Microsoft Entra ID Data Source Documentation

Overview

Singulr discovers Applications, Users and User Attributes from Microsoft Entra ID (previously known as Azure Active Directory). We require read access to Entra's applications and users. This document specifies the exact permissions and resources needed to generate the required credentials as well as the instructions to add Entra as a data source to Singulr AI.

The key steps involved include:

- Register the Singulr-Application in the Azure Tenant with specified permissions and create a client-id and client-secret. Please note you will need to have Cloud Application Administrator role for registering the application.
- Use the tenant-id, client-id and client-secret to add the Entra data source to Singulr

Resource	Use-Case	Permission name	Permission Type	Admin Consent Required	References
Applications	Required to read basic application details such as name, domain, homePageUrl etc.	Application.Read.All	Application	Yes	https://learn.microsoft.com/ us/graph/permissions-reference#userreadall
Users	Required to read user details such as name, title, department, country etc	User.Read.All	Application	Yes	https://learn.microsoft.com/ us/graph/permissions-reference#userreadall
Devices	Required to read the endpoint device associated with a user	Device.Read.All	Application	Yes	https://learn.microsoft.com/ us/graph/permissions-reference#devicereadall
Multi-tenants	Required to list the available tenants in the Organization	MultiTenantOrganization.Read.All	Application	Yes	https://learn.microsoft.com/ us/graph/permissions-reference#devicereadall

Register Singulr Application in Azure Tenant

➡️ **Note:** Move to Configure Permissions Sections, if Singulr Application is already registered in azure tenant.

To register the application, you can follow these general steps:

1. Sign in to the Microsoft Entra admin center as (at least) a Cloud Application Administrator.
2. If you have access to multiple tenants, use the **Settings** icon in the top menu to switch to the tenant in which you want to register the application from the **Directories + subscriptions** menu.

⚙

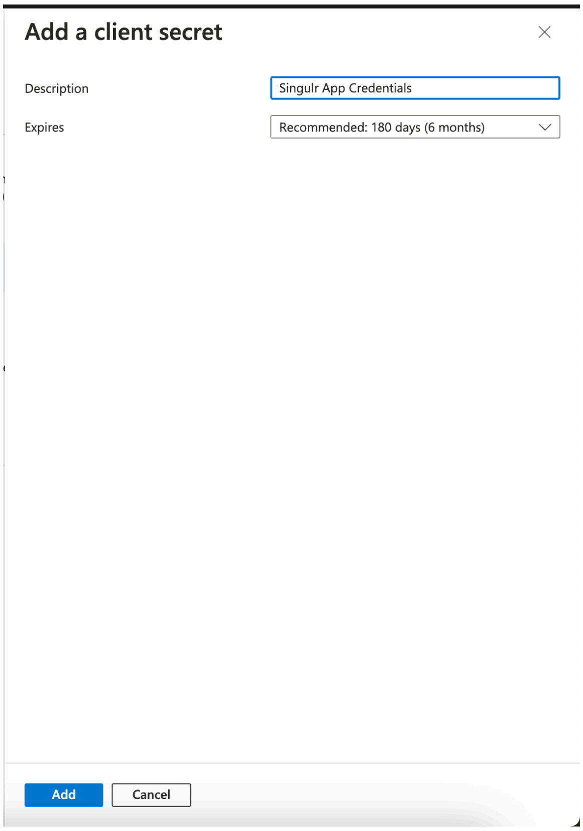
3. Browse to **Identity** > **Applications** > **App registrations** and select **New registration**.
4. Enter name of the application as **Singulr**
5. Select **"Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)"** as supported account-types.
6. Leave the optional field Redirect URI as empty.
7. Select Register to complete the initial app registration.

8. When registration finishes, the Microsoft Entra admin center displays the app registration's **Overview** pane. **Copy** the **Application (client) ID and Directory (tenant) Id** fields.

Add Credentials

To obtain client credentials for the app. Follow the steps below

1. In the Microsoft Entra admin center, in **App registrations**, select Singulr application.
2. Select **Certificates & secrets** > **Client secrets** > **New client secret**.
3. Add description as Singulr App Credentials.
4. Select expiration as 6 months.



Add a client secret

Description: Singulr App Credentials

Expires: Recommended: 180 days (6 months)

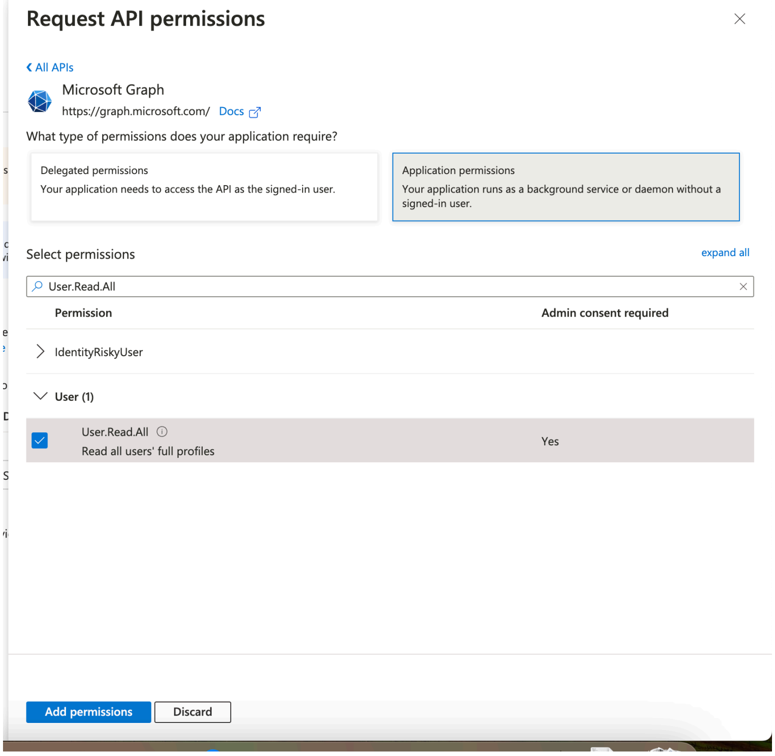
5. Select **Add**.
6. ***Copy the secret's value*** for configuring in data source.

> **Important:** Be sure to copy the **Secret** and store it in a safe place. You will not be able to retrieve it later. If you need a new secret, you must reset the feed credentials.

Configure Permissions

This section covers steps to configure permission for Microsoft Entra Id.

1. Expand **Identity** > **Applications** > select **App registrations.**
2. In the **App registrations** window, under the **All applications** tab, select Singulr app.
3. From the left pane of the window, under the **Manage** menu group, select **API permissions**. In the **Configured permissions** window, select **Add a permission**.
4. In the **Request API permissions** window, switch to the **APIs my organization uses** tab and search for Microsoft Graph. Select from the filtered result set to reveal the **Microsoft Graph** permissions window.
5. Select the **Application permissions** tab and add below **permissions**.
   a. **User.Read.All**
   b. **Application.Read.All**
   c. **Device.Read.All**
   d. **MultiTenantOrganization.Read.All**
6. Grant Admin consent to the newly added permissions (Admin access required). This may be required to be done across multiple tenants in a multi-tenant Entra setup, but this can be skipped for initial deployments.



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.

Select permissions

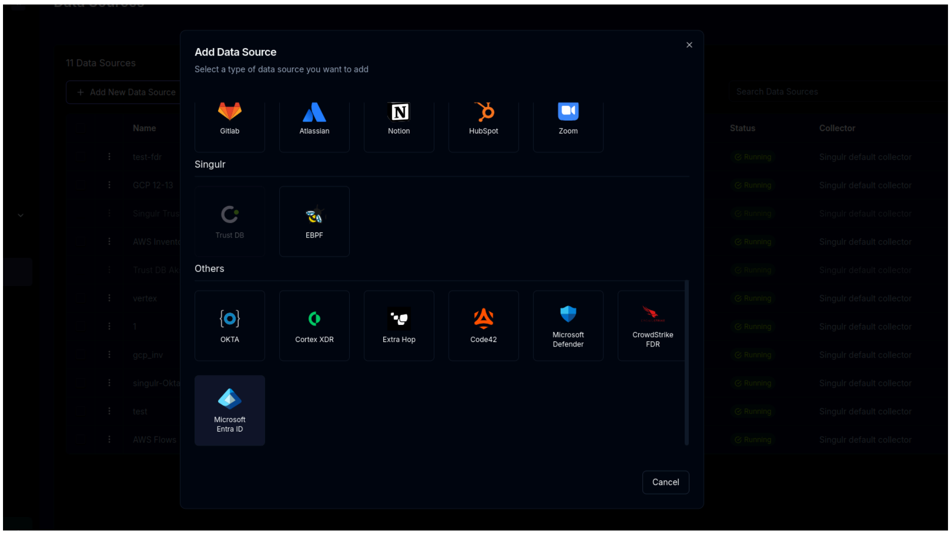
User.Read.All

Permission	Admin consent required
IdentityRiskyUser	
User (1)	
☑ User.Read.All Read all users' full profiles	Yes

Add Microsoft Entra ID Data source to Singulr

To add Microsoft Entra Id as a data source in the Singulr platform:

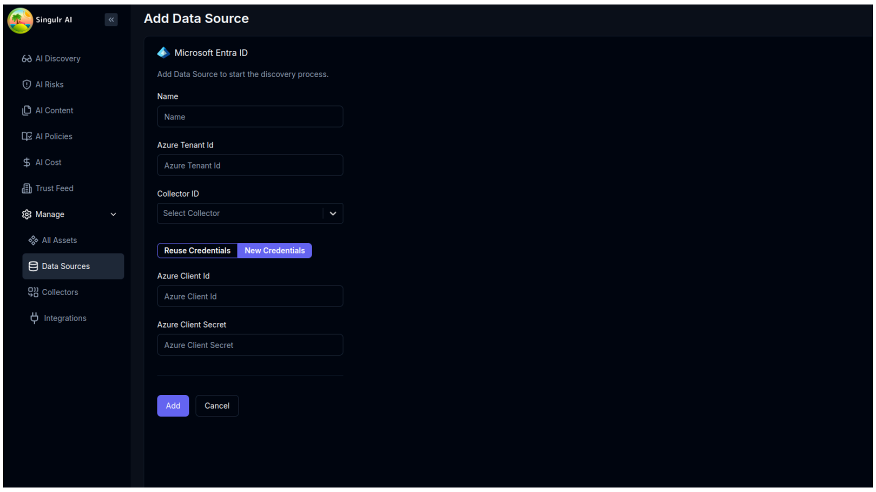
1. Log in to the Singulr platform.
2. Go to "Manage" in the left panel.
3. Navigate to "Data Sources" and click "Add New Data Source."
4. In the pop-up window, scroll down to the "Azure" section and click on Microsoft Entra Id.



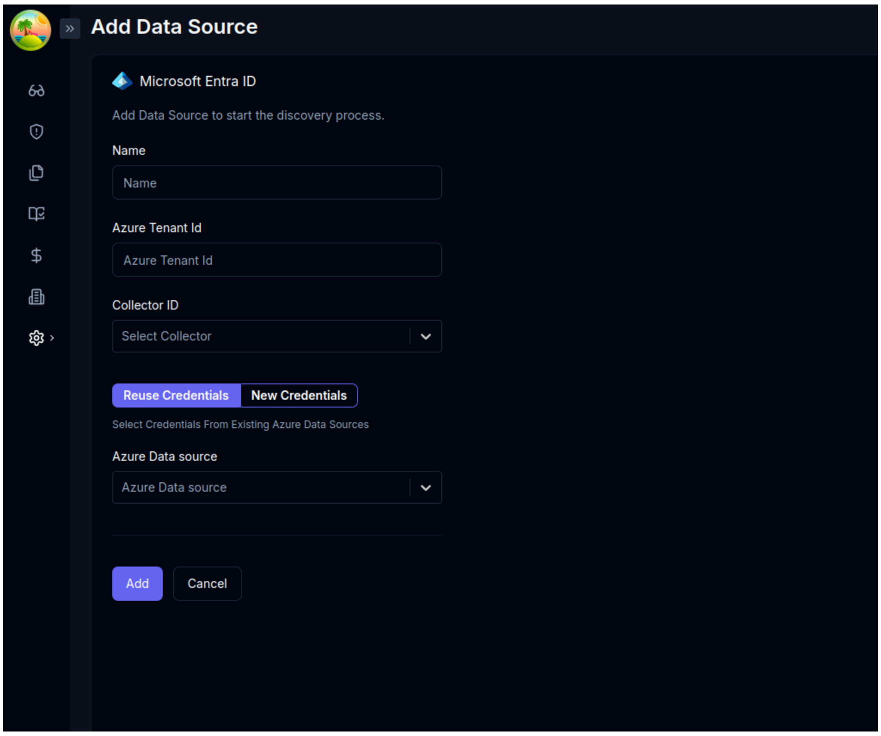
5. Fill in the following details as specified when a new feed is created in Okta:
   - **Name:** Enter a suitable name for this data source
   - **Azure Tenant Id:** Enter **Directory (Tenant Id)**
   - **Collector ID:** Select appropriate collector
6. You have option to either add new credentials or reuse credentials from an existing Datasource.

   Option-1: Fill the below fields to add **new credentials**.

   - **Azure Client Key:** Enter the **Application (client) ID**.
   - **Azure Client Secret:** Enter the Application secret.



   Option-2: Select an existing Azure Datasource for **reusing credentials**.



Add Data Source

Microsoft Entra ID

Add Data Source to start the discovery process.

Name

Name

Azure Tenant Id

Azure Tenant Id

Collector ID

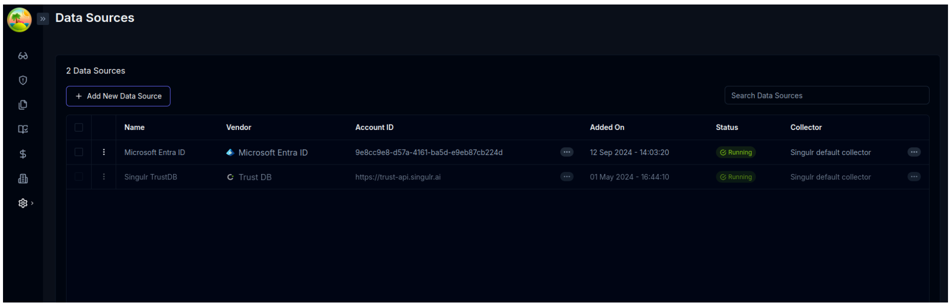
Select Collector

Select Credentials From Existing Azure Data Sources

Azure Data source

Azure Data source

7. Click "Add" Once completed, a new entry for Microsoft Entra ID Id will appear on the Data Sources page.



Data Sources

2 Data Sources

□		Name	Vendor	Account ID		Added On	Status	Collector	
□	⋮	Microsoft Entra ID	Microsoft Entra ID	9e8cc9e8-d57a-4161-ba5d-e9eb87cb224d	···	12 Sep 2024 - 14:03:20	✓ Running	Singulr default collector	···
□	⋮	Singulr TrustDB	Trust DB	https://trust-api.singulr.ai	···	01 May 2024 - 16:44:10	✓ Running	Singulr default collector	···