Creating and Configuring an Azure Active Directory System of Record

Prerequisites

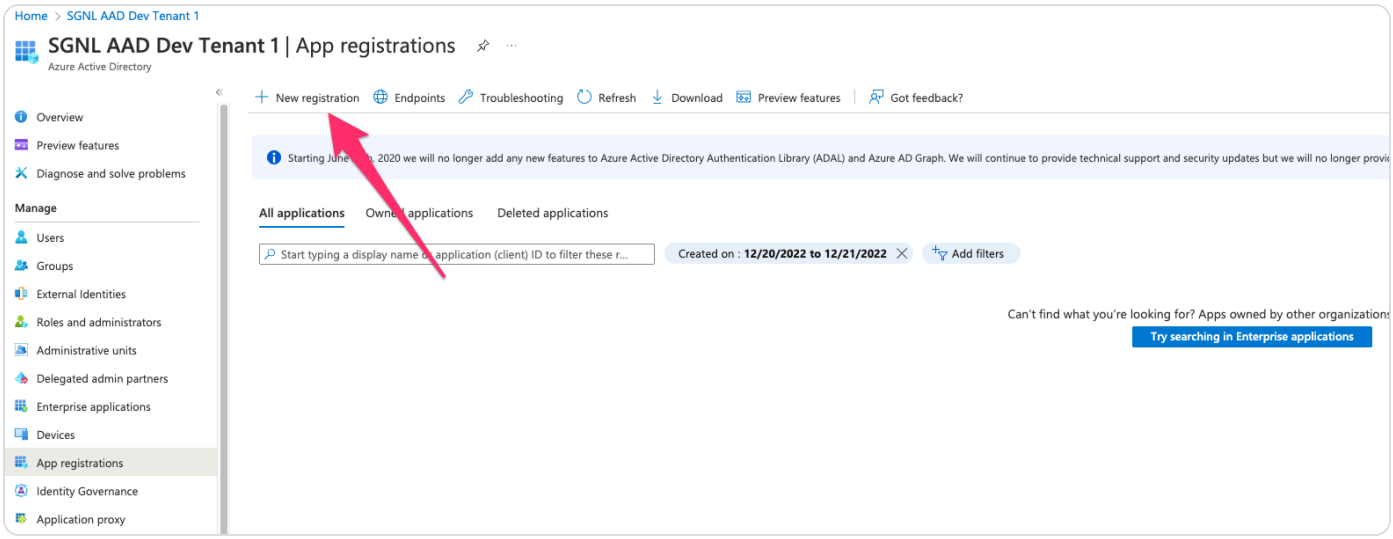
- Azure AD Account with Administrative privileges to Register Apps and Consent to User/Group Read Access in the Microsoft Graph
- SGNL User Account with Admin privileges

Permissions Required

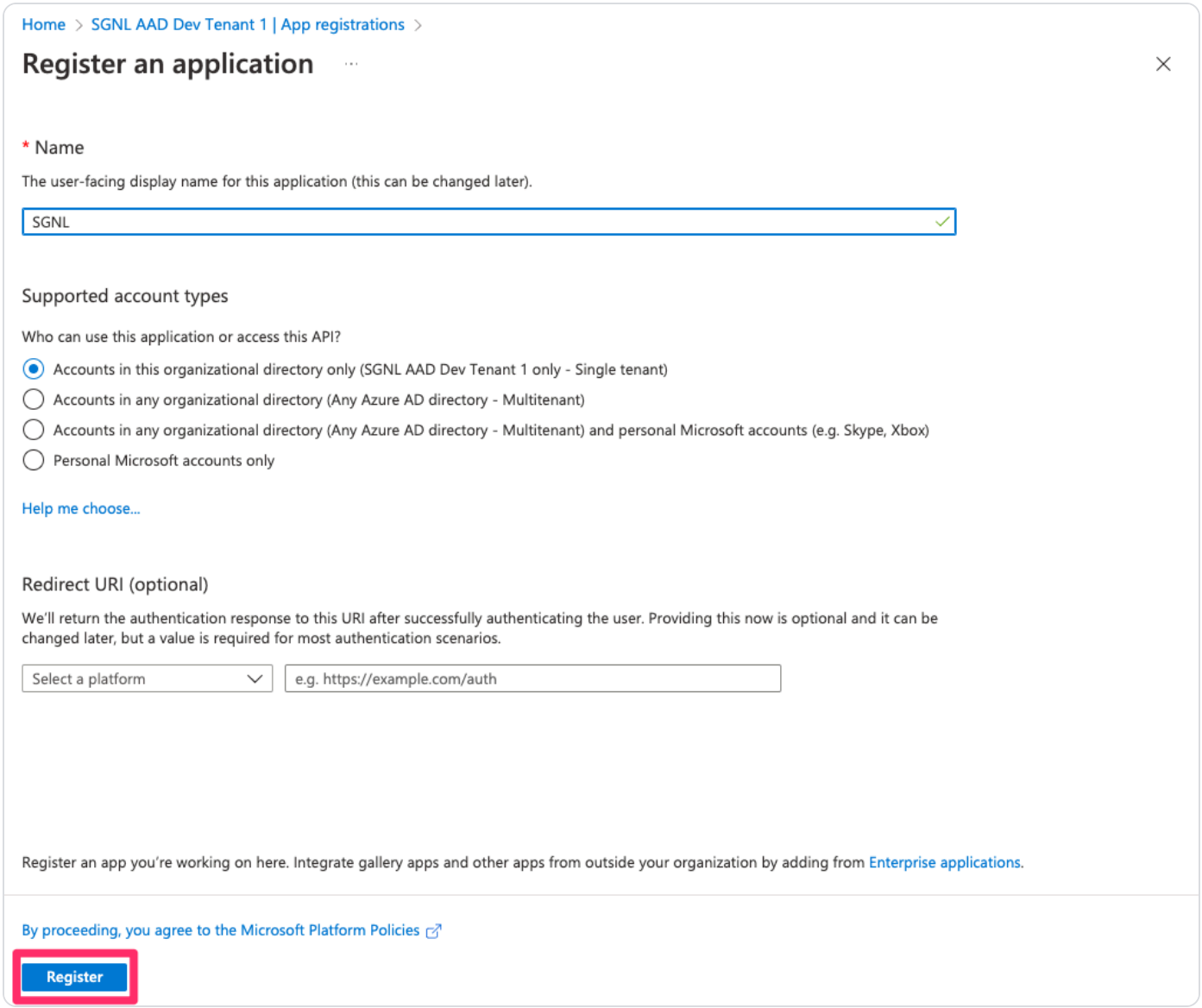
- SGNL firmly believes in the principle of least privilege, as such - only the access required to achieve your authorization use-cases should be granted.
- SGNL requires an App to be registered in the Azure AD Tenant to be synchronized that has read permissions. Depending on the objects needing to be synchronized, these permissions will vary:
  - **Users:** Requires the User.Read.All Permission (see below for configuration)
  - **Groups:** Requires the Group.Read.All Permission (see below for configuration)
  - **Applications:** Requires the Application.Read.All Permission (see below for configuration)
  - **Devices:** Requires the Device.Read.All Permission (see below for configuration)

Configuring Azure AD

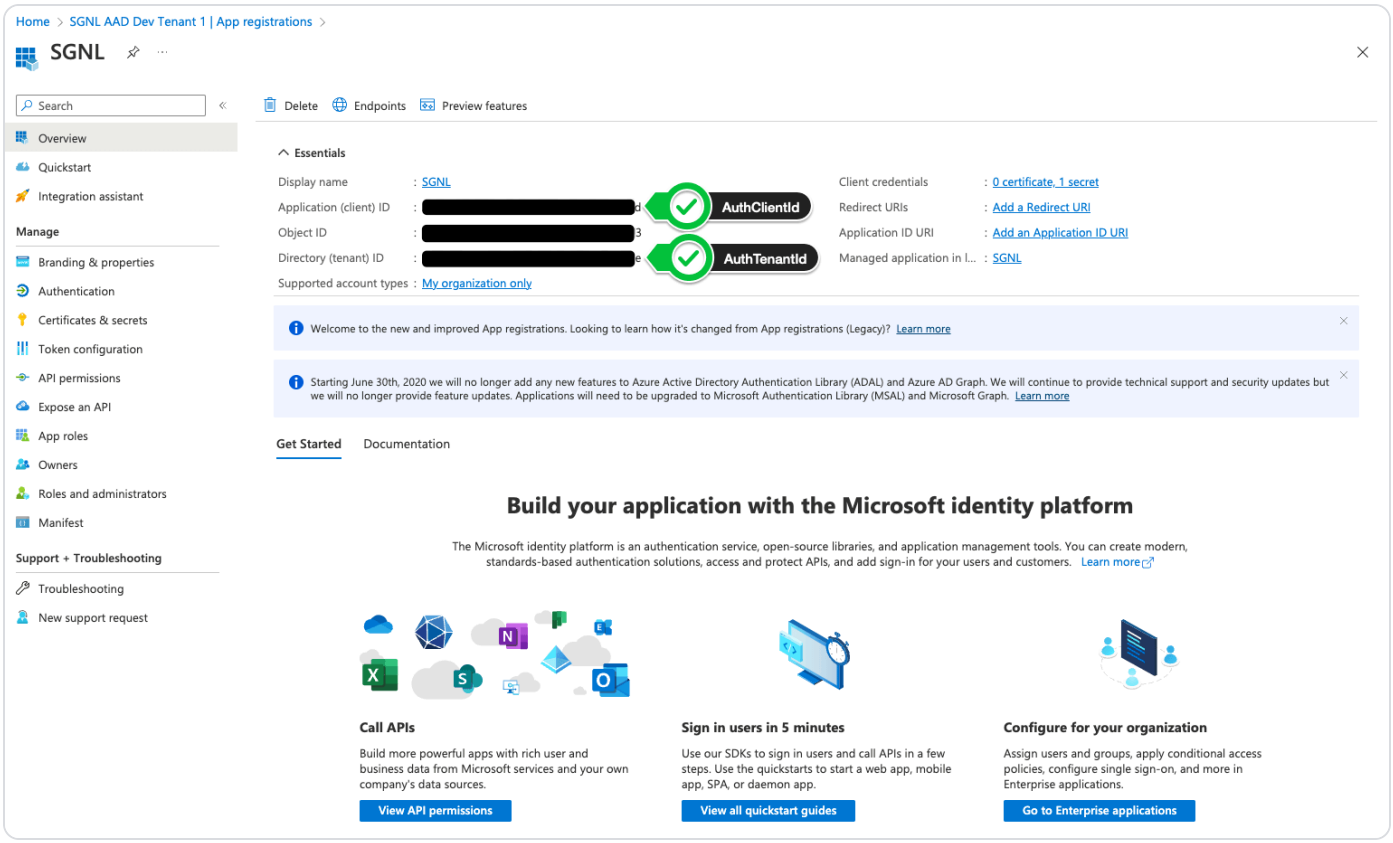
1. Login to the Microsoft Azure Portal and launch the Azure AD Console
2. From the left navigation pane, select App Registrations
3. Create a New Registration



4. Specify a Name for the App and choose Register

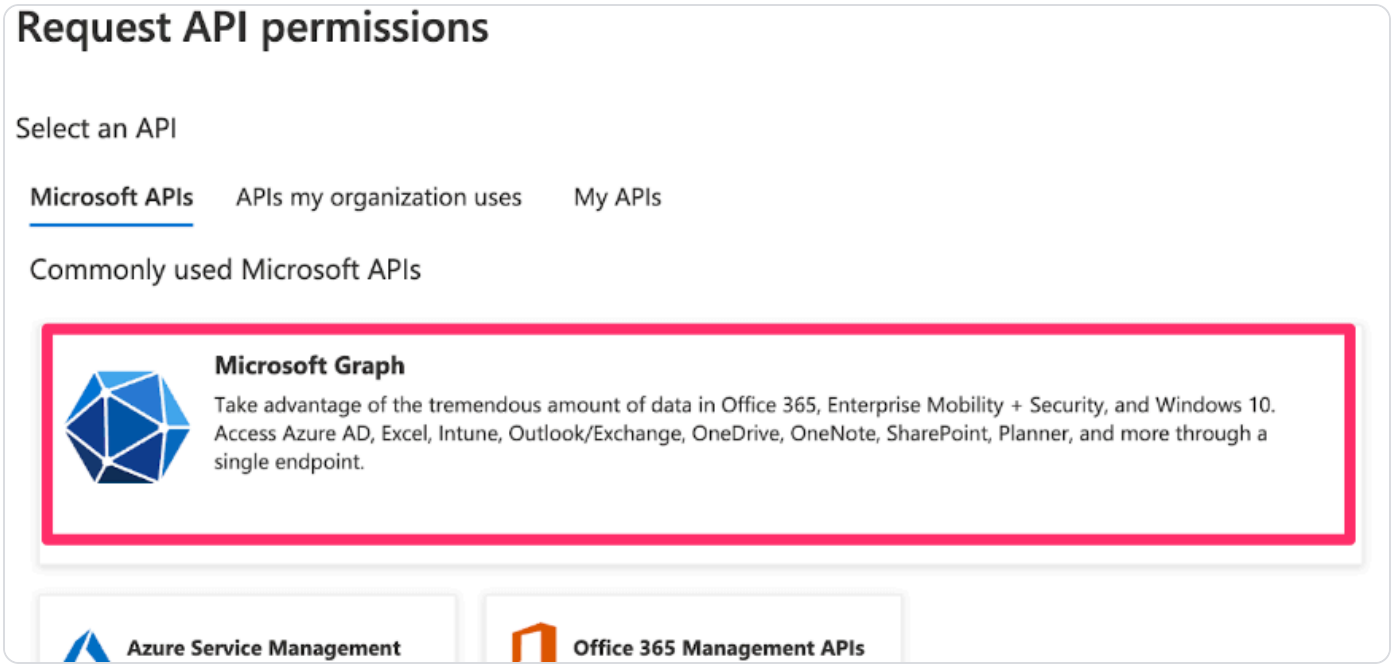


5. Within the App Registration, note the:
    - Application (client) Id (**SGNL:** AuthClientId)
    - Directory (tenant) Id (**SGNL:** AuthTenantId)

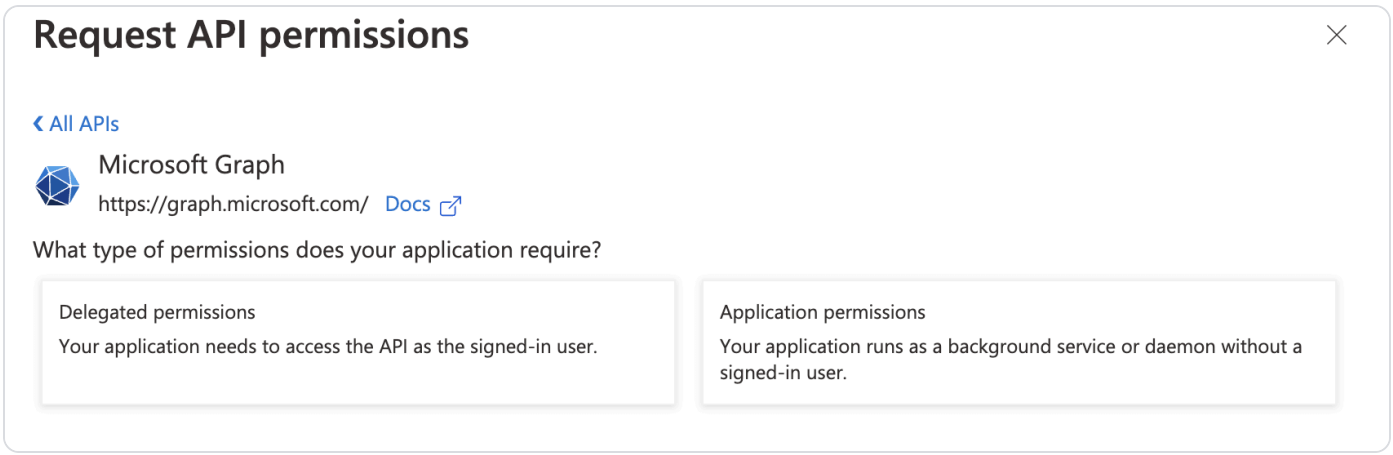


6. From the API permissions page in the left menu, choose to Add a permission

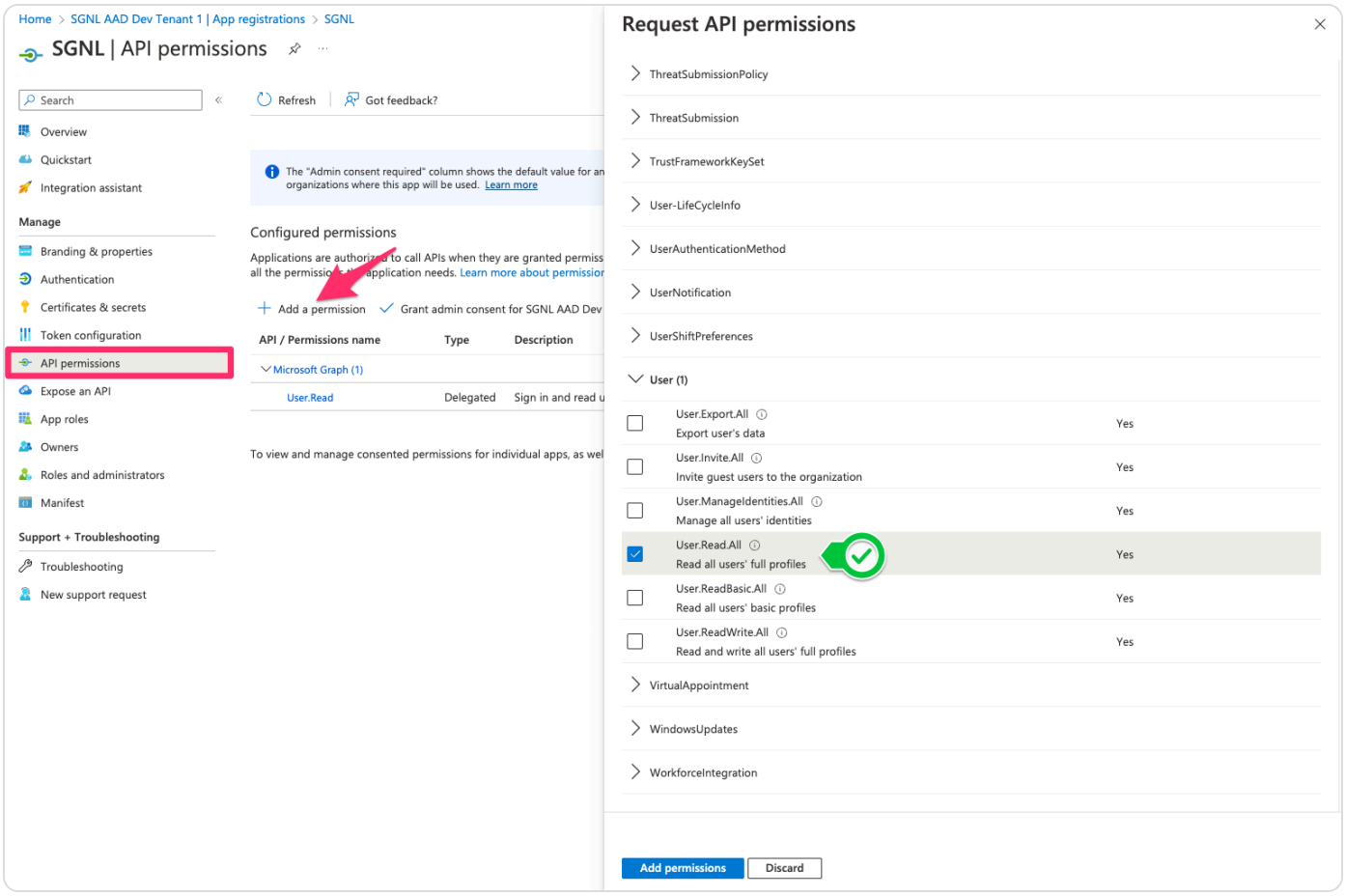
7. Select Microsoft Graph



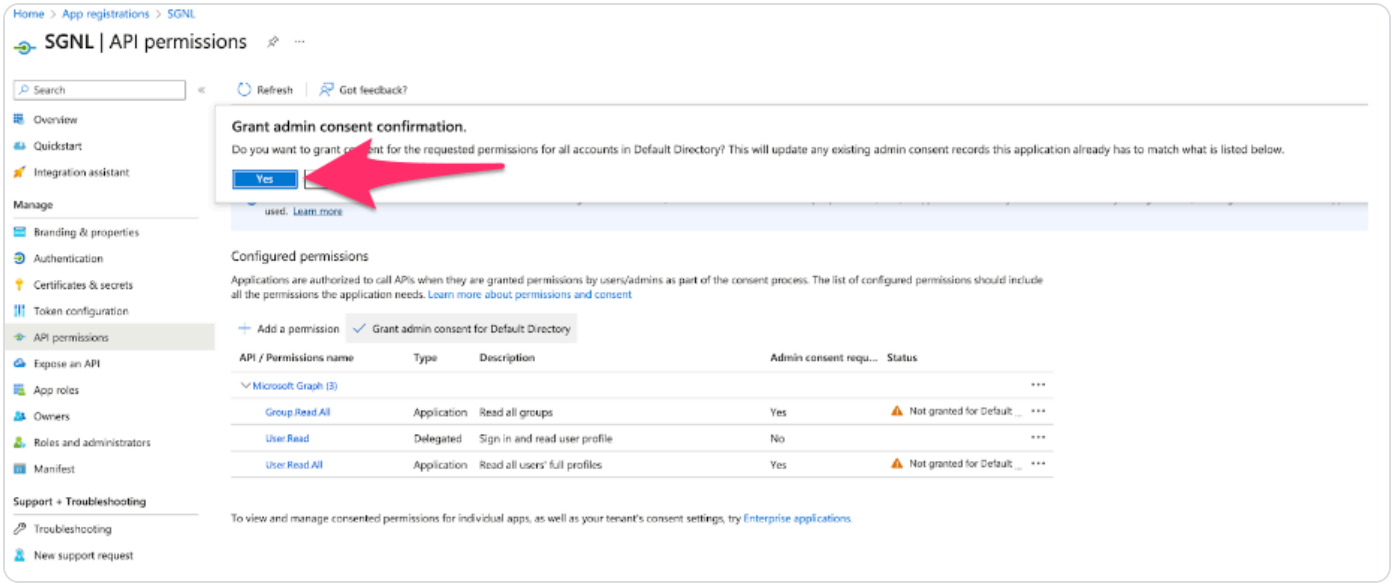
8. Select “Application Permissions”



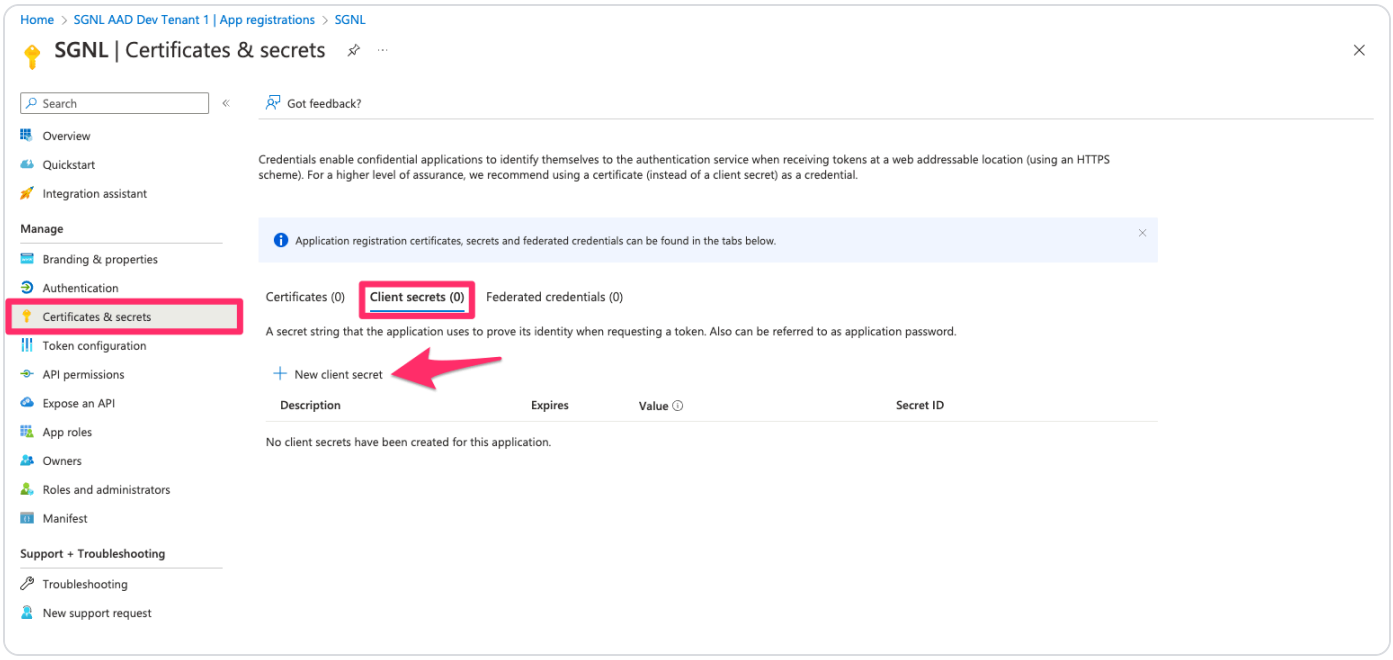
9. Select the below and Add permissions:
    - User.Read.All
    - Group.Read.All
    - Application.Read.All
    - Device.Read.All



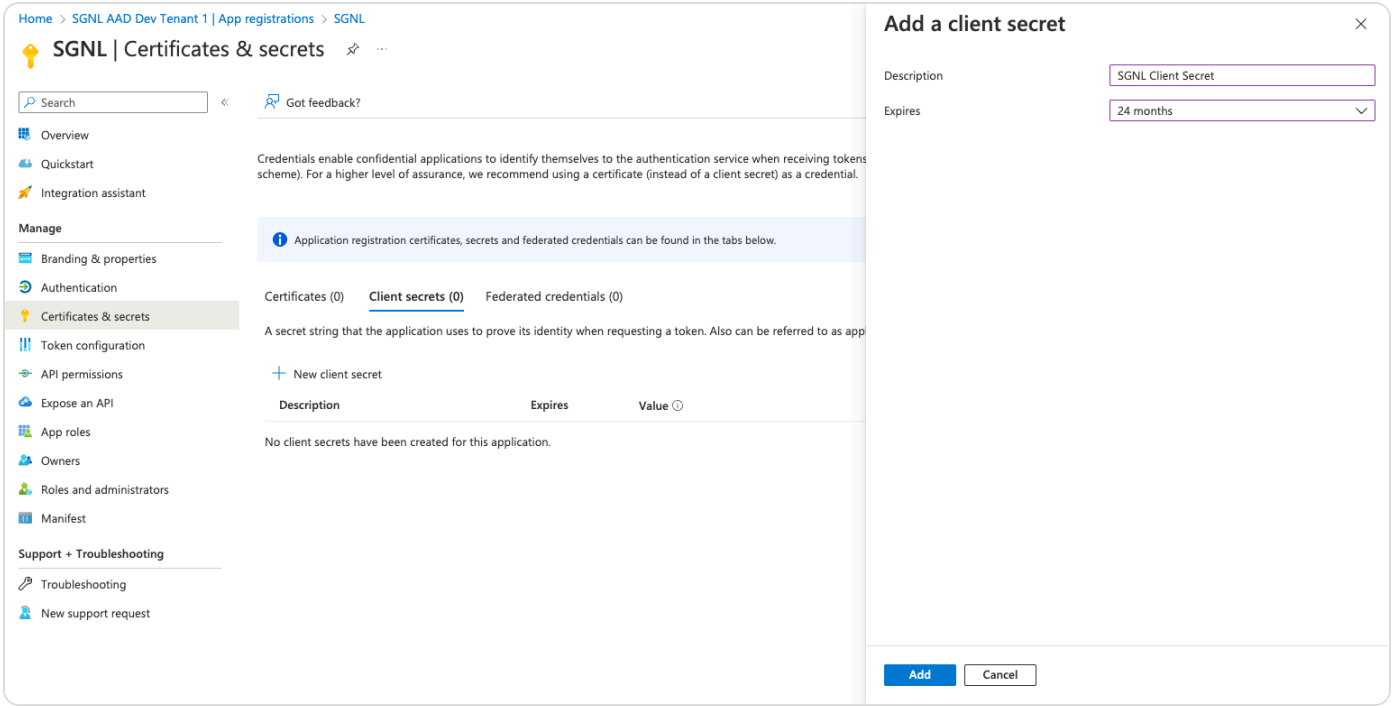
10. If asked to do so, grant “admin consent”



11. Select Certificates and Secrets from the left menu, select Client secrets, and + New Client Secret



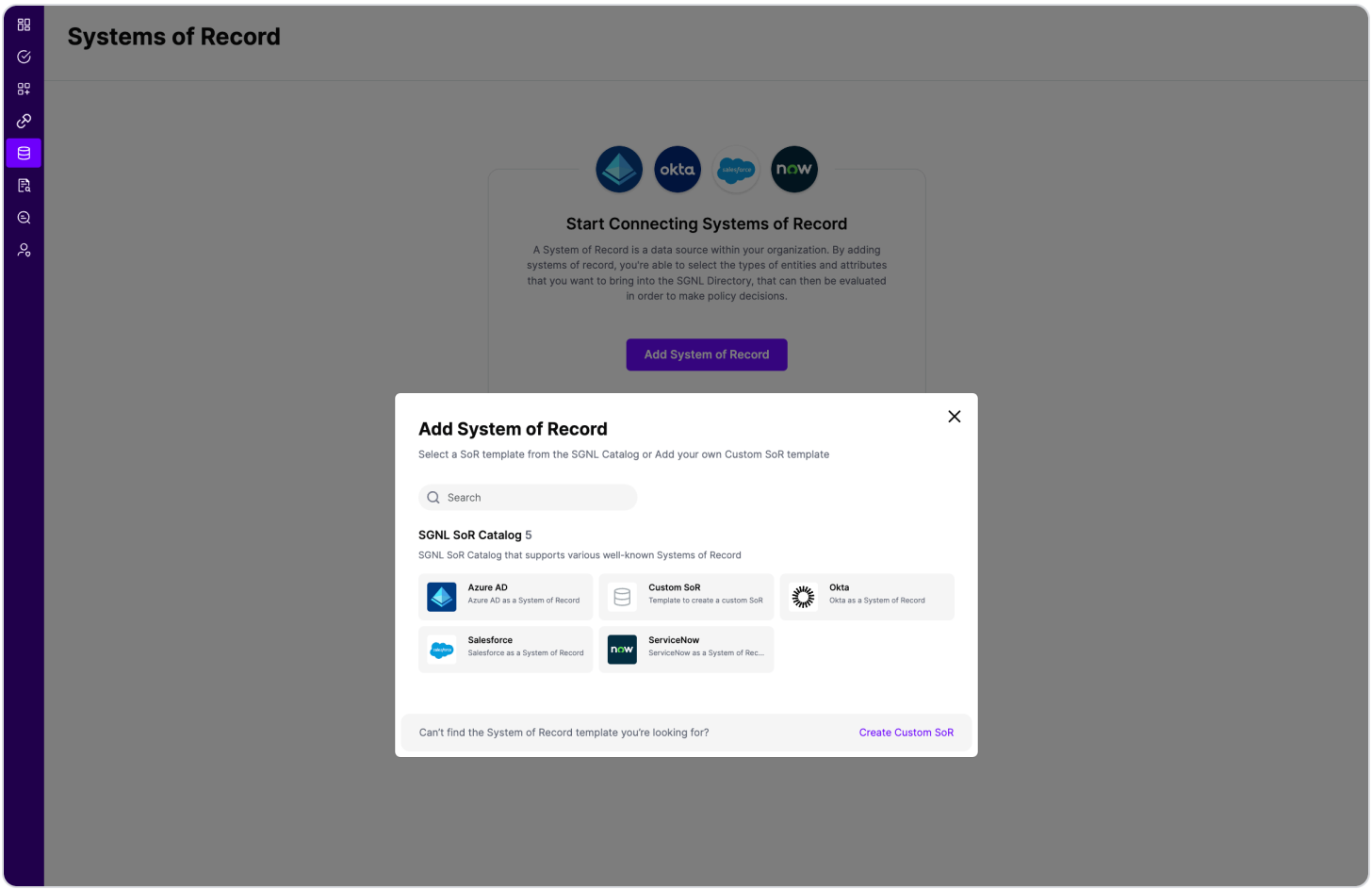
12. Give the secret a description and expiry (the length of time until a new secret will need to be generated for SGNL to communicate with Azure AD), and select Add



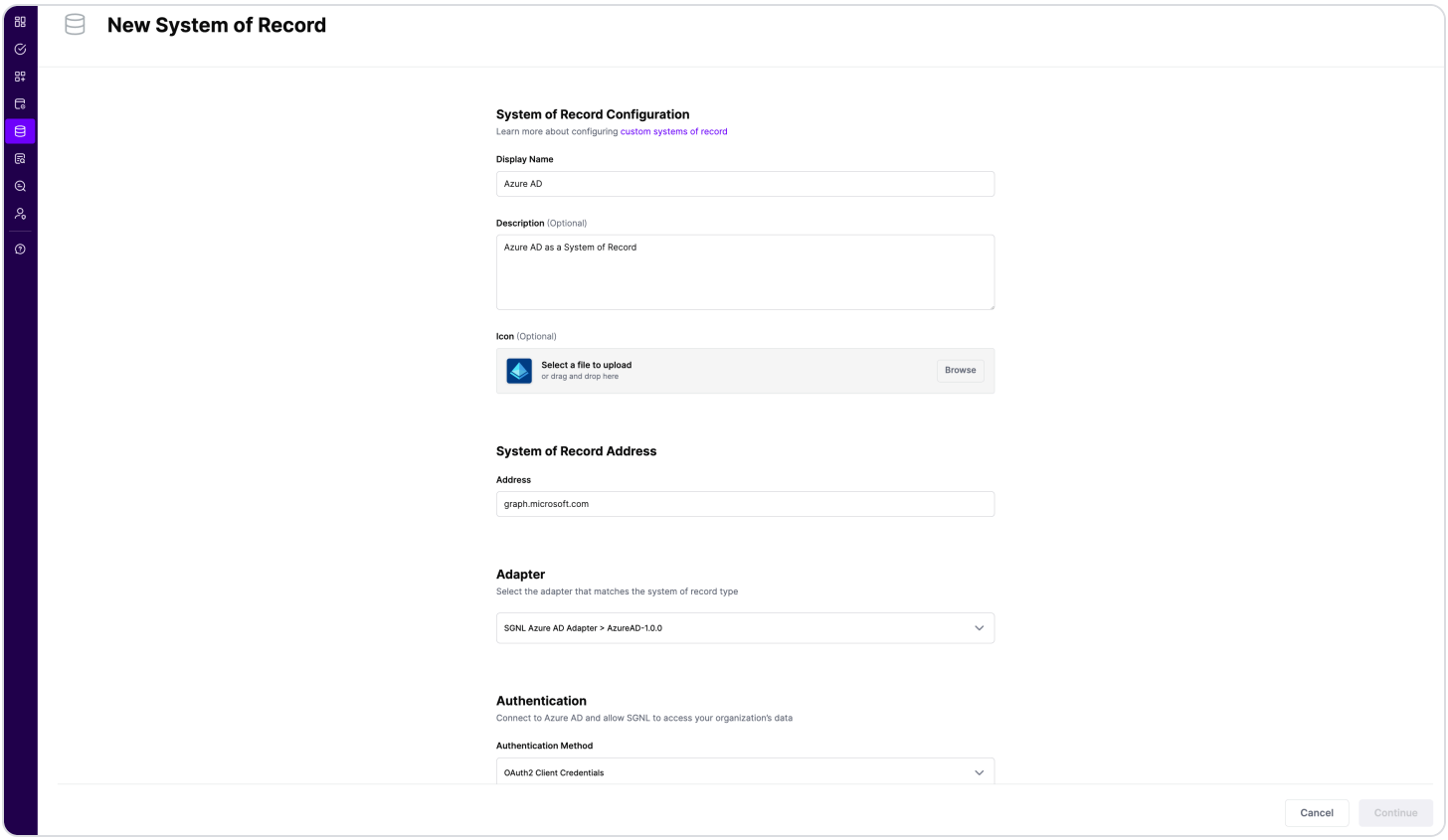
13. Copy the Value of the secret, this will be required for the SGNL Console (**SGNL:** AuthClientSecret)

Configuring SGNL

1. Login to the SGNL Console
2. From the left menu, select Systems of Record
3. Click “Add System of Record” or “Add”.
4. The SGNL SoR Catalog will show up on the screen.



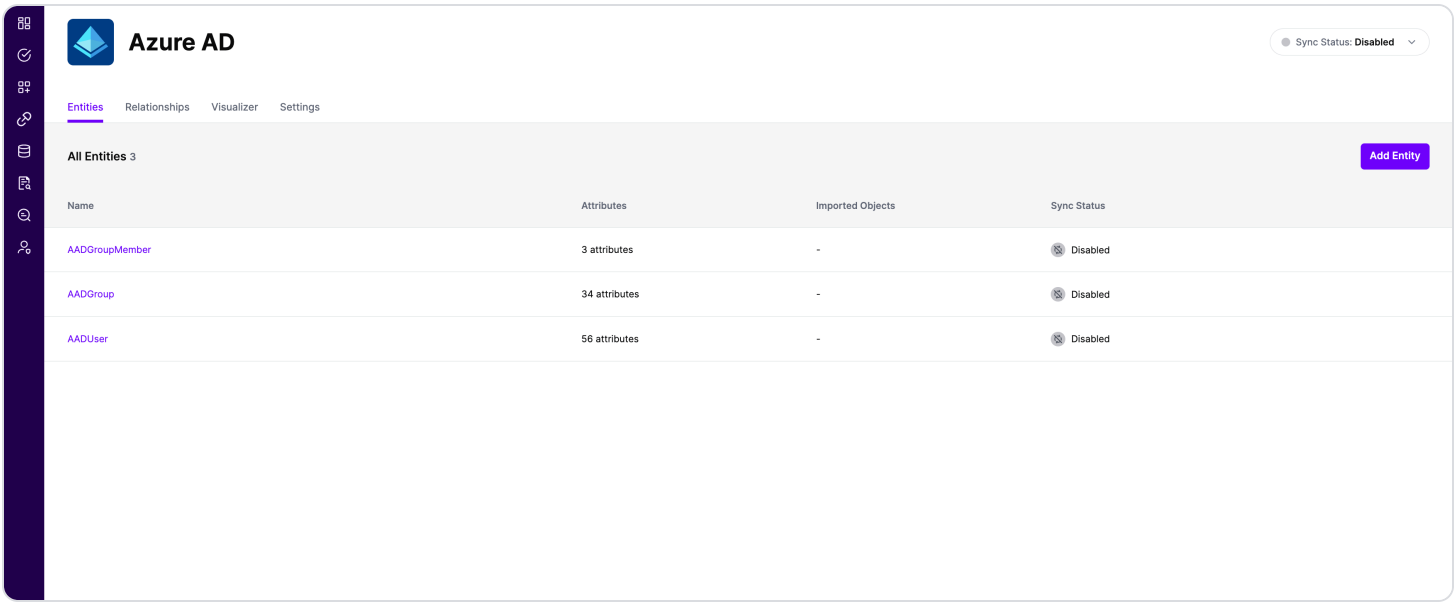
5. Click on “Azure AD” which will open up the New System of Record screen with some configuration options pre-populated from the Azure AD SoR template.



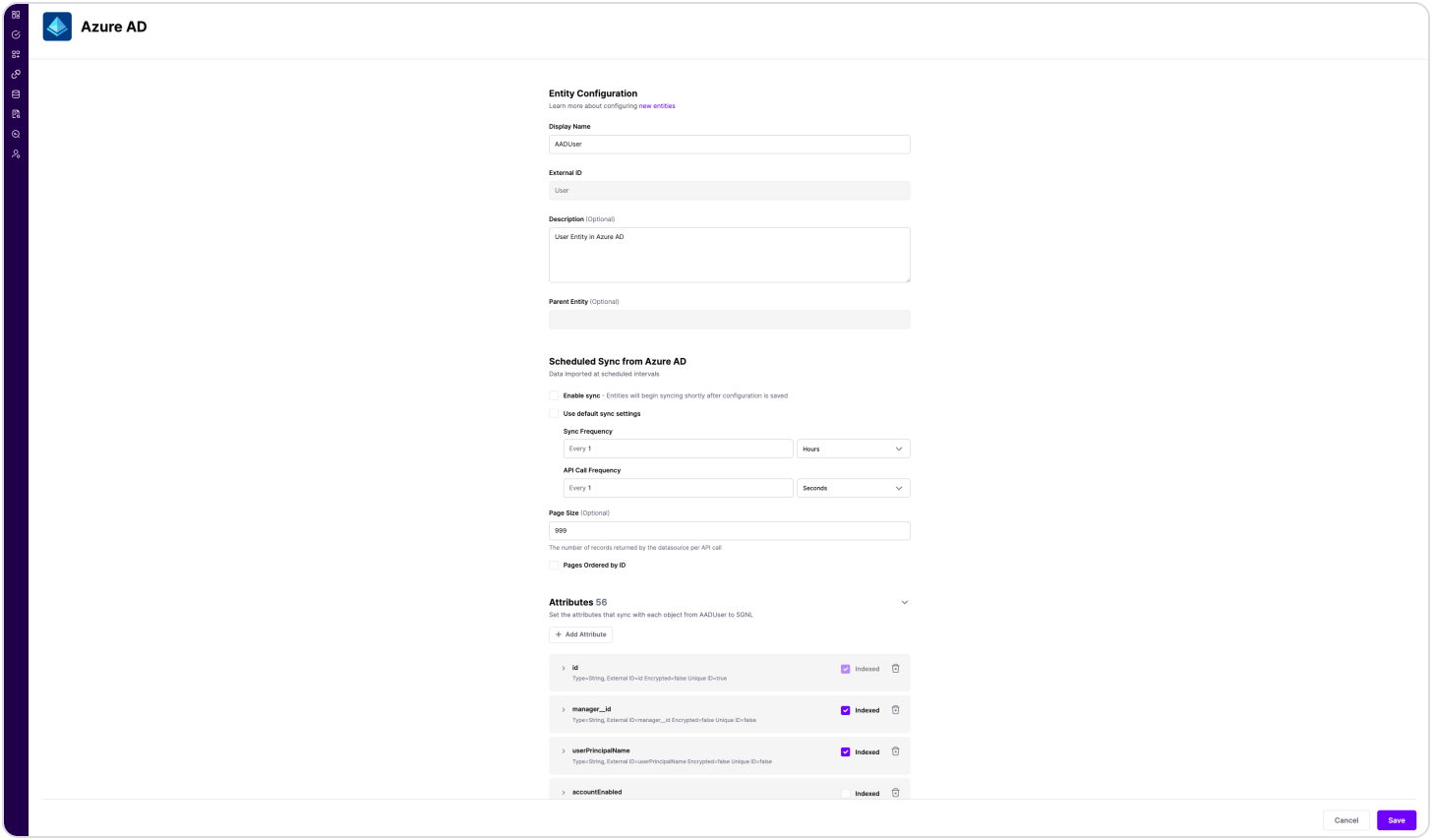
6. Choose the correct adapter that matches the AzureAD System of Record Type.
7. Replace all fields that have the {{Input Required:}} placeholder with relevant information. For Azure AD, the following fields are required:

- **Client ID**: The Application (Client) ID you copied from Azure AD
- **Client Secret**: The Client Secret value you copied from Azure AD
- **Tenant ID in the Token URL**: The Directory (tenant) ID you copied from Azure AD

8. Click “Continue” to save your Azure AD System of Record. You will be taken to Azure AD System of Record page.



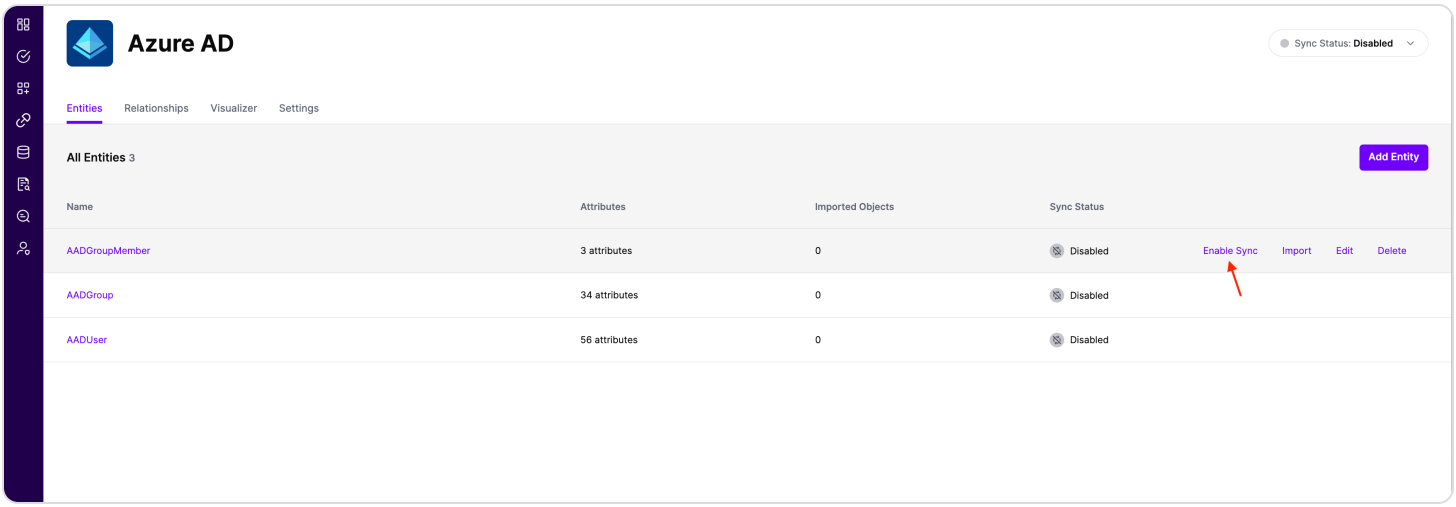
8. All entities and relationships are created as defined in the Azure AD template. If applicable, you can edit an entity and modify any properties of the entity or the associated attributes. Hover over the entity on the screen above to see the Edit button as shown below:



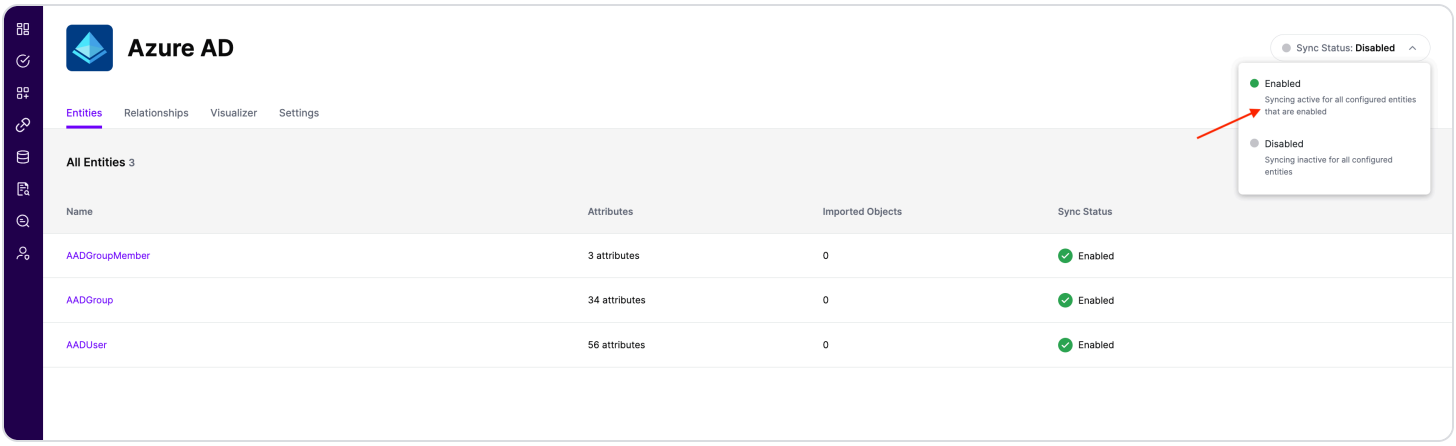
9. You can check the relationships created through the Relationships tab. However, relationships cannot be modified. You will need to delete an existing one, and create a new relationship.
10. (If applicable) You can also create relationships joining entities and attributes in Azure AD to entities and attributes in other Systems of Record configured in SGNL. For example, if User Employee IDs in your Azure AD are consistent with the Employee IDs in your HRIS system, you

can create a relationship between the Employee ID attribute in Azure AD instance and the Employee ID attribute in your HRIS System of Record. For more information on relationships, please refer to our Help Page.

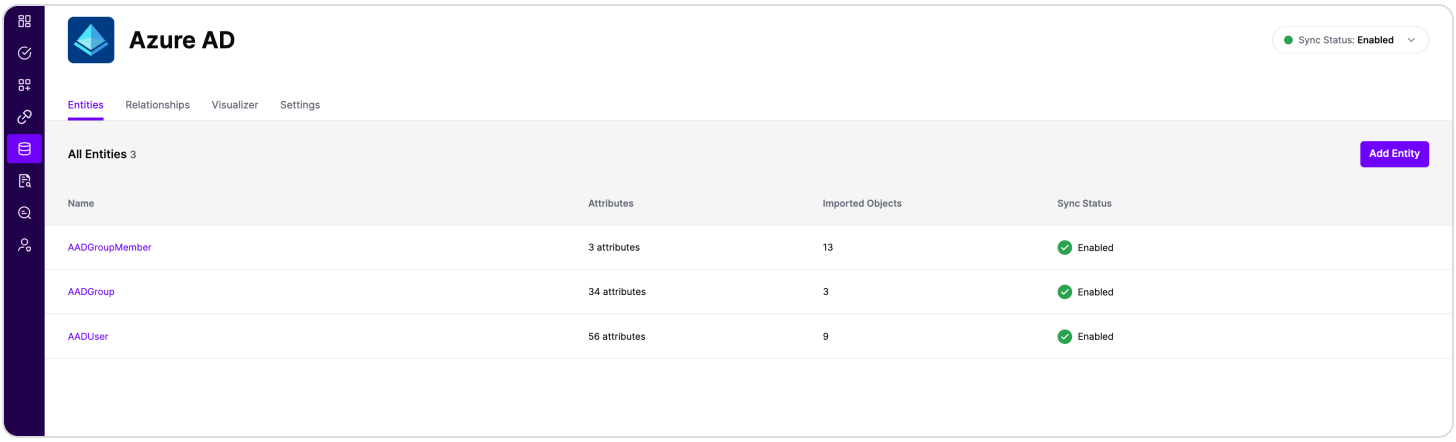
11. Note that synchronization is disabled by default when a new System of Record is created. You can choose to enable synchronization on Entities individually. Hover over the entity to see the Enable Sync button, and click on it.



12. Repeat for all Entities you want to synchronize to SGNL. Finally, Enable synchronization for the System of Record.



13. After some time, SGNL should complete ingesting the data from your Azure AD instance into the SGNL graph. The number of objects ingested per entity are displayed on the Azure AD screen. You should then be able to construct policies based on your Azure AD data and make access evaluation calls to SGNL.



14. Once ingestion is complete and Azure AD data is in the SGNL graph, you can use Data Lens to explore the SGNL graph.