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

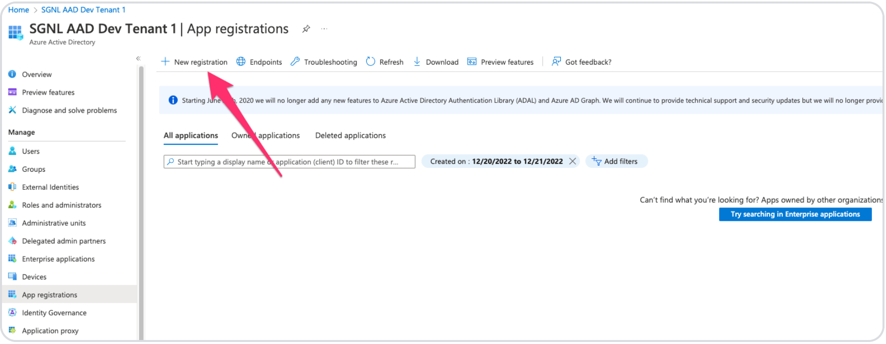
Permissions Required

- 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)

Protected Systems

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



Home > SGNL AAD Dev Tenant 1

SGNL AAD Dev Tenant 1 | App registrations

Azure Active Directory

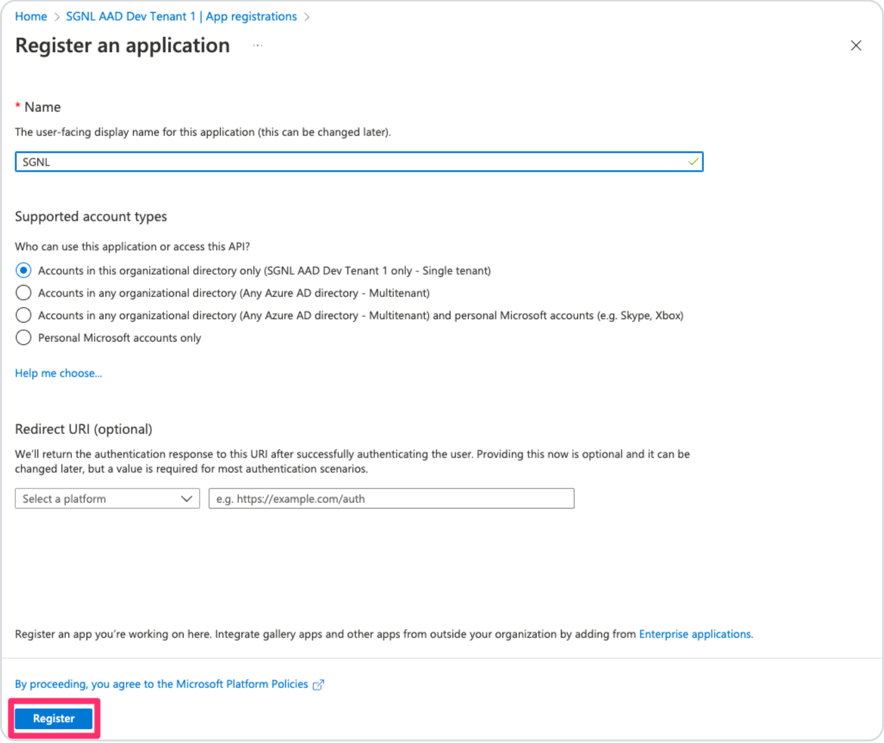
Starting June ., 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provi

Start typing a display name or application (client) ID to filter these r...

Created on : **12/20/2022 to 12/21/2022**

Can't find what you're looking for? Apps owned by other organization

4. Specify a Name for the App and choose Register



Home > SGNL AAD Dev Tenant 1 | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SGNL

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (SGNL AAD Dev Tenant 1 only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

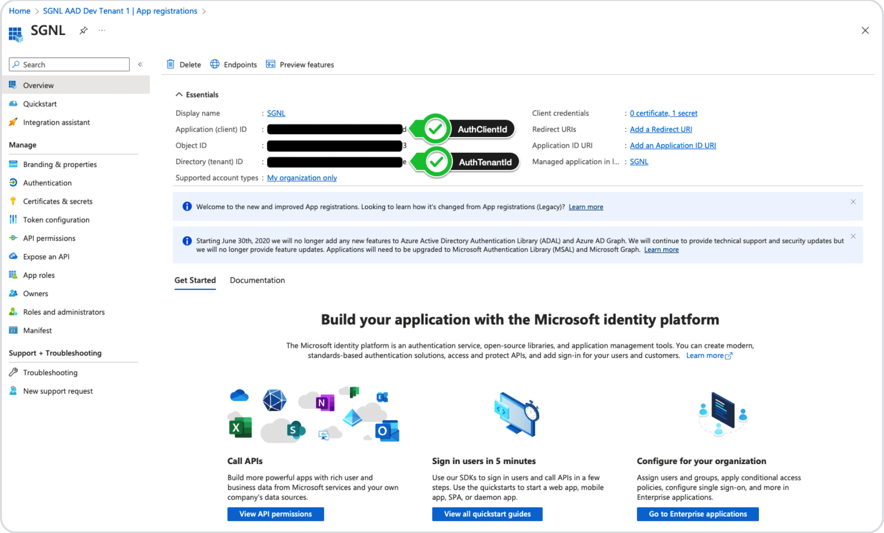
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

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



Display name : SGNL

Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : My organization only

Client credentials : 0 certificate, 1 secret

Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

Managed application in l... : SGNL

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Sign in users in 5 minutes

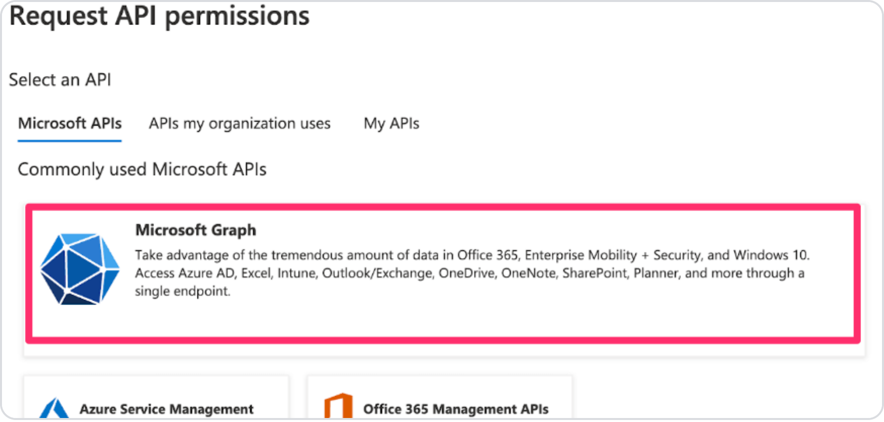
Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

Configure for your organization

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.

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

7. Select Microsoft Graph



Request API permissions

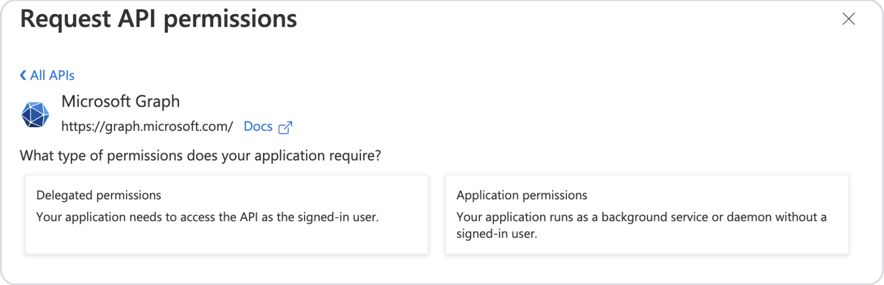
Select an API

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

8. Select “Application Permissions”



Request API permissions

Microsoft Graph

https://graph.microsoft.com/

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

9. Select the below and Add permissions:

- User.Read.All

Policy Management

SGNL Policy Overview

Quickstart: Creating Effective Policies

SGNL Policy Snippet Reference

Integrating Protected Systems with SGNL using Access APIs

Troubleshooting Access Decisions

Administration

Configuring and Managing Labels in SGNL

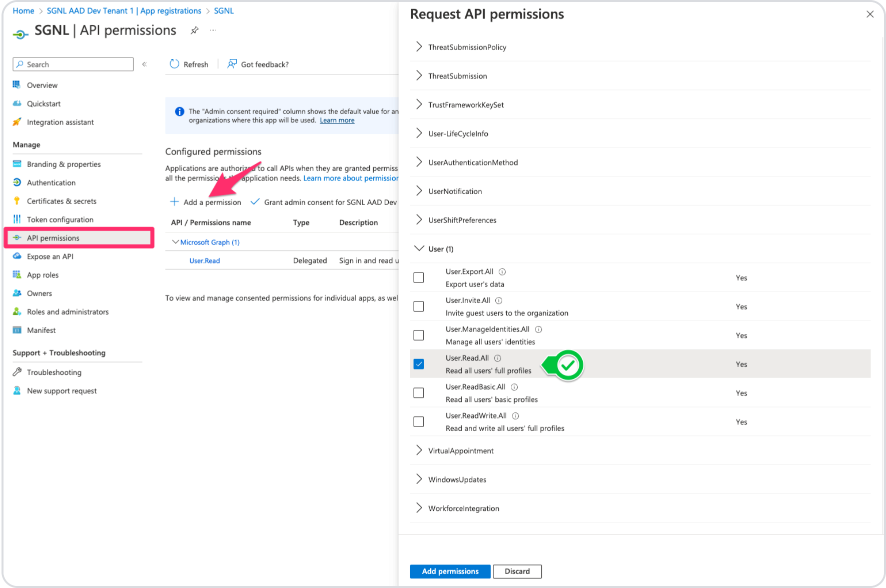
Configuring SGNL for SSO with Google Workspace

Configuring SGNL for SSO with Okta

Configuring SGNL for SSO with OpenID Connect

SGNL Service Availability

- Group.Read.All
- Application.Read.All
- Device.Read.All



The "Admin consent required" column shows the default value for an organizations where this app will be used. Learn more

Configured permissions

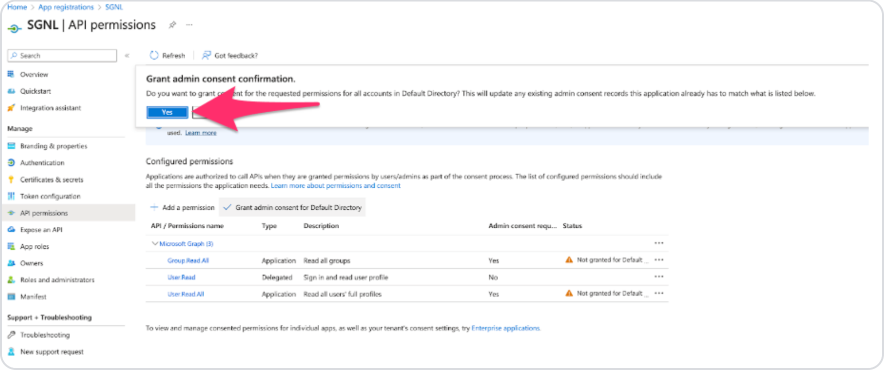
Applications are authorized to call APIs when they are granted permiss all the permissions the application needs. Learn more about permissior

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read u

To view and manage consented permissions for individual apps, as wel

□	User.Export.All Export user's data	Yes
□	User.Invite.All Invite guest users to the organization	Yes
□	User.ManageIdentities.All Manage all users' identities	Yes
☑	User.Read.All Read all users' full profiles	Yes
□	User.ReadBasic.All Read all users' basic profiles	Yes
□	User.ReadWrite.All Read and write all users' full profiles	Yes

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



Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in Default Directory? This will update any existing admin consent records this application already has to match what is listed below.

used. Learn more

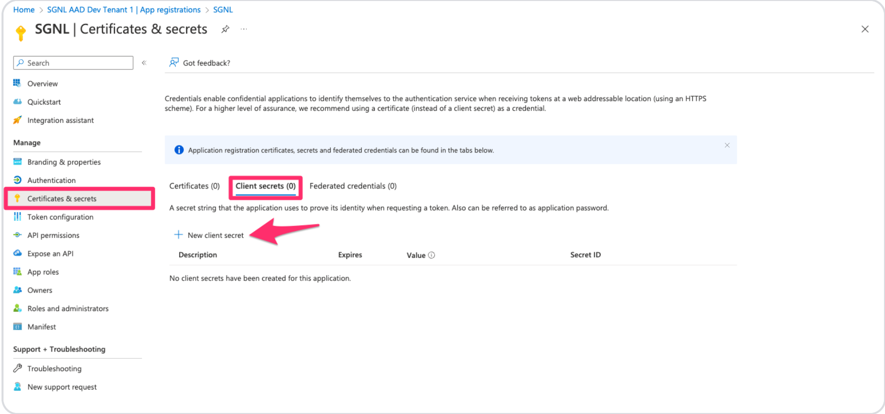
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	Not granted for Default ...
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for Default ...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

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



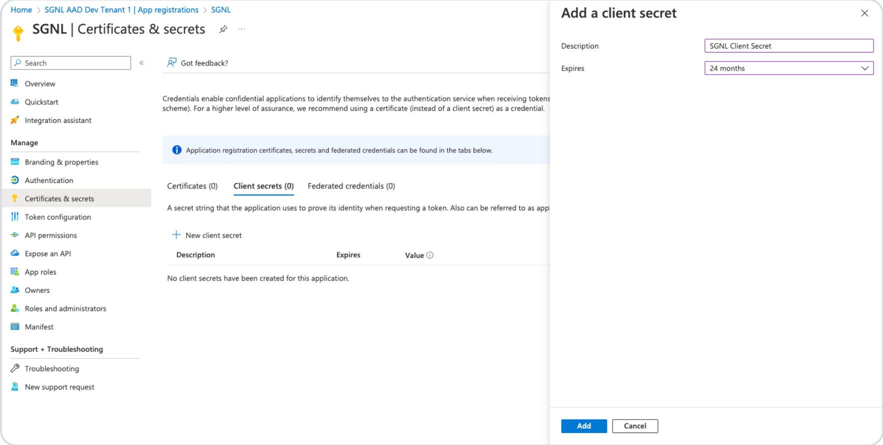
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

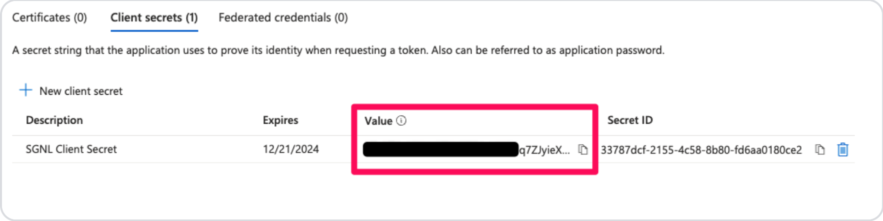
12. Give the secret a description and expiry (the length of time until a new secret will need to be generated for SGNL to communicate with Azure AD), and select Add



Description: SGNL Client Secret

Expires: 24 months

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



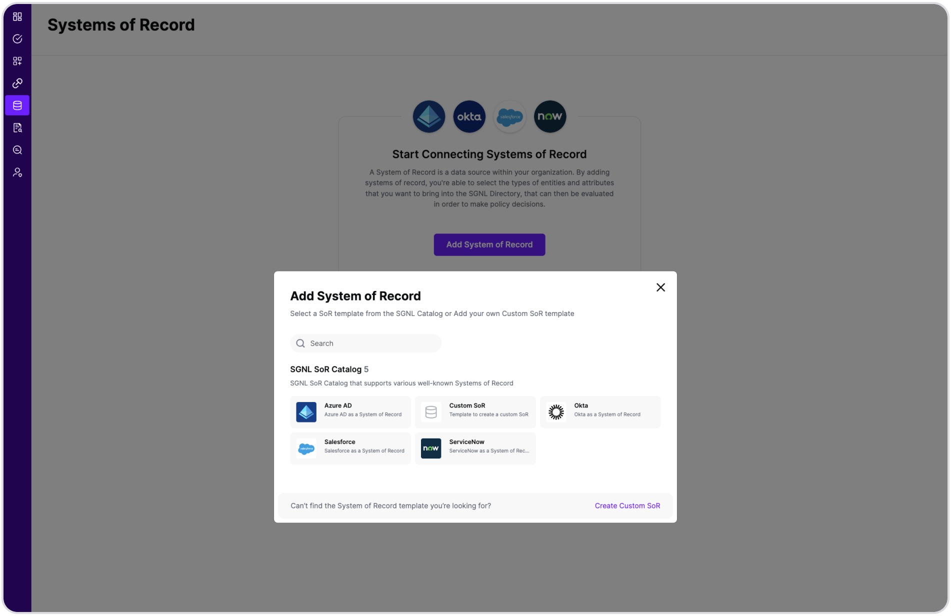
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
SGNL Client Secret	12/21/2024	[redacted]q7ZJyieX...	33787dcf-2155-4c58-8b80-fd6aa0180ce2

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.



Systems of Record

Start Connecting Systems of Record

A System of Record is a data source within your organization. By adding systems of record, you're able to select the types of entities and attributes that you want to bring into the SGNL Directory, that can then be evaluated in order to make policy decisions.

Add System of Record

Add System of Record

Select a SoR template from the SGNL Catalog or Add your own Custom SoR template

Search

SGNL SoR Catalog 5

SGNL SoR Catalog that supports various well-known Systems of Record

Azure AD
Azure AD as a System of Record

Custom SoR
Template to create a custom SoR

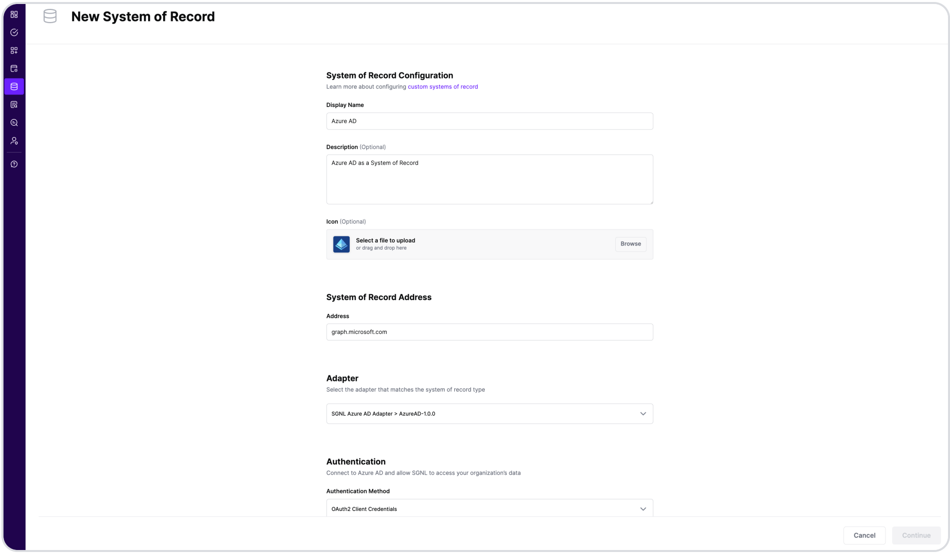
Okta
Okta as a System of Record

Salesforce
Salesforce as a System of Record

ServiceNow
ServiceNow as a System of Rec...

Can’t find the System of Record template you’re looking for? Create Custom SoR

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.



New System of Record

System of Record Configuration

Learn more about configuring custom systems of record

Display Name: Azure AD

Description (Optional): Azure AD as a System of Record

Icon (Optional): Select a file to upload or drag and drop here — Browse

System of Record Address

Address: graph.microsoft.com

Adapter

Select the adapter that matches the system of record type

SGNL Azure AD Adapter > AzureAD-1.0.0

Authentication

Connect to Azure AD and allow SGNL to access your organization’s data

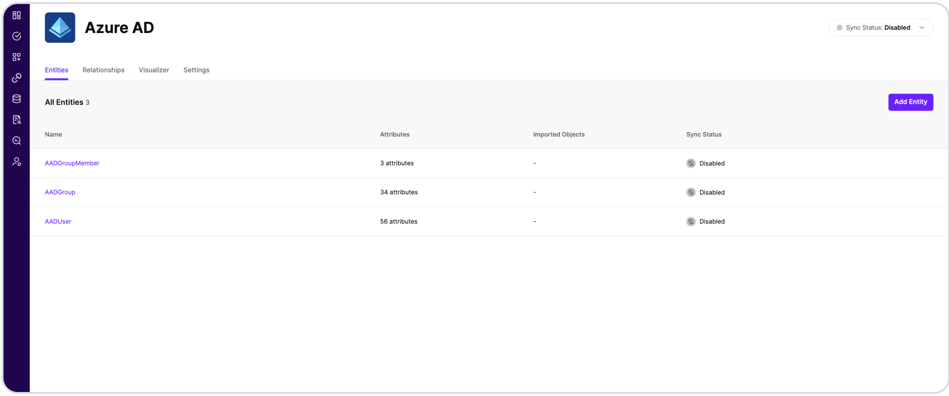
Authentication Method: OAuth2 Client Credentials

Cancel Continue

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.

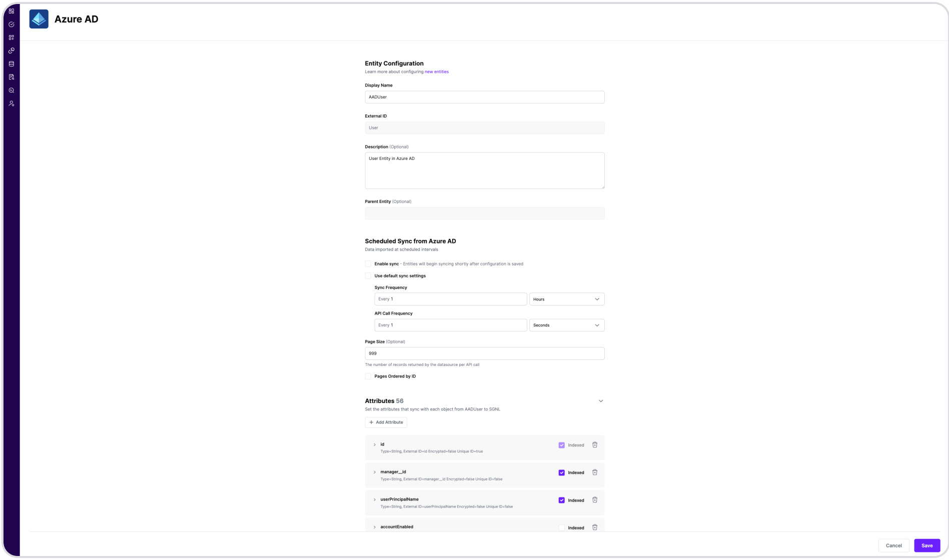


Azure AD

All Entities 3

Name	Attributes	Imported Objects	Sync Status
AADGroupMember	3 attributes	-	Disabled
AADGroup	34 attributes	-	Disabled
AADUser	56 attributes	-	Disabled

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:



Azure AD

Entity Configuration

Learn more about configuring new entities

Display Name: AADUser

External ID: User

Description (Optional): User Entity in Azure AD

Parent Entity (Optional):

Scheduled Sync from Azure AD

Data imported at scheduled intervals

□ **Enable sync** - Entities will begin syncing shortly after configuration is saved

□ Use default sync settings

Sync Frequency: Every 1 Hours

API Call Frequency: Every 1 Seconds

Page Size (Optional): 999

The number of records returned by the datasource per API call

□ Pages Ordered by ID

Attributes 56

Set the attributes that sync with each object from AADUser to SGNL

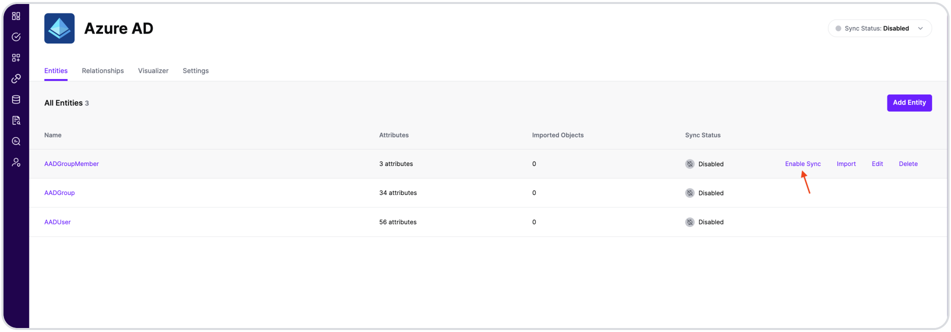
- id — Type=String, External ID=id Encrypted=false Unique ID=true — ☑ Indexed
- manager__id — Type=String, External ID=manager__id Encrypted=false Unique ID=false — ☑ Indexed
- userPrincipalName — Type=String, External ID=userPrincipalName Encrypted=false Unique ID=false — ☑ Indexed
- accountEnabled — □ Indexed

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.

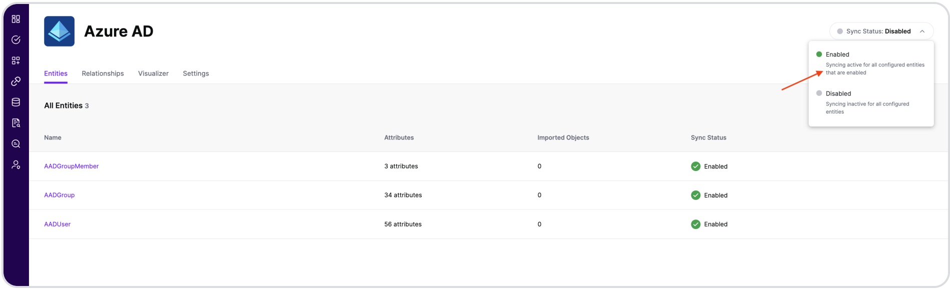


Azure AD

All Entities 3

Name	Attributes	Imported Objects	Sync Status
AADGroupMember	3 attributes	0	Disabled
AADGroup	34 attributes	0	Disabled
AADUser	56 attributes	0	Disabled

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



Azure AD

Enabled
Syncing active for all configured entities that are enabled

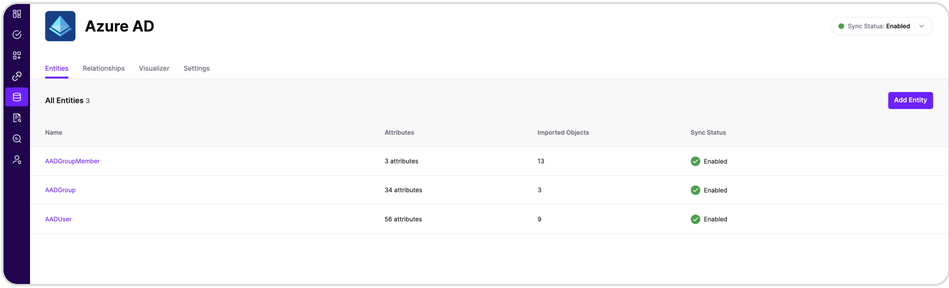
Disabled
Syncing inactive for all configured entities

All Entities 3

Name	Attributes	Imported Objects	Sync Status
AADGroupMember	3 attributes	0	Enabled
AADGroup	34 attributes	0	Enabled
AADUser	56 attributes	0	Enabled

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.



All Entities 3

Name	Attributes	Imported Objects	Sync Status
AADGroupMember	3 attributes	13	✓ Enabled
AADGroup	34 attributes	3	✓ Enabled
AADUser	56 attributes	9	✓ Enabled

Company

About

Careers

Contact Us

Security & Trust

Privacy Policy

Terms of Use

Responsible Disclosure

+1 844-4-SGNL-AI