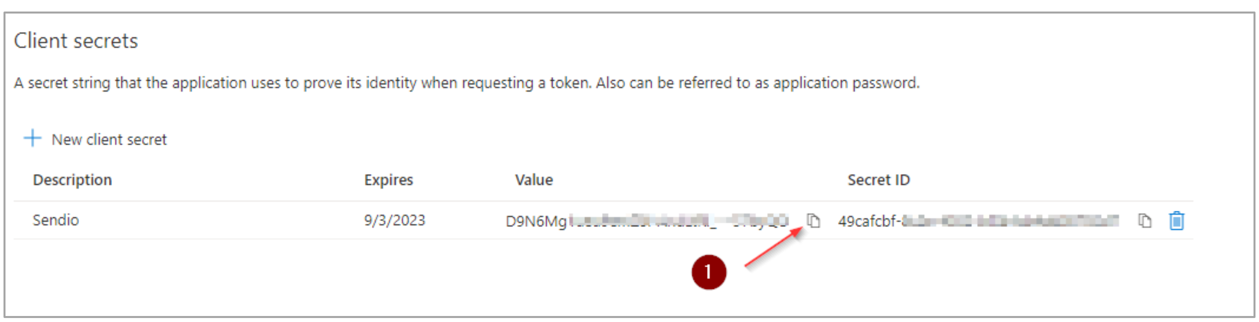
1. Under Client Secrets, click New client secret



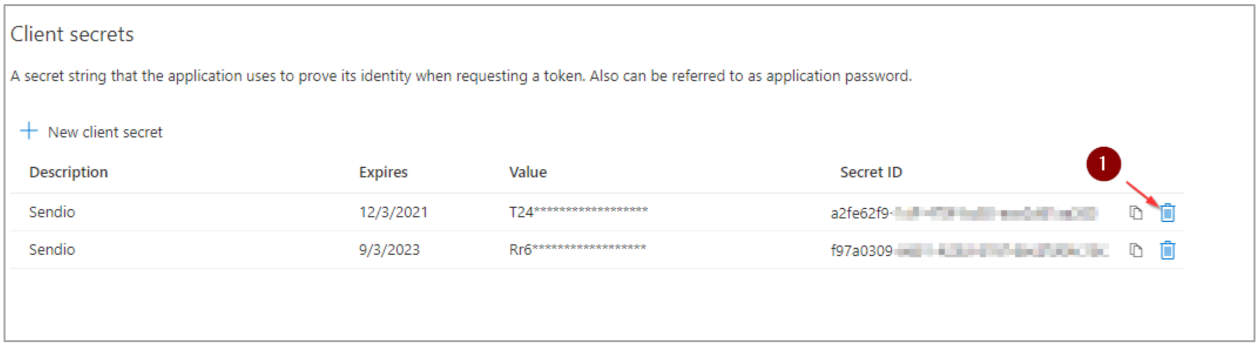
1. Description is Sendio
2. Expires – Select 24 months, maximum. ***Customer will need to update every year or lose access***
3. Click Add



1. Copy new Value immediately to the clipboard, paste into Client Secret field in Sendio UI Directory setup.



When replacing your Client Secret, repeat the steps to create a secret (above) then delete the old/expiring secret using the trash can icon

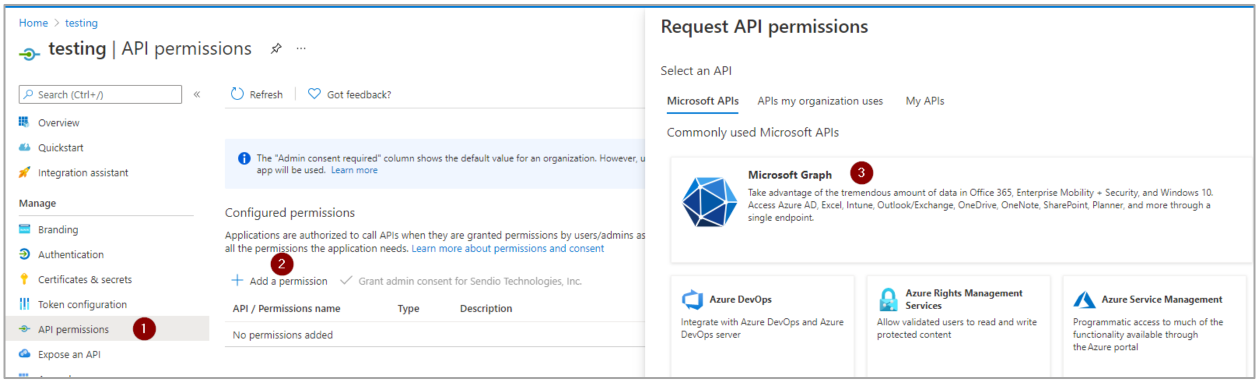


Add API Permissions

You will need to add read permissions to allow Directory sync in Sendio.

Click on API Permissions

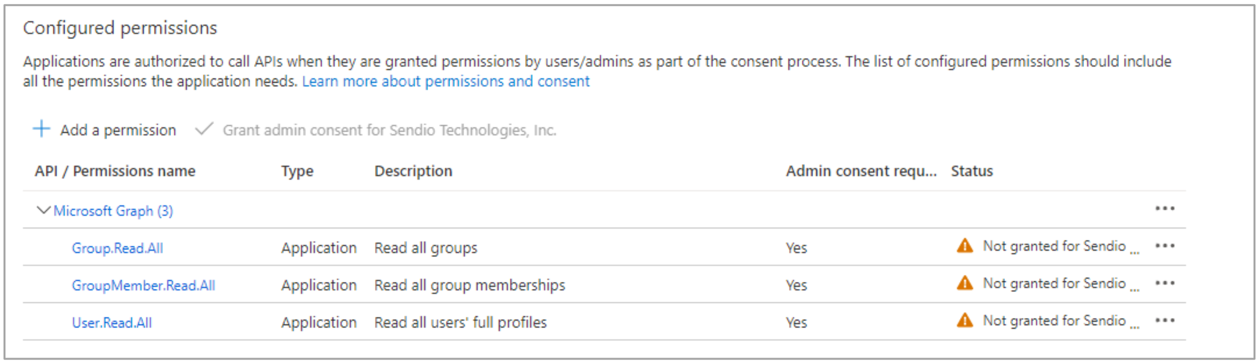
1. Click Add a permission
2. Click on the Microsoft Graph box



When adding permissions, you will need to add each one individually. Once you have added a permission, you will be returned the main API Permissions screen, you will need to click the Add a permission link, then on the Microsoft Graph box, then Application Permissions each time to add a permission.

1. Click Application permissions
2. In search bar, type user.read.all. Click the ">" next to User to expand the field
3. Check the box for User.Read.All, click Add Permission at the bottom of the screen
4. In search bar, type group.read. Click the ">" next to Group to expand the field
5. Check the box for Group.Read.All. click Add Permission at the bottom of the screen
6. In the search bar, type groupmember. Click the ">" next to GroupMember to expand the field
7. Check the box for GroupMember.Read.All, click Add permission at the bottom of the screen

This will return you to the Configured Permissions screen. Click Grant Admin consent for (name). These permissions operate at an admin level.



It will take a few minutes for these settings to propagate through Microsoft's infrastructure.

Record directory info for Sendio

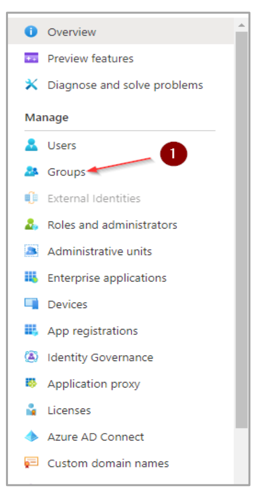
1. Click on Overview in menu
2. Copy Directory (tenant) ID and paste into Tenant ID field in Directory setup in Sendio UI
3. Copy Application (client) ID and paste into Client ID field in Directory setup in Sendio UI

Optionally, you can include a Group ID to only sync users belonging to a specific group.

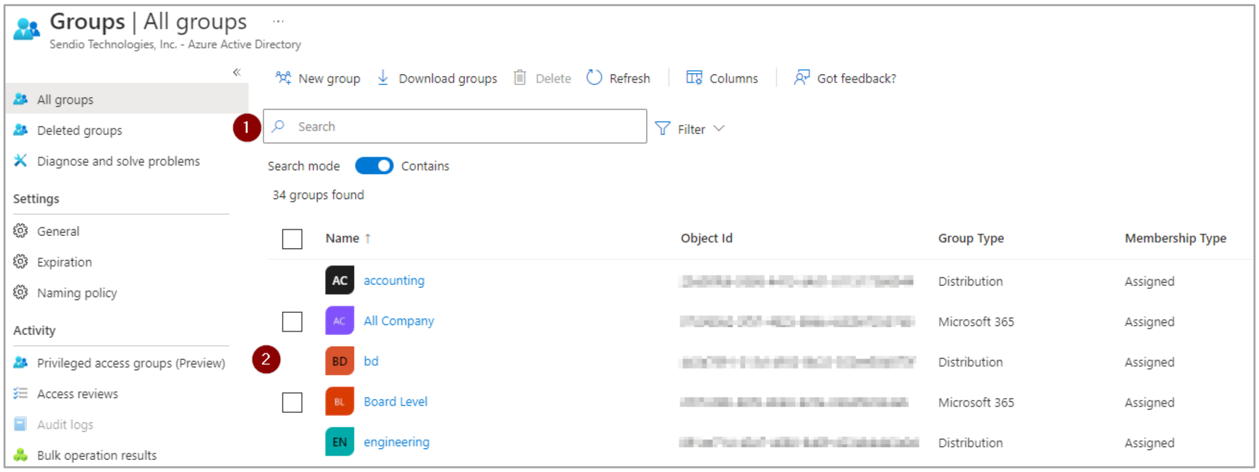
Once this configuration is complete, Click Save on Directory window in Sendio UI to save the new Directory setup. Click Sync to sync this new directory. Sync will add all user and group accounts contained within the directory to Sendio. Sendio also allows you to disable syncing of group accounts should you choose to.

Syncing a Specific Group from Azure

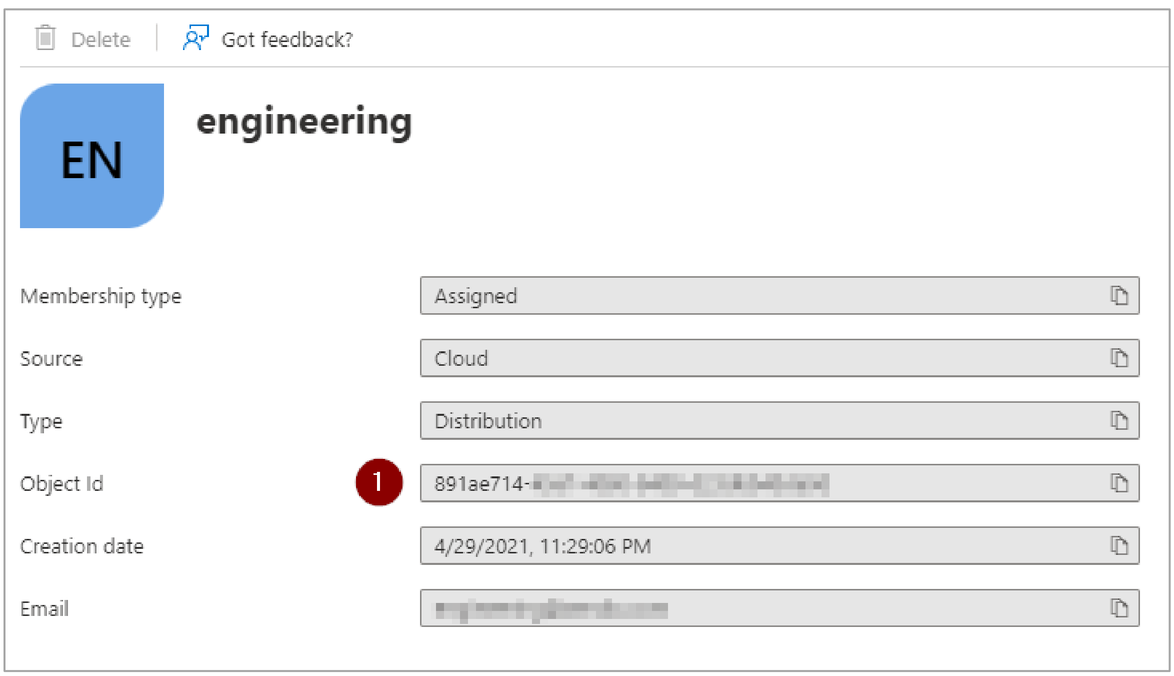
To sync users belonging to a specific group instead of the entire Azure Active Directory you will need to find the group's specific Object ID. This Object ID will be entered into the Group Id field in the Sendio UI directory setup. Login to portal.azure.com. On the Overview screen, click on Groups under Manage



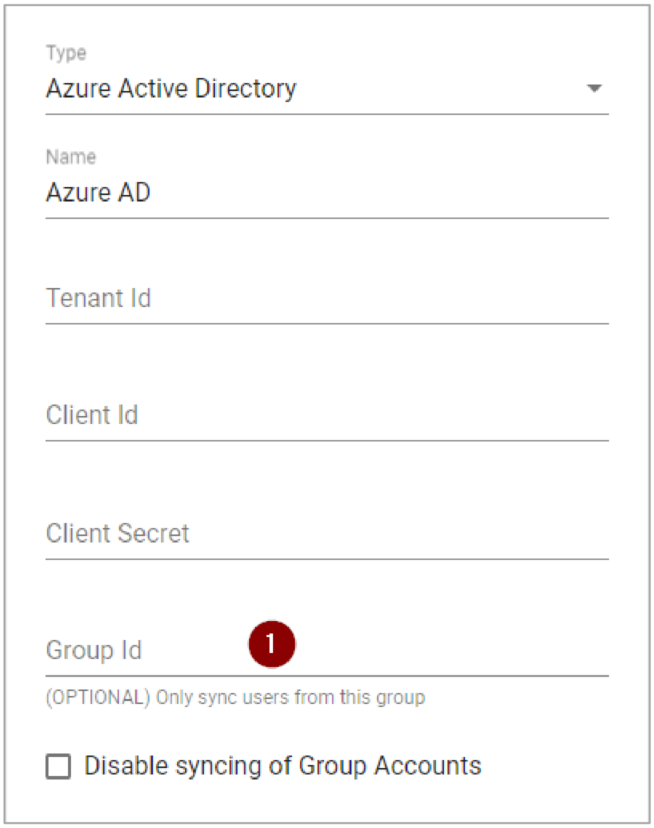
On the Groups screen, you can search for a specific Group using the Search Bar (1) or scroll through your list of Groups to find the specific Group to sync (2)



To get the Group ID for Sendio, click on the specific group you want, and it will open a new window. In this window, you will copy the Object ID for use in the Directory screen of the Sendio web UI.



Next, you will paste the Group's Object ID into the Sendio directory Group ID in the Directory window for your Azure Active Directory Sendio directory



This will allow you to sync users belonging to a specific group into Sendio. If you need to sync multiple groups of users instead of the entire directory, you will need to create separate Directories in Sendio, each one syncing a specific group. Syncing a specific group will add all users contained within the specific group to Sendio. Nested groups within the specified group will not be synced.

Disable Syncing of Group Accounts

Admins can disable syncing of group accounts by checking "Disable syncing of Group Accounts". Enabling this setting will cause only user accounts to be added to Sendio. Groups will not be added to Sendio.

Known Issues

1. Duplicate accounts may be created when syncing Azure AD in Sendio. Sendio Support can merge duplicate accounts if needed.
2. Local password for Accounts synced from Azure AD is not supported.