

Creating and Configuring an Azure Active Directory System of Record

Prerequisites

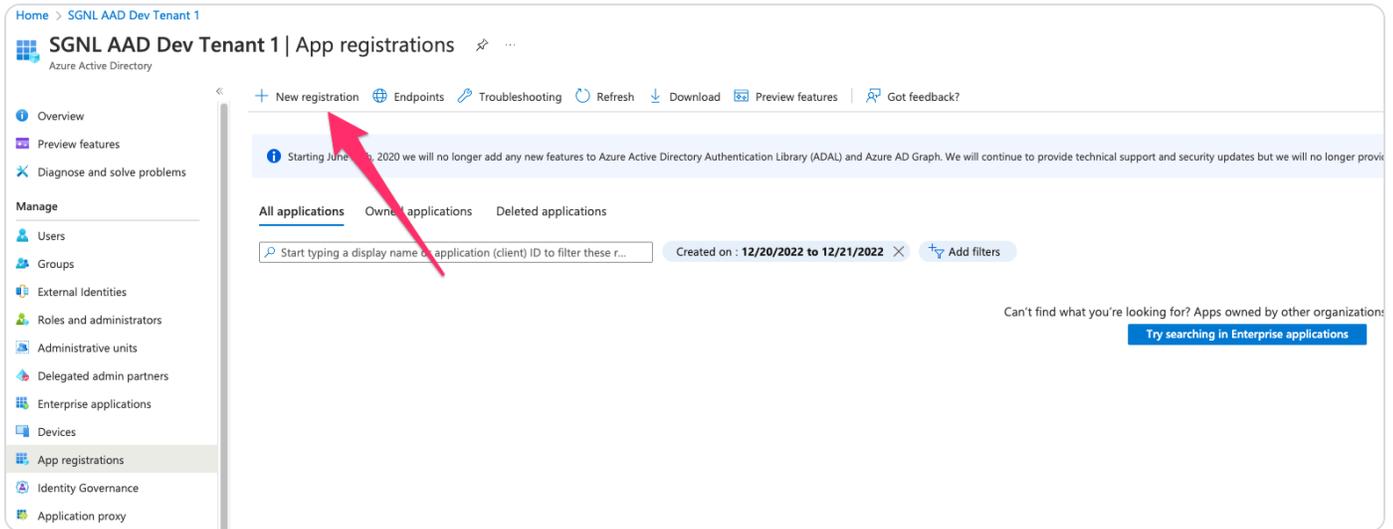
- Azure AD Account with Administrative privileges to Register Apps and Consent to User/Group Read Access in the Microsoft Graph
- SGNL User Account with Admin privileges

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

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](#)

Register

5. Within the App Registration, note the:

- Application (client) Id (**SGNL: AuthClientId**)
- Directory (tenant) Id (**SGNL: AuthTenantId**)

The screenshot shows the Azure App Registrations portal for 'SGNL AAD Dev Tenant 1'. The left-hand navigation menu includes sections for Overview, Quickstart, Integration assistant, Manage (with sub-items like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting (with sub-items like Troubleshooting, New support request). The main content area is titled 'Essentials' and displays the following information:

- Display name: SGNL
- Application (client) ID: [Redacted] **AuthClientId**
- Object ID: [Redacted]
- Directory (tenant) ID: [Redacted] **AuthTenantId**
- 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
- Supported account types: My organization only

Below the essentials, there are two informational messages:

- 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](#)

The 'Get Started' section features a heading 'Build your application with the Microsoft identity platform' and a descriptive paragraph. Below this, three key actions are highlighted with icons and buttons:

- Call APIs**: Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources. [View API permissions](#)
- 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. [View all quickstart guides](#)
- Configure for your organization**: Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications. [Go to 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

Microsoft APIs

APIs my organization uses

My APIs

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.



Azure Service Management



Office 365 Management APIs

8. Select "Application Permissions"

Request API permissions



[< All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) [↗](#)

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

Home > SGNL AAD Dev Tenant 1 | App registrations > SGNL

SGNL | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Request API permissions

ThreatSubmissionPolicy
ThreatSubmission
TrustFrameworkKeySet
User-LifeCycleInfo
UserAuthenticationMethod
UserNotification
UserShiftPreferences

✓ Grant admin consent for SGNL AAD Dev

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 well as your tenant's consent settings, try [Enterprise applications](#).

User (1)

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

VirtualAppointment
WindowsUpdates
WorkforceIntegration

Add permissions Discard

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

Home > App registrations > SGNL

SGNL | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Grant admin consent confirmation.
Do you want to grant admin 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.

Yes

used. [Learn more](#)

Grant admin consent for Default Directory

API / Permissions name Type Description Admin consent requ... Status

Microsoft Graph (3)

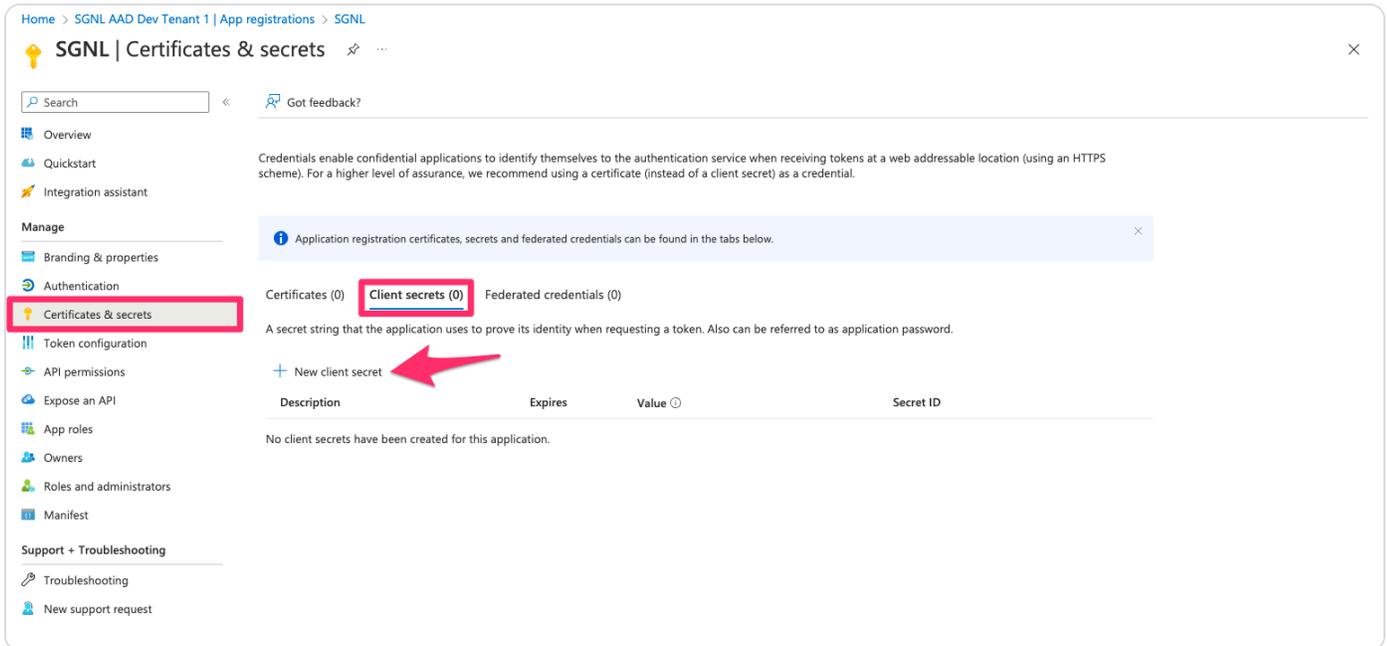
Group.Read.All Application Read all groups Yes ⚠ Not granted for Default ...

User.Read Delegated Sign in and read user profile No

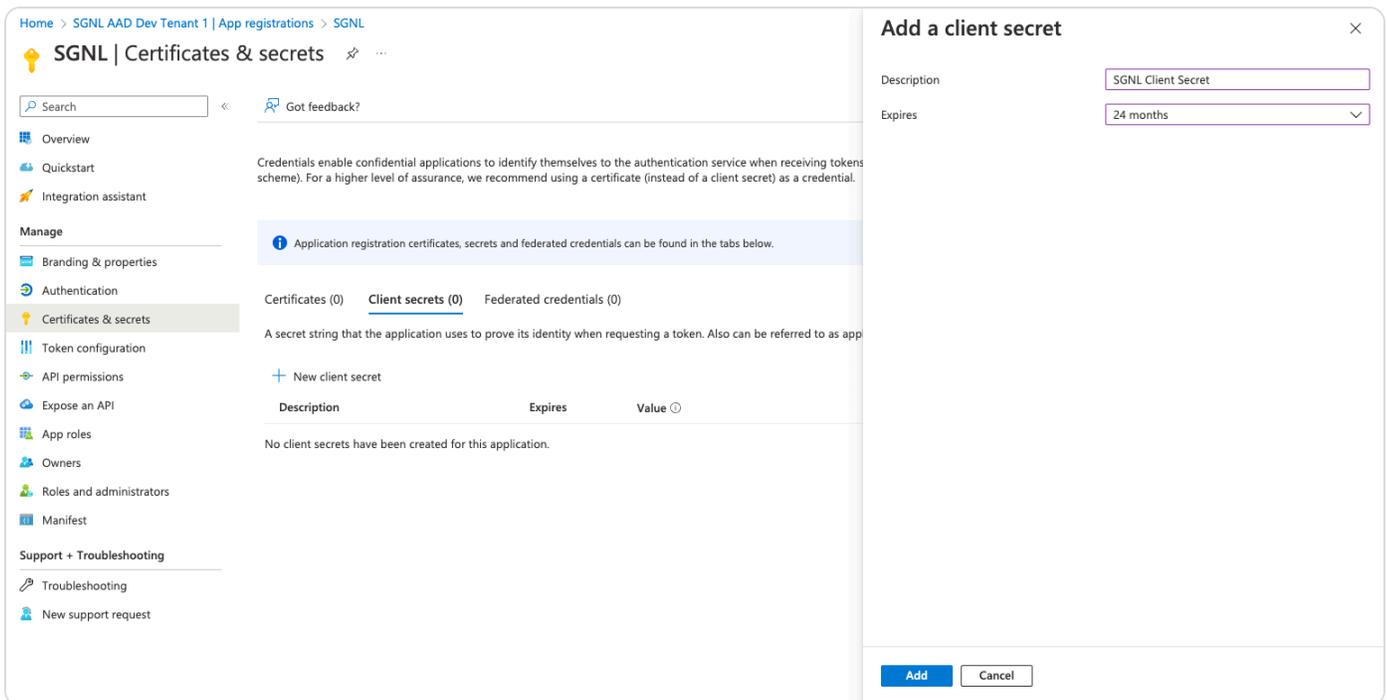
User.Read.All Application Read all users' full profiles Yes ⚠ Not granted for Default ...

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



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**)

Certificates (0) Client secrets (1) Federated credentials (0)

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

+ New client secret

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.

The screenshot shows the 'Systems of Record' page in the SGNL console. The main heading is 'Systems of Record'. Below it, there are logos for Azure AD, Okta, Salesforce, and ServiceNow. A central message reads 'Start Connecting Systems of Record' with a subtext explaining that a System of Record is a data source within an organization. A purple button labeled 'Add System of Record' is visible. A modal dialog box titled 'Add System of Record' is open, showing a search bar and a list of templates under 'SGNL SoR Catalog 5'. The templates include Azure AD, Custom SoR, Okta, Salesforce, and ServiceNow. At the bottom of the dialog, there is a link to '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 Sync Status: Disabled

Entities Relationships Visualizer Settings

All Entities 3 Add Entity

Name	Attributes	Imported Objects	Sync Status
ADGroupMember	3 attributes	-	Disabled
ADGroup	34 attributes	-	Disabled
ADUser	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: ADUser

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 ADUser to SGNL

+ Add Attribute

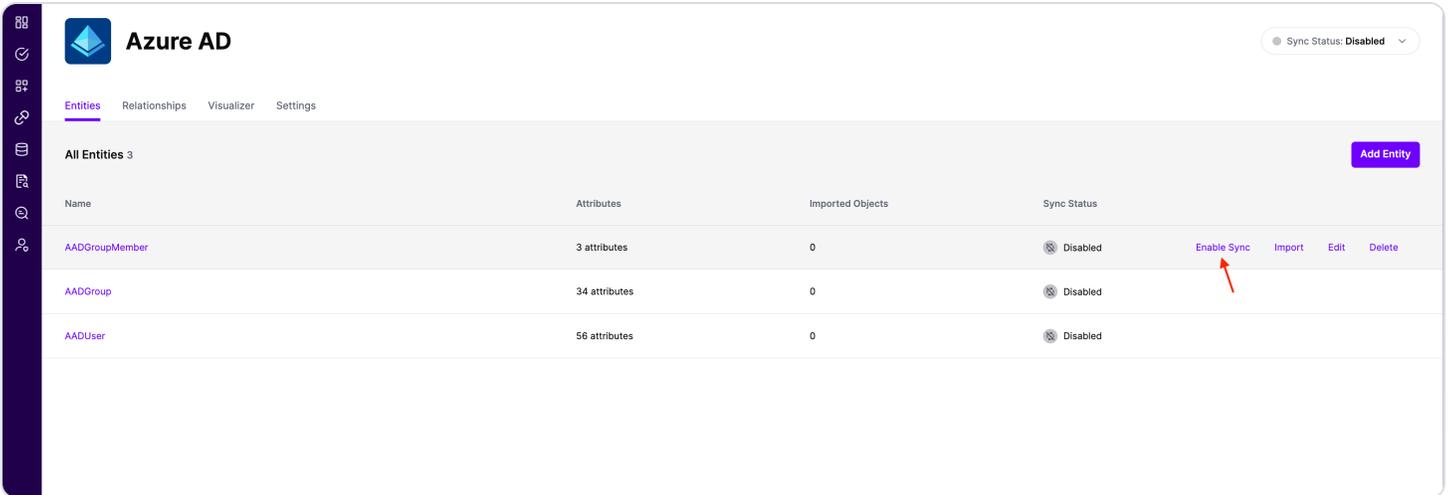
- id [Indexed] [Edit]
- manager_id [Indexed] [Edit]
- userPrincipalName [Indexed] [Edit]
- accountEnabled [Indexed] [Edit]

Cancel Save

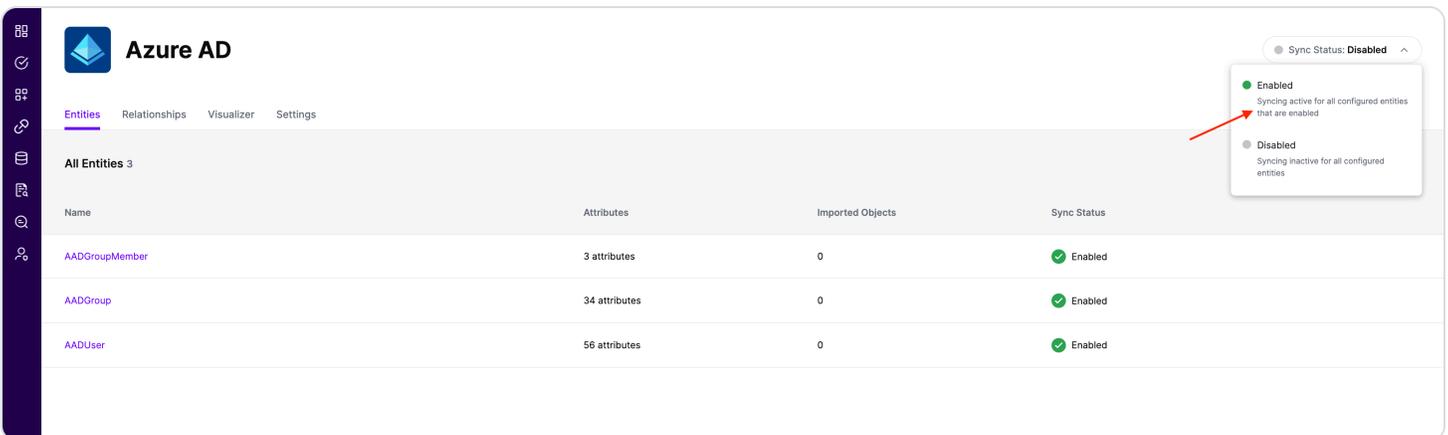
9. You can check the relationships created through the Relationships tab. However, relationships cannot be modified. You will need to delete an existing one, and create a new relationship.
10. (If applicable) You can also create relationships joining entities and attributes in Azure AD to entities and 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](#).

- 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.



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



- 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.

The screenshot shows the Azure AD interface. At the top left is the Azure AD logo and the text "Azure AD". In the top right corner, there is a "Sync Status: Enabled" dropdown menu. Below the header, there are navigation tabs for "Entities", "Relationships", "Visualizer", and "Settings". The "Entities" tab is active, showing "All Entities 3" and an "Add Entity" button. A table lists the entities with columns for Name, Attributes, Imported Objects, and Sync Status.

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

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