

# Information oversharing template setup

## Contents

Overview .....	1
Installing Pre-reqs .....	1
Synapse pipeline template.....	9
PBI report template .....	17

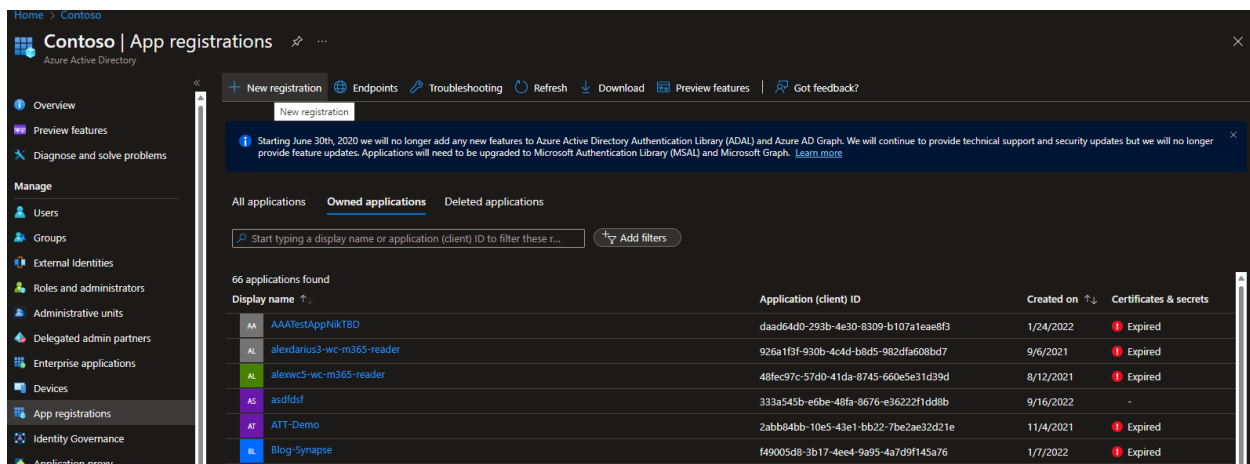
## Overview

Information oversharing is a security and compliance use case powered by our newly available SharePoint datasets. This allows customers to better understand how secure their SharePoint is, maintain information boundaries, and establish new rules based on how sensitive data is managed and classified.

## Installing Pre-reqs

The first step to running this template would be to create an application in the tenant and use that appld and secret to setup the other required resources.

### 1. Navigate to app registrations in your subscription



### 2. Register a new application

Microsoft Azure Search resources, services, and docs (G+)

Home > Contoso | App registrations >

## Register an application

\* Name

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

test\_application ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Contoso 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...](#)

3. Save the application id (In the screenshot, the one ending in 9826). Navigate to API permissions

Home > Contoso | App registrations >

**test\_application**

Search Delete Endpoints Preview features

Overview Quickstart Integration assistant

**Manage**

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

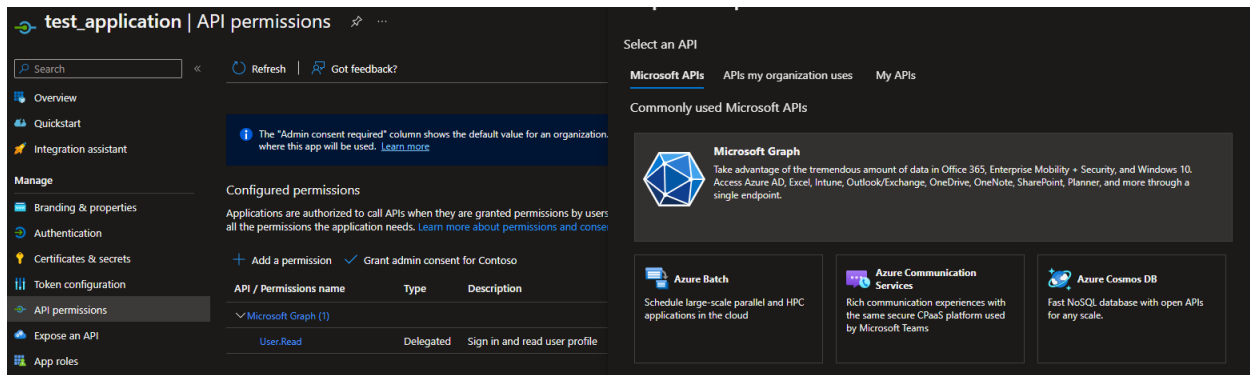
**Essentials**

Display name	: test_application	Client credentials	: <a href="#">Add a certificate or secret</a>
Application (client) ID	: df7ae62b-cee6-4311-9684-d074ff929826	Redirect URIs	: <a href="#">Add a Redirect URI</a>
Object ID	: 4460a398-5543-478c-a7e4-ce9092f385de	Application ID URI	: <a href="#">Add an Application ID URI</a>
Directory (tenant) ID	: 82100b66-ace5-4bd1-a137-f11432b93451	Managed application in L...	: <a href="#">test_application</a>
Supported account types	: <a href="#">My organization only</a>		

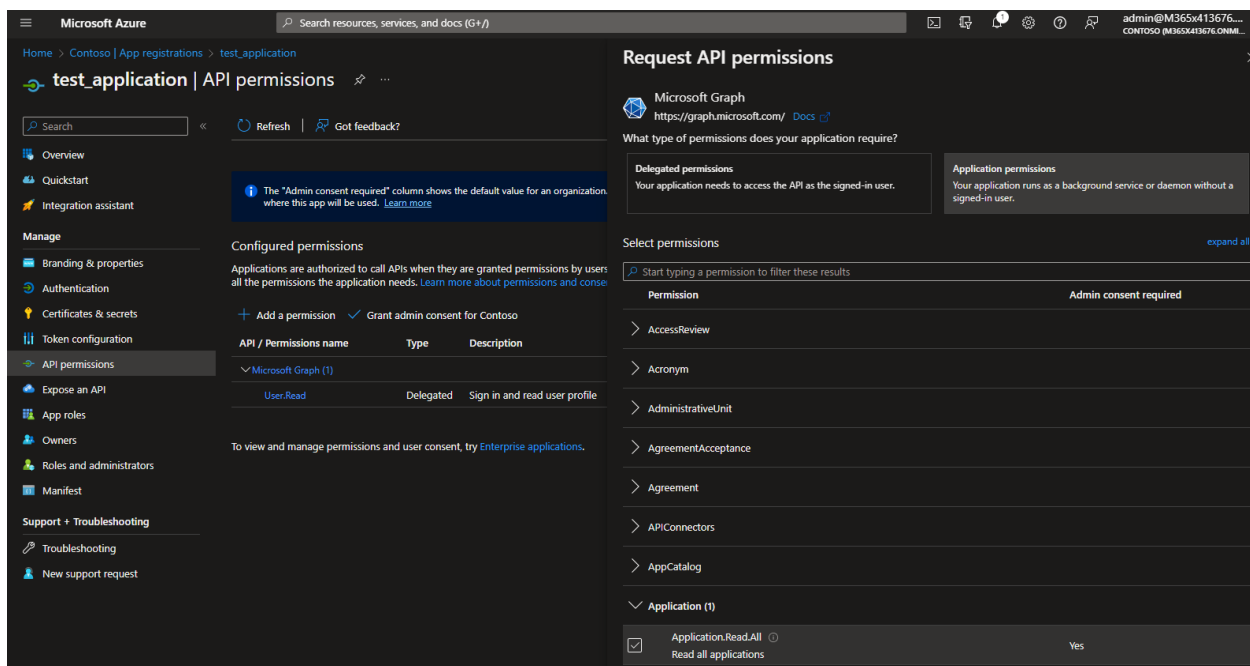
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

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. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

4. Select "Microsoft Graph" from the Add permission flyout



## 5. Select “Application permissions -> Applications -> Application.Read.All”



## 6. Explicitly Grant consent for the new permissions

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Contoso | App registrations > test\_application

test\_application | 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

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in where this app will be 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](#)

+ Add a permission Grant admin consent for Contoso

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (2)				
Application.Read.All	Application	Read all applications	Yes	Not granted for Contoso

7. Verify that that the status shows as granted for the new Application.Read.All permission

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Contoso | App registrations > test\_application

test\_application | 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

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in where this app will be 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](#)

+ Add a permission Grant admin consent for Contoso

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (2)				
Application.Read.All	Application	Read all applications	Yes	Granted for Contoso
User.Read	Delegated	Sign in and read user profile	No	Granted for Contoso

8. Navigate to "Certificates and secrets" in the left pane and click on "New client secret"

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Contoso | App registrations > test\_application

test\_application | Certificates & secrets

Search Got feedback?

Overview Quickstart Integration assistant

Manage

Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles

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.

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

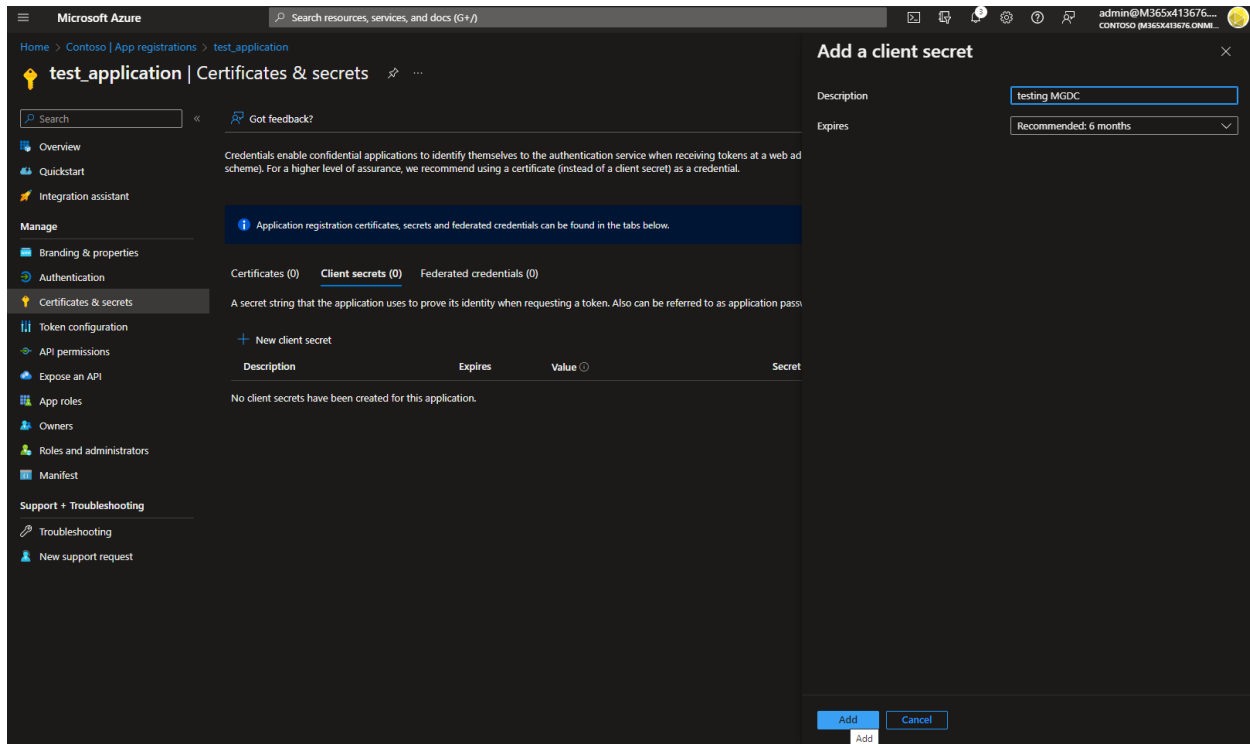
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

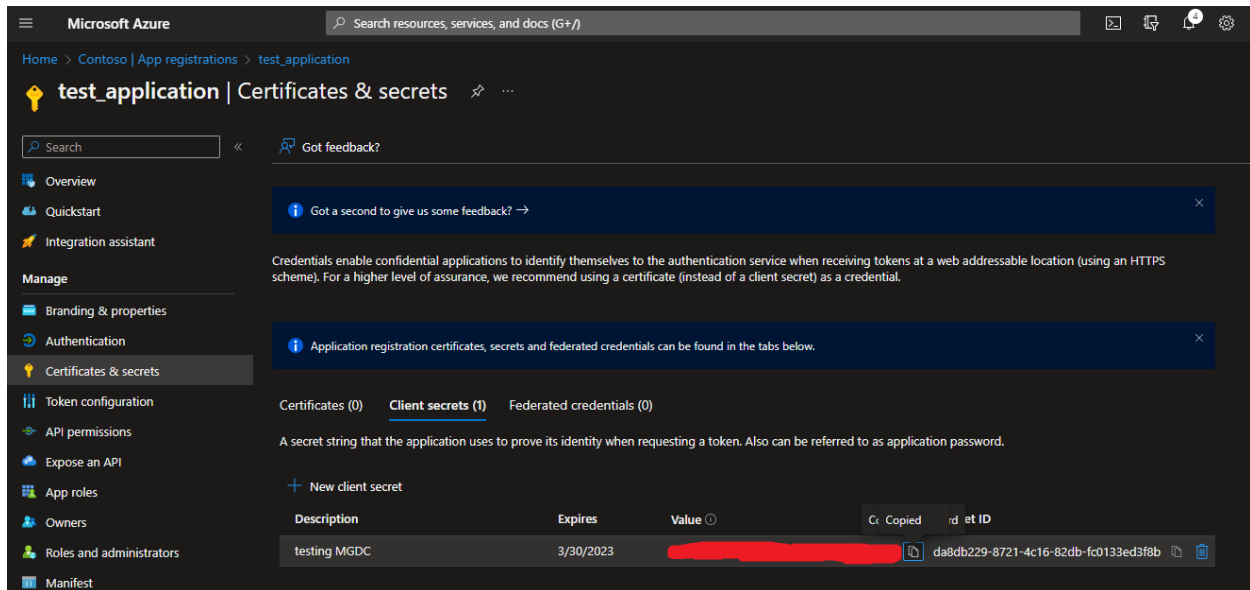
Description	Expires	Value	Secret ID
New client secret			

No client secrets have been created for this application.

## 9. Provide a description and add a secret



## 10. Copy the value of this new secret and save it securely before navigating away from this page



## 11. Use this link to initiate the setup of the pre-requisites. Use the appid and secret created in the previous steps. [Custom deployment - Microsoft Azure](#)

The link above sets up the pre-requisites to using the information oversharing template, which are:

- Create a Synapse Workspace
- Create a Spark Pool for the Synapse workspace
- Create a storage account for the extracted data
- Grant permission to the Synapse workspace & the MGDC Service Principal to the storage account as Blob Data Contributor
- Create an Azure SQL Server
- Create a sample database within the Azure SQL Server.

By clicking on the above button (or navigating to the linked URL), users will be brought to the Azure portal on the Custom deployment page.

On that screen, on top of providing information about the resource group and region to deploy the components into, they will need to provide the following information:

- Application Id to be used by MGDC (from step #3, ending in 9826)
- Application secret for that app
- A new password for the Azure SQL Server

Once all required information has been provided, click on the **Review + create** button at the bottom of the page:

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) >


## Custom deployment


Deploy from a custom template


Basics


Review + create

Template

 Customized template [↗](#)  
18 resources

 Edit template

 Edit parameters

 Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Microsoft Azure Sponsorship 2 (30a81c99-6121-40ba-99d7-ac67496... ▼

Resource group \* ⓘ

(New) Demo\_test\_RG ▼

[Create new](#)

Instance details

Region \* ⓘ

East US ▼

App Id \* ⓘ

df7ae62b-cee6-4311-9684-d074ff929826 ✓

App Secret \* ⓘ

..... ✓

SQL Admin Password \* ⓘ

..... ✓

Review + create

< Previous

Next : Review + create >

This will validate that the information provided to the template is correct. Once the information has been validated, click on the **Create** button at the bottom of the page.

Microsoft Azure

Search resources, services, and docs (G+ /)

[Home](#) >

# Custom deployment


Deploy from a custom template

✓ Validation Passed

Basics

Review + create

## Summary



Customized template  
18 resources

## Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the [Azure Marketplace](#); both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

## Basics

Subscription	Microsoft Azure Sponsorship 2
Resource group	Demo_test_RG
Region	East US

Create

< Previous

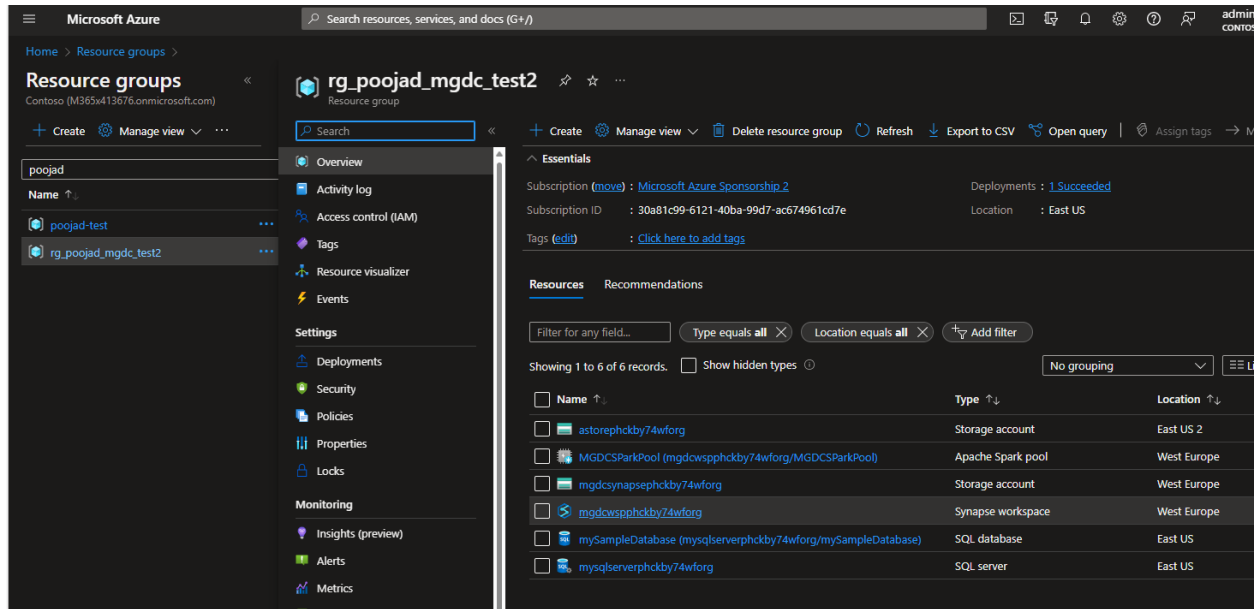
Next

This will initiate the deployment. It should normally take about 5 minutes for the whole deployment to complete.

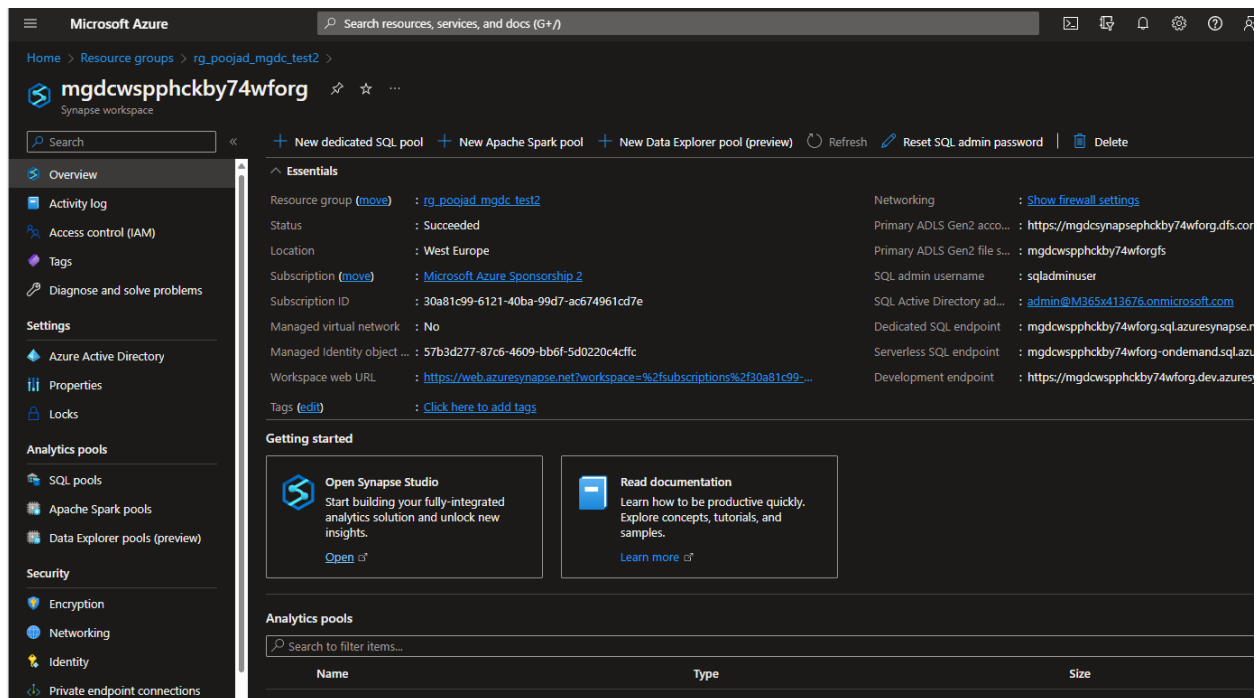


## Synapse pipeline template

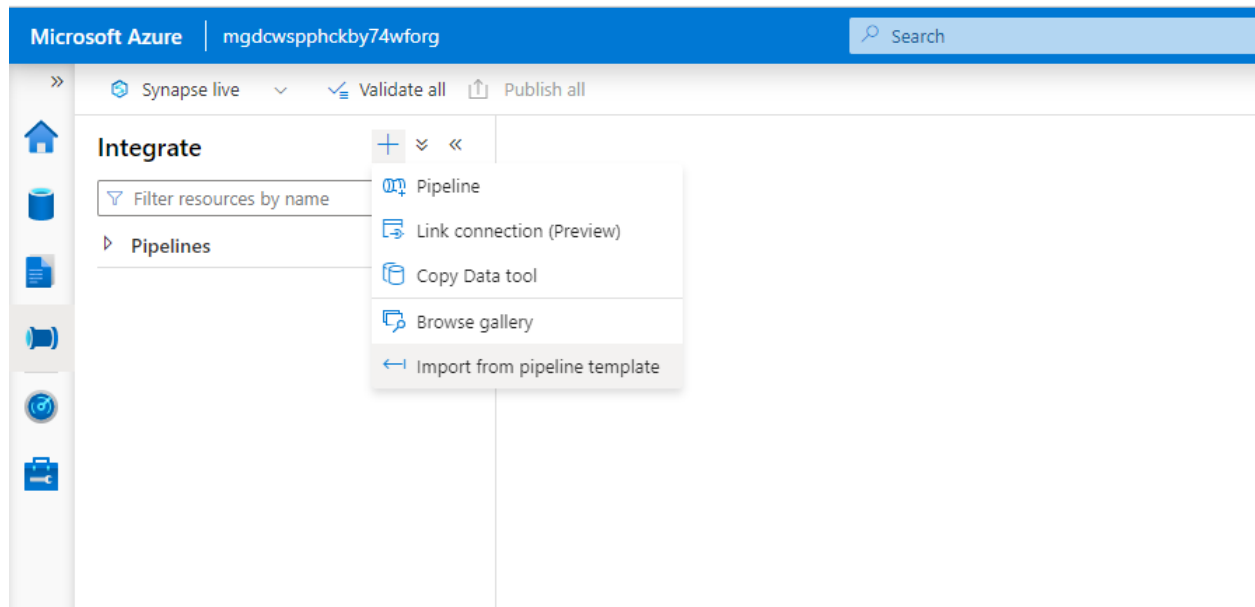
1. After the pre-reqs are complete, navigate to the Synapse workspace just created



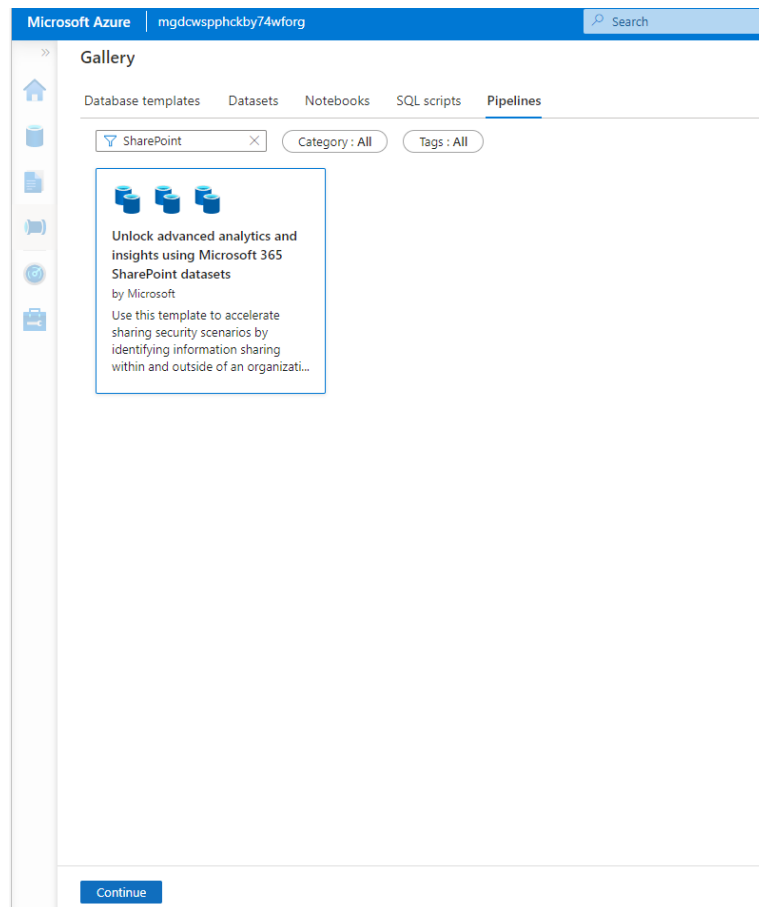
2. Open the Synapse Studio



3. Navigate to “Integrate -> Add new resource ->Browse gallery”



4. Search for “SharePoint” and select the “Unlock advanced analytics and insights using Microsoft 365 SharePoint datasets” template and Continue



## 5. Create the new Linked services required by this pipeline

The screenshot displays the Microsoft Azure portal interface for a data pipeline template. The top navigation bar shows the user's account and a search bar. The left sidebar contains navigation icons for home, data, pipelines, and other resources.

**Description**

Use this template to accelerate sharing security scenarios by identifying information sharing within and outside of an organization. This template extracts Microsoft 365 SharePoint data via Microsoft Graph Data Connect and aggregates with Azure Active Directory groups to produce analytics-ready data for analysis.

[View documentation](#)

**Tags**

MGDC, Azure Synapse Analytics, OneDrive, SharePoint, Security, AAD, Sharing, Sites, SPGroups, Documents, Syntex, M365, Office365, Graph

**Services**

Azure Synapse Analytics, Azure Data Lake Storage

**Inputs**

**Linked service \***  
For DS\_GroupMembers\_Target (Binary dataset),  
DS\_GroupDetails\_Target (Binary dataset),  
DS\_GroupOwners\_Target (Binary dataset),  
DS\_Sharing\_Target (Binary dataset),  
DS\_Sites\_Target (Binary dataset),  
DS\_SPGroups\_Target (Binary dataset)

Select...  
Filter...  
Select...  
+ New  
mgdcwspphckby74wforg-Wo + New defaultStorage  
AzureDataLakeStorage1

**Preview**

The preview section shows a data flow diagram. It starts with three 'Copy data' activities: 'ExtractAADGroupMembers', 'ExtractAADGroupDetails', and 'ExtractAADGroupOwners'. These feed into a 'Notebook' activity 'AADGroupExpansion'. This notebook then feeds into another 'Copy data' activity 'ExtractSharingInfo'. This activity feeds into a 'Notebook' activity 'SPGroup'. Finally, this notebook feeds into a 'Copy data' activity 'ExtractSPGroups'.

## 6. Provide the parameters of the Linked Service

- Select Authentication Type = Service Principal
- Use the storage account name, SPN id and secret (SPN key) from the pre-req steps above
- Test Connection and then click on Create

Microsoft Azure | mgdcwspphckby74wfor

Search

admin@M365x413676.onmicrosoft.com

CONTOSO

**Description**

Use this template to accelerate sharing security scenarios by identifying information sharing within and outside of an organization. This template extracts Microsoft 365 SharePoint data via Microsoft Graph Data Connect and aggregates with Azure Active Directory groups to produce analytics-ready data for analysis.

[View documentation](#)

**Tags**

MGDC Azure Synapse Analytics OneDrive SharePoint Security AAD Sharing Sites SPGroups Documents Syntax M365 Office365 Graph

**Services**

Azure Synapse Analytics Azure Data Lake Storage

**Inputs**

**Linked service \***  
For DS\_GroupMembers\_Target (Binary dataset), DS\_GroupDetails\_Target (Binary dataset), DS\_GroupOwners\_Target (Binary dataset), DS\_Sharing\_Target (Binary dataset), DS\_Sites\_Target (Binary dataset), DS\_SPGroups\_Target (Binary dataset)

Select...

**Linked service \***  
For DS\_GroupMembers\_Source (Microsoft 365 (Office 365) dataset), DS\_GroupDetails\_Source (Microsoft 365 (Office 365) dataset), DS\_GroupOwners\_Source (Microsoft 365 (Office 365) dataset), DS\_Sharing\_Source (Microsoft 365 (Office 365) dataset), DS\_Sites\_Source (Microsoft 365 (Office 365) dataset), DS\_SPGroups\_Source (Microsoft 365 (Office 365) dataset)

Select...

**Open pipeline** **Back**

**Preview**

Copy data ExtractAADGroupMembers  
Copy data ExtractAADGroupDetails  
Copy data ExtractAADGroupOwners

**New linked service**  
Azure Data Lake Storage Gen2 [Learn more](#)

**Description**

Connect via integration runtime \*  
AutoResolveIntegrationRuntime

**Authentication type**  
Service Principal

**Account selection method**  
From Azure subscription Enter manually

**Azure subscription**  
Select all

**Storage account name \***  
mgdcwspphckby74wfor

**Authentication reference method**  
Inline Credential

**Tenant \***  
82100b66-ace5-4bd1-a137-f11432b93451

**Service principal ID \***

**Service principal credential type \***  
Service principal key

**Service principal key \***  
Service principal key Azure Key Vault

**Azure cloud type**  
workspace's cloud type

**Create** **Cancel** [Test connection](#)

## 7. Repeat the inked Service creation steps for the source linked service

Microsoft Azure | mgdcwspphckby74wfor

Search

admin@M365x413676.onmicrosoft.com

CONTOSO

**Description**

Use this template to accelerate sharing security scenarios by identifying information sharing within and outside of an organization. This template extracts Microsoft 365 SharePoint data via Microsoft Graph Data Connect and aggregates with Azure Active Directory groups to produce analytics-ready data for analysis.

[View documentation](#)

**Tags**

MGDC Azure Synapse Analytics OneDrive SharePoint Security AAD Sharing Sites SPGroups Documents Syntax M365 Office365 Graph

**Services**

Azure Synapse Analytics Azure Data Lake Storage

**Inputs**

**Linked service \***  
For DS\_GroupMembers\_Target (Binary dataset), DS\_GroupDetails\_Target (Binary dataset), DS\_GroupOwners\_Target (Binary dataset), DS\_Sharing\_Target (Binary dataset), DS\_Sites\_Target (Binary dataset), DS\_SPGroups\_Target (Binary dataset)

AzureDataLakeStorage3

**Linked service \***  
For DS\_GroupMembers\_Source (Microsoft 365 (Office 365) dataset), DS\_GroupDetails\_Source (Microsoft 365 (Office 365) dataset), DS\_GroupOwners\_Source (Microsoft 365 (Office 365) dataset)

Filter...

Select...

+ New

**Preview**

Copy data ExtractAADGroupMembers  
Copy data ExtractAADGroupDetails  
Copy data ExtractAADGroupOwners

Notebook AADGroupExpansion

Copy data ExtractSharingInfo

Copy data ExtractSites

Copy data ExtractSPGroups

Notebook SPGroupExpansion

Set variable (X) Success

## 8. Select “Open Pipeline”

The screenshot displays the Microsoft Azure Data Factory portal interface. The top navigation bar shows the user is logged in as 'admin@M365x413676.onmicrosoft.com'. The main content area is divided into two panels: 'Description' on the left and 'Preview' on the right.

**Description Panel:**

- Description:** A paragraph explaining the template's purpose: "Use this template to accelerate sharing security scenarios by identifying information sharing within and outside of an organization. This template extracts Microsoft 365 SharePoint data via Microsoft Graph Data Connect and aggregates with Azure Active Directory groups to produce analytics-ready data for analysis."
- View documentation:** A link to view the documentation.
- Tags:** A collection of tags including MGDC, Azure Synapse Analytics, OneDrive, SharePoint, Security, AAD, Sharing, Sites, SPGroups, Documents, Syntex, M365, Office365, and Graph.
- Services:** A collection of services including Azure Synapse Analytics and Azure Data Lake Storage.
- Inputs:** A section for linked services. It lists several datasets (e.g., DS\_GroupMembers\_Target, DS\_GroupDetails\_Target) and shows two dropdown menus for selecting linked services. The first dropdown is set to 'AzureDataLakeStorage3' and the second is set to 'Microsoft3653'.
- Buttons:** At the bottom of the Description panel, there are two buttons: 'Open pipeline' (highlighted in blue) and 'Back'.

**Preview Panel:**

- Diagram:** A flow diagram showing the data pipeline. It starts with three 'Copy data' activities: 'ExtractAADGroupMembers', 'ExtractAADGroupDetails', and 'ExtractAADGroupOwners'. These feed into a 'Notebook' activity labeled 'AADGroupExpansion'. This notebook activity then feeds into another 'Copy data' activity 'ExtractSharingInfo', which feeds into a second 'Notebook' activity 'SPGroupExpansion'. This second notebook activity feeds into a 'Set variable' activity, which finally leads to a 'Success' icon.
- Notification:** A green checkmark icon with the text 'Successfully created' and 'Successfully created Microsoft3653 (Linked service)'.

## 9. Click on “Publish All” to validate and publish the pipeline

Synapse live Validate all Publish all 15

Unlock advanced analytics... Validate all resources and publish them to the live, running factory

Activities

Search activities

- Synapse
- Move & transform
- Azure Data Explorer
- Azure Function
- Batch Service
- Databricks
- Data Lake Analytics
- General
- HDInsight
- Iteration & conditionals
- Machine Learning

Copy data ExtractAADGroupMembers

Copy data ExtractAADGroupDetails

Copy data ExtractAADGroupOwners

Notebook AADGroupExpansion

Copy data ExtractSharingInfo

Notebook SPGroupExpansion

Set variable Success

Parameters Variables Settings Output

+ New Delete

Name	Type	Default value
StartTime	String	2022-08-31T00:00:00Z
EndTime	String	2022-08-31T00:00:00Z
StorageAccountName	String	<< PipelineParameters.FillStc
StorageContainerName	String	<< PipelineParameters.FillStc
SparkPoolName	String	<< PipelineParameters.FillSp

## 10. Review the changes and click Publish

Synapse live Validate all Publishing 15

Unlock advanced analytics... Validate Debug Add trigger

Activities

Search activities

- Synapse
- Move & transform
- Azure Data Explorer
- Azure Function
- Batch Service
- Databricks
- Data Lake Analytics
- General
- HDInsight
- Iteration & conditionals
- Machine Learning

Copy data ExtractAADGroupMembers

Copy data ExtractAADGroupDetails

Copy data ExtractAADGroupOwners

Notebook AADGroupExpansion

Copy data ExtractSharingInfo

Notebook SPGroupExpansion

Parameters Variables Settings Output

+ New Delete

Name	Type	Default value
StartTime	String	2022-08-31T00:00:00Z
EndTime	String	2022-08-31T00:00:00Z
StorageAccountName	String	<< PipelineParameters.FillStc
StorageContainerName	String	<< PipelineParameters.FillStc
SparkPoolName	String	<< PipelineParameters.FillSp

**Publish all**

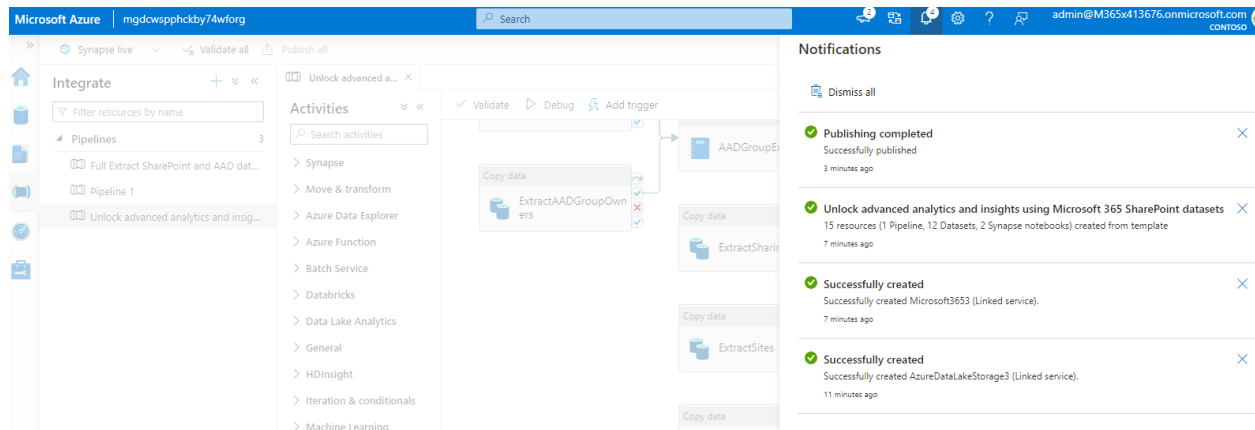
You are about to publish all pending changes to the live environment. [Learn more](#)

**Pending changes (15)**

NAME	CHANGE	EXISTING
<b>Pipelines</b>		
Unlock advanced analytics... (New)	-	-
<b>Datasets</b>		
DS_GroupMembers_Source1 (New)	-	-
DS_GroupMembers_Target1 (New)	-	-
DS_GroupDetails_Source1 (New)	-	-
DS_GroupDetails_Target1 (New)	-	-
DS_GroupOwners_Source1 (New)	-	-
DS_GroupOwners_Target1 (New)	-	-
DS_Sharing_Source1 (New)	-	-
DS_Sharing_Target1 (New)	-	-
DS_Sites_Source1 (New)	-	-
DS_Sites_Target1 (New)	-	-
DS_SPGroups_Source1 (New)	-	-
DS_SPGroups_Target1 (New)	-	-
<b>Notebook</b>		
AADGroupExpansion1 (New)	-	-
SPGroupExpansion1 (New)	-	-

Publish Cancel

## 11. Verify that the pipeline has been successfully published



Microsoft Azure | mgdcwspphckby74wforg

Integrate

Filter resources by name

Pipelines

- Full Extract SharePoint and AAD dat...
- Pipeline 1
- Unlock advanced analytics and insig...

Activities

- Synapse
- Move & transform
- Azure Data Explorer
- Azure Function
- Batch Service
- Databricks
- Data Lake Analytics
- General
- HDInsight
- Iteration & conditionals
- Machine Learning

Copy data

ExtractAADGroupOwners

Copy data

ExtractSharingInfo

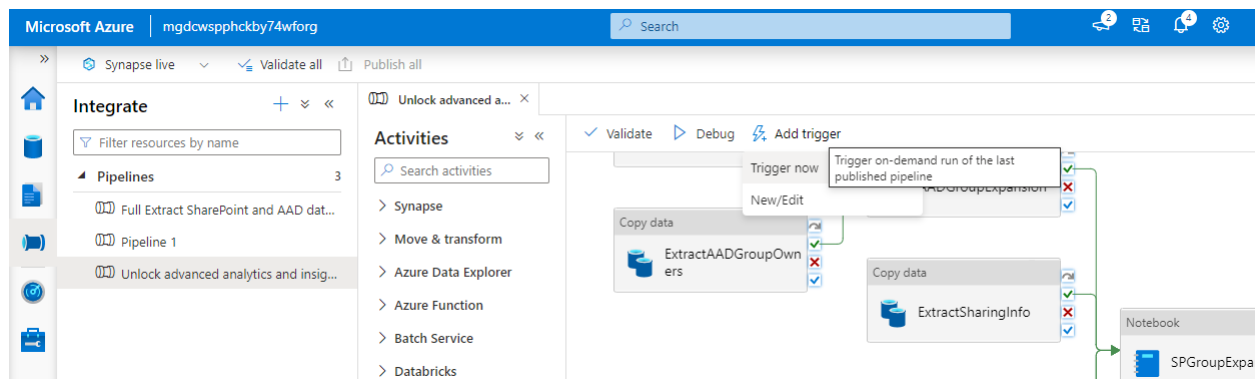
Copy data

ExtractSites

Notifications

- Dismiss all
- Publishing completed  
Successfully published  
3 minutes ago
- Unlock advanced analytics and insights using Microsoft 365 SharePoint datasets  
15 resources (1 Pipeline, 12 Datasets, 2 Synapse notebooks) created from template  
7 minutes ago
- Successfully created  
Successfully created Microsoft3653 (Linked service).  
7 minutes ago
- Successfully created  
Successfully created AzureDataLakeStorage3 (Linked service).  
11 minutes ago

## 12. Trigger the pipeline



Microsoft Azure | mgdcwspphckby74wforg

Integrate

Filter resources by name

Pipelines

- Full Extract SharePoint and AAD dat...
- Pipeline 1
- Unlock advanced analytics and insig...

Activities

- Synapse
- Move & transform
- Azure Data Explorer
- Azure Function
- Batch Service
- Databricks

Copy data

ExtractAADGroupOwners

Copy data

ExtractSharingInfo

Copy data

ExtractSites

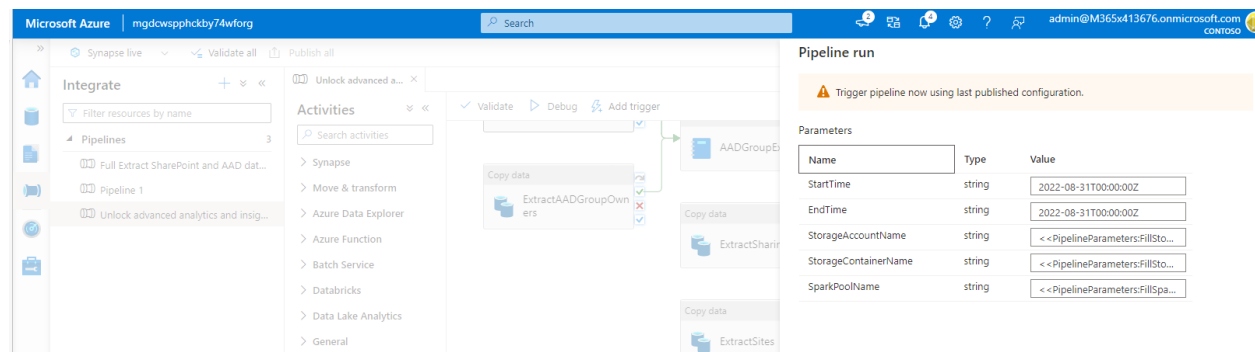
Trigger now

Trigger on-demand run of the last published pipeline

Notebook

SPGroupExpa

## 13. Provide the required parameters. Use the Storage Account, Storage Container and Spark Pool Name created by the pre-req steps above (Note: names are case sensitive)



Microsoft Azure | mgdcwspphckby74wforg

Integrate

Filter resources by name

Pipelines

- Full Extract SharePoint and AAD dat...
- Pipeline 1
- Unlock advanced analytics and insig...

Activities

- Synapse
- Move & transform
- Azure Data Explorer
- Azure Function
- Batch Service
- Databricks
- Data Lake Analytics
- General

Copy data

ExtractAADGroupOwners

Copy data

ExtractSharingInfo

Copy data

ExtractSites

Pipeline run


Trigger pipeline now using last published configuration.


Parameters

Name	Type	Value
StartTime	string	2022-08-31T00:00:00Z
EndTime	string	2022-08-31T00:00:00Z
StorageAccountName	string	<< PipelineParameters.FillSto...
StorageContainerName	string	<< PipelineParameters.FillSto...
SparkPoolName	string	<< PipelineParameters.FillSpa...

14. Congratulations! You just triggered your first MGDC pipeline! Once the admin consents to the request the data will be processed and delivered to your storage account.

15. You will see the data in the storage account.

 Add filter

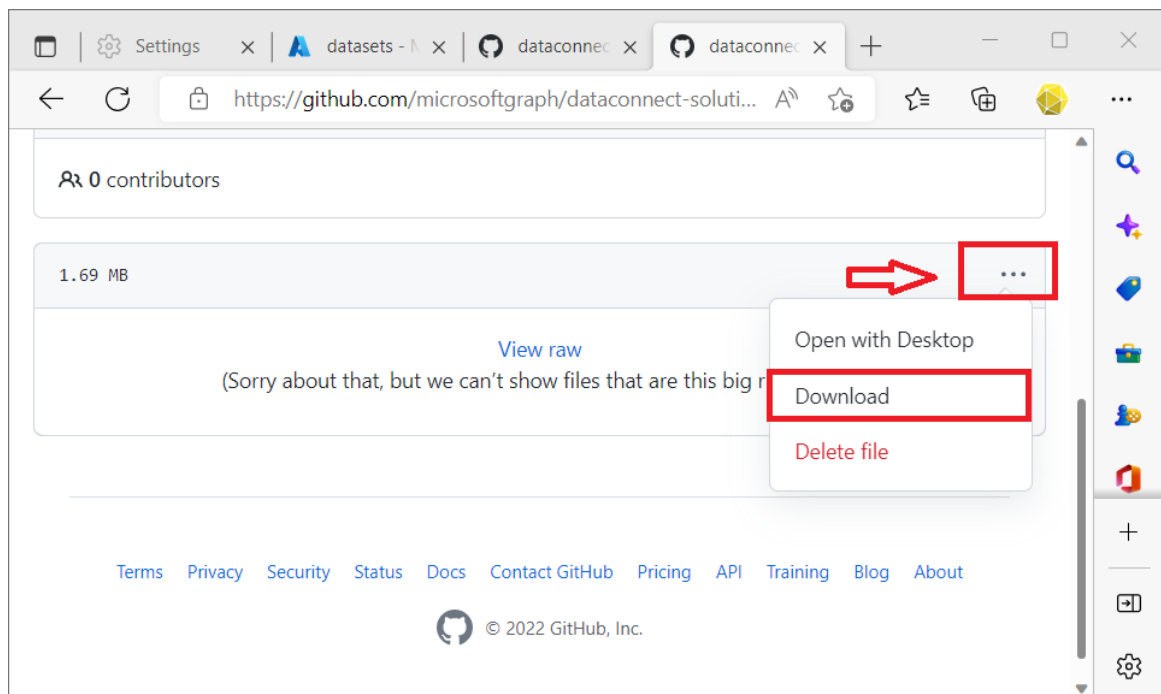
Name	Modified	Access tier	Archive status
<input type="checkbox"/>  groupdetails			
<input type="checkbox"/>  groupmembers			
<input type="checkbox"/>  groupowners			
<input type="checkbox"/>  latest			
<input type="checkbox"/>  sharing			
<input type="checkbox"/>  sites			
<input type="checkbox"/>  spgroups			



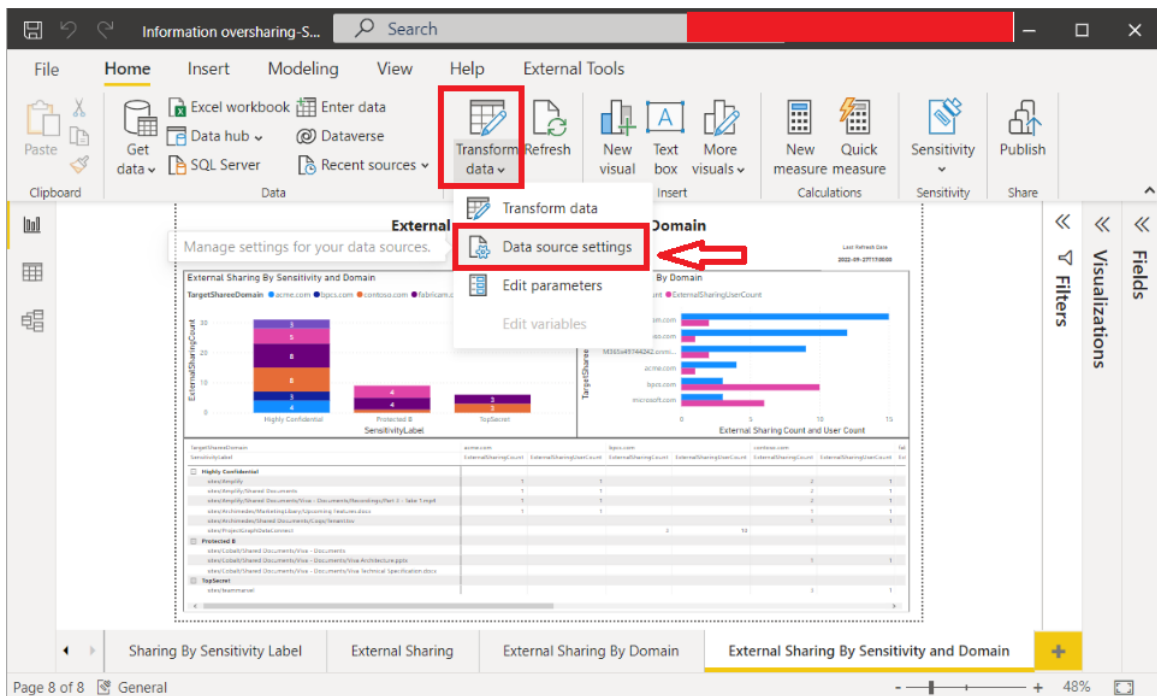
## PBI report template

Below steps will help to link datasets that are generated using Synapse pipeline above to link to PowerBI Template.

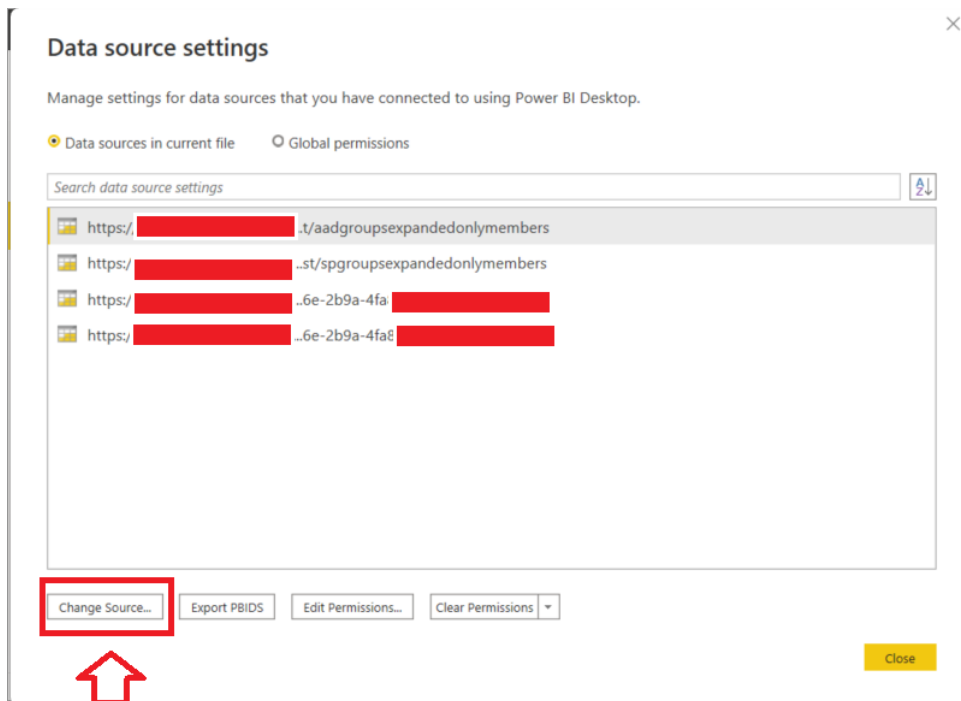
1. Download and install Microsoft Power BI Desktop if you don't have it installed already on your machine.
  - a. Link to download [Download Microsoft Power BI Desktop from Official Microsoft Download Center](#)
2. Download the pre-created PowerBI security report that can generate insights from data that is produced using Synapse pipeline in azure storage locations. Link to download [PowerBI Report](#)



3. Open the PowerBI file and click on Transform data → Data source settings



4. You will see 4 data sources in the Data source settings page.



5. Select one of the data source settings and click on Change Source.
  - a. Change the Storage account path in URL with right storage account that data is generated from synapse pipeline in the steps above. **You can get the storage account that is used in Synapse template pipeline Step 6 above.**

**Azure Data Lake Storage Gen2**

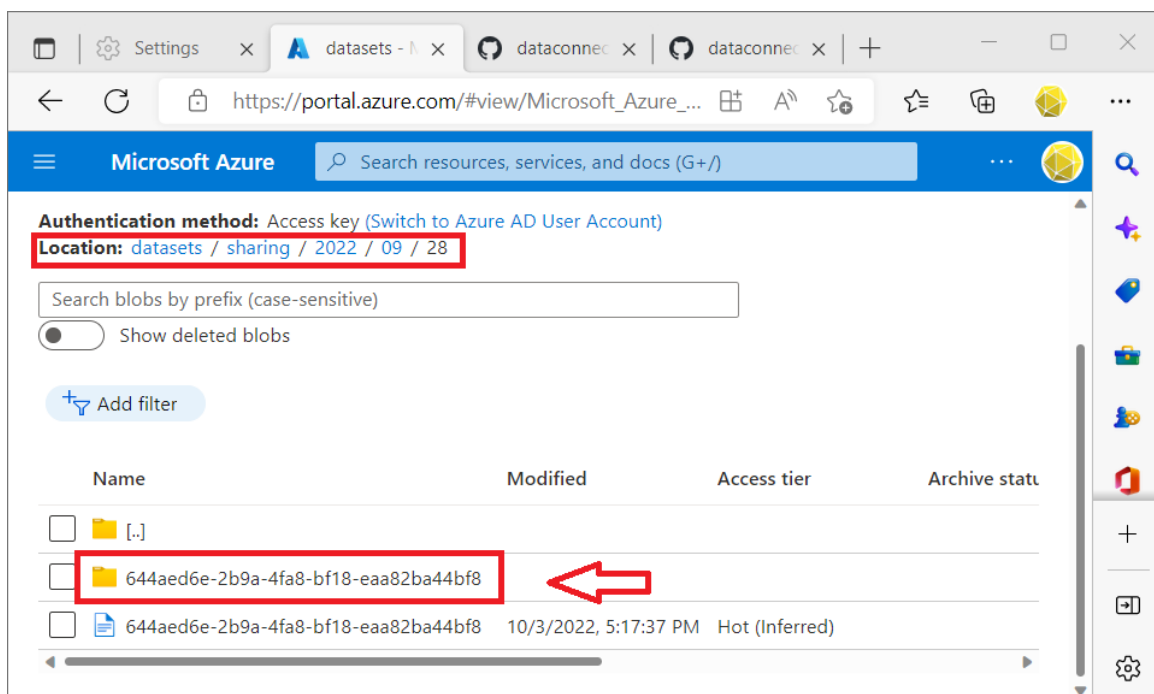
URL  
https://[redacted].dfs.core.windows.net/datasets/latest/aadgroupsexpand

Data View  
☒ File System View   
☐ CDM Folder View (Beta)

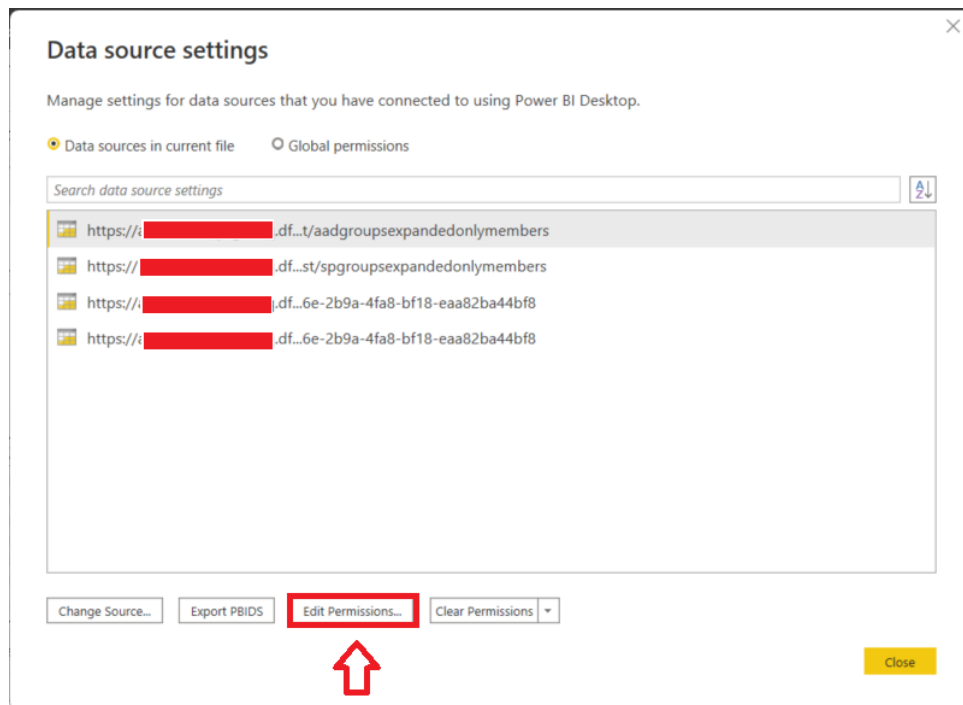
OK Cancel

- b. Repeat changing storage account names to all **4 Data sources in current file.**

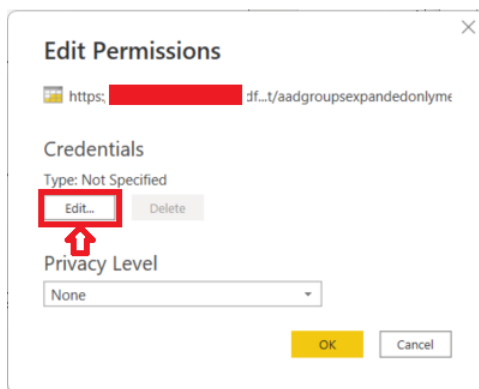
6. Two data sources you need to update the path with right Date and correct GUID values for the data generated for **Sharing** and **Sites** datasets.
- Click on data sources that contain GUID's (Most likely data sources 3 and 4 listed)
  - Change path with right date and GUID Values  
<https://<<StorageAccountName>>.dfs.core.windows.net/datasets/sharing/<<YYYY>>/<<MM>>/<<DD>>/<<GUID>>>
- After changing the paths your new path should be like below  
**<https://xyzabcpqr1234.dfs.core.windows.net/datasets/sharing/2022/10/03/12345678-0000-0000-0000-000000000000>**
- You can get GUID/dates Values by navigating to storage account



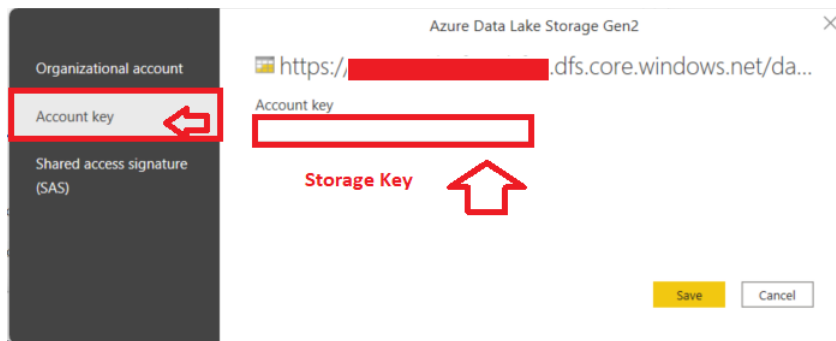
7. Now we need to give the right storage account key / credentials for these data sources.
  - a. Click on Edit Permissions



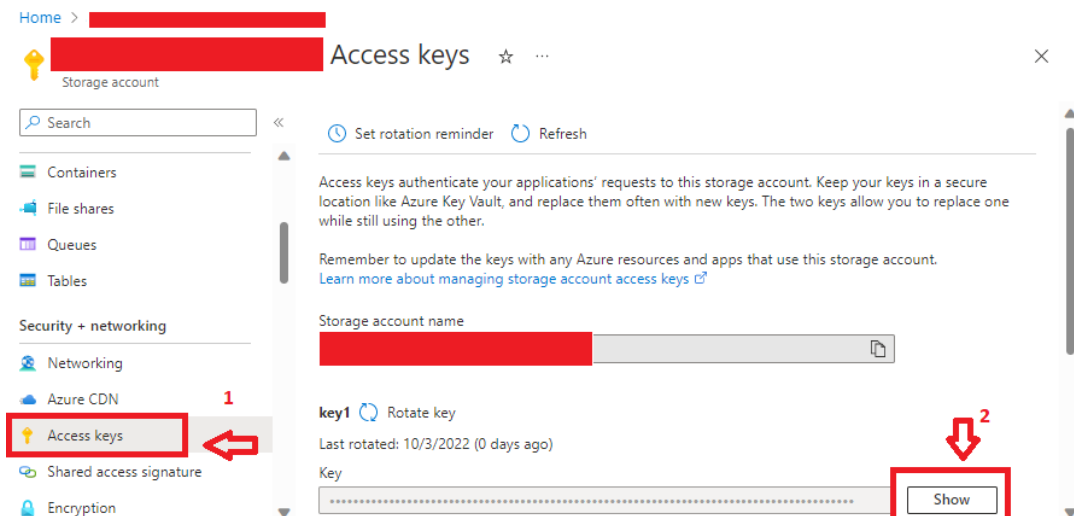
- b. Click on Edit under credentials



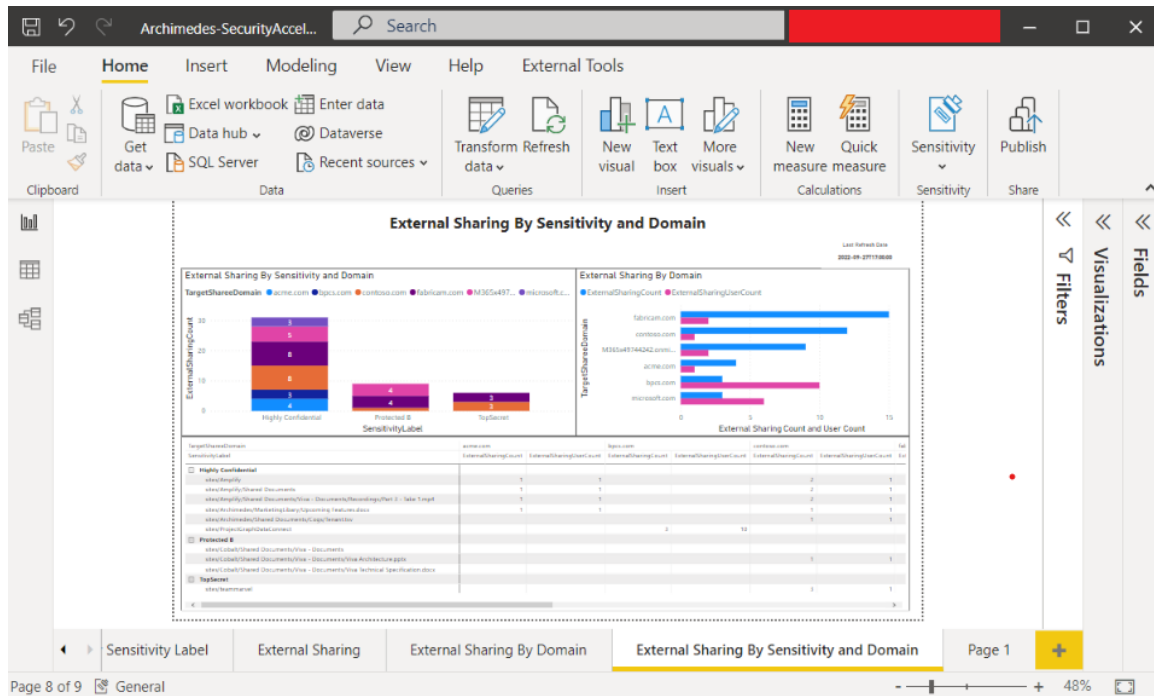
c. Enter the storage account key value.



d. If you don't know have storage key get the storage account key by navigating to storage account in azure portal (storage account → access keys)



8. Congratulations, you are all set and will see that the report will be refreshed with the latest data.



9. If you see any error or data is not being refreshed then please make sure your entered right storage account details, path and GUID information along with credentials in data source settings.