

Azure Synapse Link Setup

How to get data from D365 F&O through Dataverse and Fabric

Last update: September 2024

Version 2.2

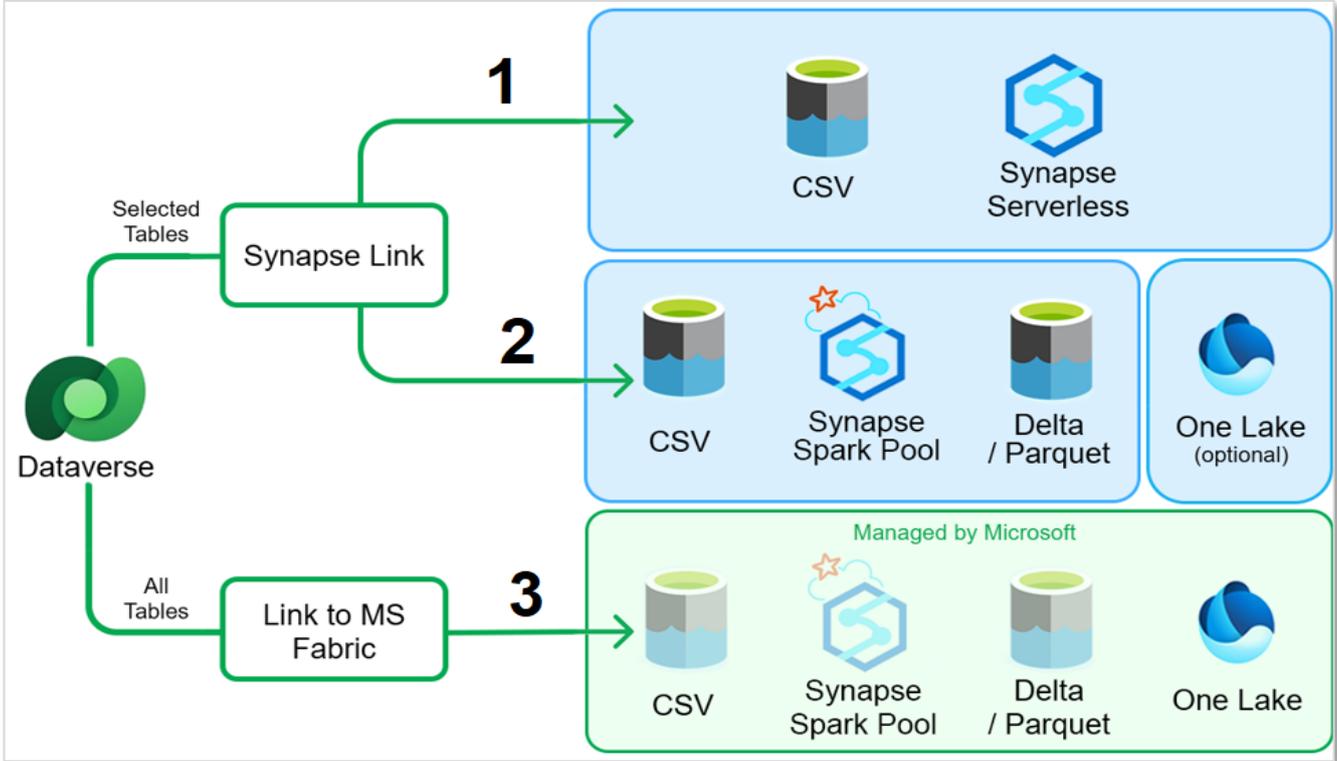
Table of Content

1	Introduction	3
1.1	Architecture	3
1.2	Implementation options comparison.....	3
1.3	Prerequisites (6)	4
1.4	Microsoft Sources	6
2	Setting up Azure Resources	7
2.1	Create a Data Lake Storage (Gen2) Account.....	7
2.2	Add Role Assignments to Data Lake Storage (Gen2) Account	9
2.3	Create Synapse Workspace.....	11
2.4	Assign the role of Synapse Administrator in Synapse Studio.....	12
3	Setting up Azure Synapse Link	13
4	Adding Custom Tables to the Azure Synapse Link.....	16
5	Setting up Application for Metadata Connector	18
5.1	Register an app in Azure Active Directory.....	18
5.2	Add BI4Dynamics Application	19

1 Introduction

1.1 Architecture

D365 Finance and Operations data is not available to external tools due to security and performance reasons. Microsoft is providing the following ETL process options (extract, transform, load) to get data out of D365:



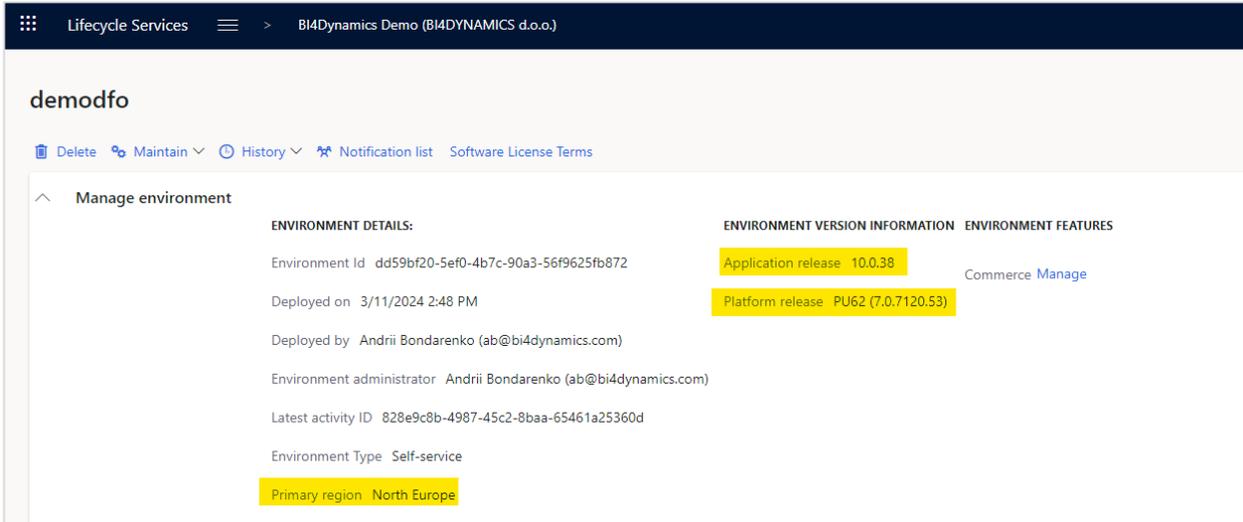
1.2 Implementation options comparison

Option	Data Format	Installation & Management	Cost	Latency
#1: Synapse link	CSV files	The customer manually selects FO tables in Power Apps.	The most economical option is priced at 5\$ per TB of data processed.	Best latency among available options. On-Demand, delay up to 5 minutes.
#2: Synapse link with Spark Pool	Delta / Parquet	The customer manually selects FO tables in Power Apps.	Additional cost for Synapse Spark Pool, which is priced per hour.	Higher latency due to Spark conversion from CSV to Delta/Parquet format. Scheduled in 15 minutes.
#3: Link to MS Fabric	Delta / Parquet in OneLake	All Dataverse tables are selected by Microsoft, FO tables have to be selected manually in Power Apps.	The most expensive option: costs 40\$ per additional GB per month for database storage in Dataverse. Also, requires Fabric Capacity during the processing.	The highest latency due to the conversion process to One Lake. Scheduled in 60 minutes.

1.3 Prerequisites (6)

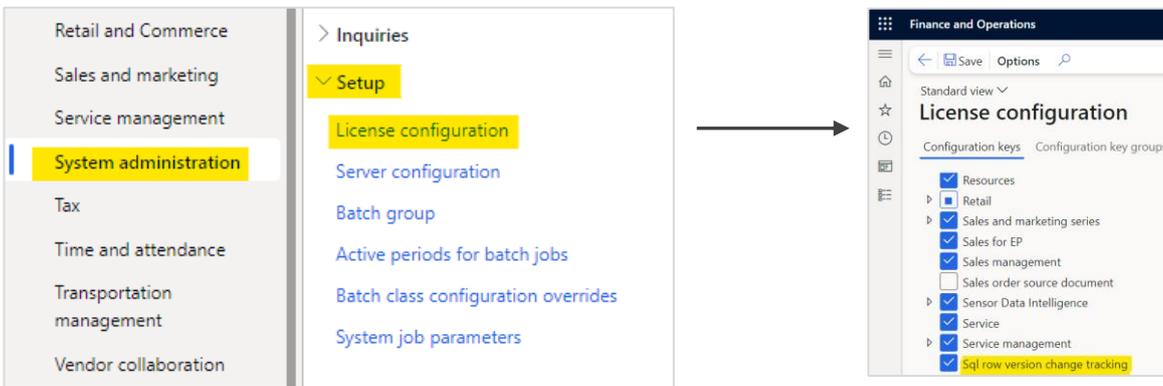
1. The DFO environment must be version 10.0.36 (PU 60) or higher
2. The resources in Azure must be created in **the same region** as your DFO environment
(not applicable for the latest versions of the DFO environment)

The version and primary region can be checked under **Manage environment** in **LifeCycle Services** under **Environment Full Details**:



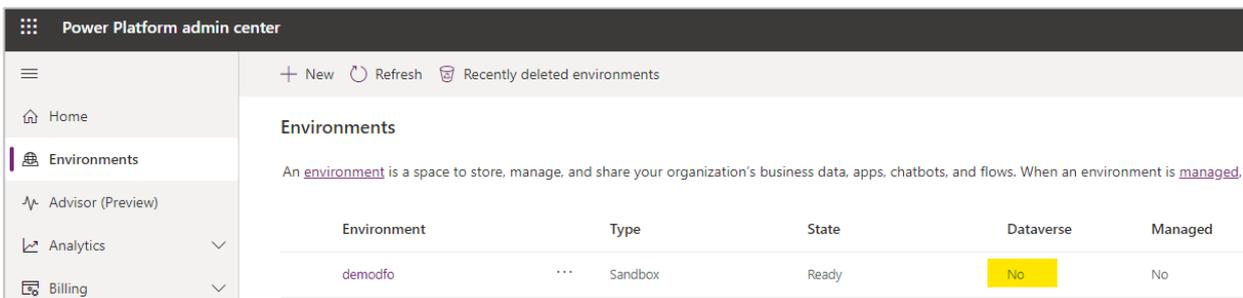
3. SQL row version change tracking property enabled under the License configuration in DFO

Please note that it can be enabled only in the **maintenance mode** during non-working hours. Maintenance mode must be enabled in **LifeCycle Services** under **Environment Full Details**. Once it is done, navigate to the **Finance and Operations license configuration** and enable this property:



4. Dataverse Environment with Power Platform Integration Setup

By default, the environment is created, but it does not have Dataverse capacities enabled:



To enable it, navigate to **Power Platform Integration** in **LifeCycle Services** and click on **Setup**:

Power Platform Integration

Expand your environments capabilities through Power Platform integration. Unlock features such as Dual-write, add-ins and all the capabilities of Microsoft Dataverse.

POWER PLATFORM ENVIRONMENT INFORMATION

Environment name demodfo

Environment Id fe5e5cc6-60b5-e69d-b193-07c926c38057

Status Initial Power Platform environment created. Use the Setup button to add Dataverse capabilities.

Setup

ENVIRONMENT ADD-INS

Power platform environment must be setup to install add-ins.

Select the option **Dynamics 365 standard** and finish the setup:

Power Platform Integration Setup

Use a different Power Platform Environment

No

Template

Dynamics 365 standard

I agree by selecting the template 'Dynamics 365 standard' that this Finance and Operations environment will be connected to a Power Platform environment with Dataverse. Platform solutions for Dual-write and Virtual Entities will also be installed but not enabled. Data will not be written via Dual-write to the Power Platform environment by default, but can be configured to do so as part of a later step.

By selecting any template other than the one mentioned above, data will be synchronized via Dual-write functionality by default. The available template options vary based on the licenses for the tenant which owns this LCS project.

By clicking 'Setup' below, I agree that Power Platform Integration will be enabled and the Finance and Operations environment will be unavailable during this operation.

Once it is done, the setup should be completed, and the **Environment URL** should become available:

Power Platform Integration

Expand your environments capabilities through Power Platform integration. Unlock features such as Dual-write, add-ins and all the capabilities of Microsoft Dataverse.

POWER PLATFORM ENVIRONMENT INFORMATION

Environment name demodfo

Environment Id fe5e5cc6-60b5-e69d-b193-07c926c38057

Environment Uri <https://operations-demodfo.crm4.dynamics.com/>

Status Power Platform environment setup is complete. Features such as Dual-write, add-ins could be installed now.

Setup Dual-write application

Dual-write application will finish installing data entity mappings and configure data for sync across to Microsoft Dataverse. [Learn more](#)

ENVIRONMENT ADD-INS

Also, the **Dataverse** property in the **Power Platform admin center** should change to **Yes**:

Power Platform admin center

+ New Refresh Recently deleted environments

Environments

An **environment** is a space to store, manage, and share your organization's business data, apps, chatbots, and flows. When an environment is **managed**.

Environment	Type	State	Dataverse	Managed
demodfo	Sandbox	Ready	Yes	No

5. Account with Dataverse **system administrator** security role in Dataverse

The System Administrator role is required to create Azure Synapse Link in Power Apps. Account role can be checked under **Settings > User** in the **Environment**:

The screenshot shows the Power Platform admin center interface. The left sidebar contains navigation options: Home, Environments, Advisor (Preview), Analytics, Billing, Resources, and Help + support. The main content area displays the 'Users' page for the 'demodfo' environment. It includes a breadcrumb trail 'Environments > demodfo > Settings > Users', a title 'Manage users so they can access data within their environment. This list includes users with disabled and enabled statuses. [Learn more](#)', and two links: 'Looking for application users? Click here to go to the [app users list](#)' and 'To validate user permissions for specific app(s), go to [app access checker](#)'. Below this is a table of users:

Name ↑	Username	Main phone
Andrii Bondarenko	ab@bi4dynamics.com	

Below the table is a detailed user profile for 'Andrii Bondarenko'. It shows the user's status as 'Enabled', a 'Run diagnostics' button, and a 'Refresh user' button. The 'Summary' section lists the 'User Name' as 'ab@bi4dynamics.com'. The 'Roles' section lists 'System Administrator' (highlighted in yellow) and 'Basic User'. The 'Teams' section lists 'operations-demodfo' and 'Manage teams'.

6. The account must be also:

- **Storage Blob Data Contributor** and **Owner** of the **Azure Storage Account**
- **Owner** and **Synapse Administrator** of the **Synapse Workspace**
- **Reader** on the **Resource Group**

1.4 Microsoft Sources

<https://learn.microsoft.com/en-us/power-apps/maker/data-platform/azure-synapse-link-synapse>

<https://learn.microsoft.com/en-us/power-apps/maker/data-platform/azure-synapse-link-select-fno-data>

2 Setting up Azure Resources

2.1 Create a Data Lake Storage (Gen2) Account

Create a new **Storage Account** in the BI4Dynamics resource group. Make sure that the Storage Account is in the same region as your **DFO Environment**:

The screenshot shows the 'Create a storage account' wizard in the 'Basics' tab. The 'Project details' section shows the subscription as 'Customers POC' and the resource group as 'dataverse'. The 'Instance details' section shows the storage account name as 'bi4dystorage', the region as '(Europe) North Europe', the performance tier as 'Standard', and the redundancy as 'Locally-redundant storage (LRS)'.

Enable **Hierarchical Namespace** and select **Hot Access Tier** in the tab **Advanced**:

The screenshot shows the 'Create a storage account' wizard in the 'Advanced' tab. A message states: 'Certain options have been disabled by default due to the combination of storage account performance, redundancy, and region.' The 'Security' section includes options for 'Require secure transfer for REST API operations' (checked), 'Allow enabling anonymous access on individual containers' (unchecked), 'Enable storage account key access' (checked), 'Default to Microsoft Entra authorization in the Azure portal' (unchecked), 'Minimum TLS version' (Version 1.2), and 'Permitted scope for copy operations (preview)' (From any storage account). The 'Hierarchical Namespace' section has 'Enable hierarchical namespace' checked. The 'Access protocols' section is partially visible.

The screenshot shows the 'Create a storage account' wizard in the 'Advanced' tab. The 'Hierarchical Namespace' section has 'Enable hierarchical namespace' checked. The 'Access protocols' section includes 'Enable SFTP' (unchecked) and 'Enable network file system v3' (unchecked). The 'Blob storage' section has 'Allow cross-tenant replication' (unchecked) and a message: 'Cross-tenant replication and hierarchical namespace cannot be enabled simultaneously.' The 'Access tier' section has 'Hot: Optimized for frequently accessed data and everyday usage scenarios' selected. The 'Azure Files' section has 'Enable large file shares' (unchecked).

Under Networking keep the following selection, while **Recovery** settings can be unchecked:

Home > Storage accounts >

Create a storage account

Basics Advanced **Networking** Data protection Encryption Tags Review

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

- Enable public access from all networks
- Enable public access from selected virtual networks and IP addresses
- Disable public access and use private access

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference ⓘ *

- Microsoft network routing
- Internet routing

Review < Previous Next: Data protection >

Home > Storage accounts >

Create a storage account

Basics Advanced Networking **Data protection** Encryption Tags Review

Recovery

Protect your data from accidental or erroneous deletion or modification.

- Enable point-in-time restore for containers
- Enable soft delete for blobs
- Enable soft delete for containers
- Enable soft delete for file shares

Tracking

Manage versions and keep track of changes made to your blob data.

- Enable versioning for blobs
- Enable blob change feed

Access control

- Enable version-level immutability support

Review < Previous Next: Encryption >

Under Encryption select **Microsoft-managed keys** and **Blobs and files only**. Under Review revise the properties and create a storage account:

Home > Storage accounts >

Create a storage account

Basics Advanced Networking Data protection **Encryption** Tags Review

Encryption type * ⓘ

- Microsoft-managed keys (MMK)
- Customer-managed keys (CMK)

Enable support for customer-managed keys ⓘ

- Blobs and files only
- All service types (blobs, files, tables, and queues)

Enable infrastructure encryption ⓘ

Review < Previous Next: Tags >

Home > Storage accounts >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags **Review**

Basics

Subscription	Customers POC
Resource Group	dataverse
Location	northeurope
Storage account name	bi4dynstorage
Deployment model	Resource manager
Performance	Standard
Replication	Locally-redundant storage (LRS)

Advanced

Enable hierarchical namespace	Enabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot
Enable SFTP	Disabled
Large file shares	Disabled

Networking

Network connectivity	Public endpoint (all networks)
Default routing tier	Microsoft network routing
Endpoint type	Standard

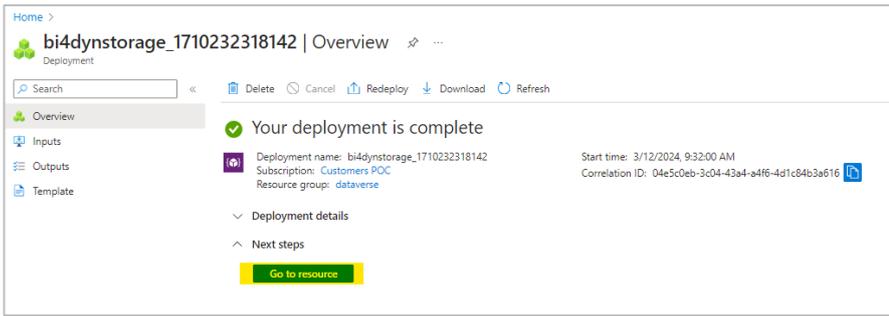
Security

Secure transfer	Enabled
Allow storage account key access	Enabled
Default to Microsoft Entra authorization in the Azure portal	Disabled
Blob anonymous access	Disabled
Minimum TLS version	Version 1.2
Permitted scope for copy operations (preview)	From any storage account

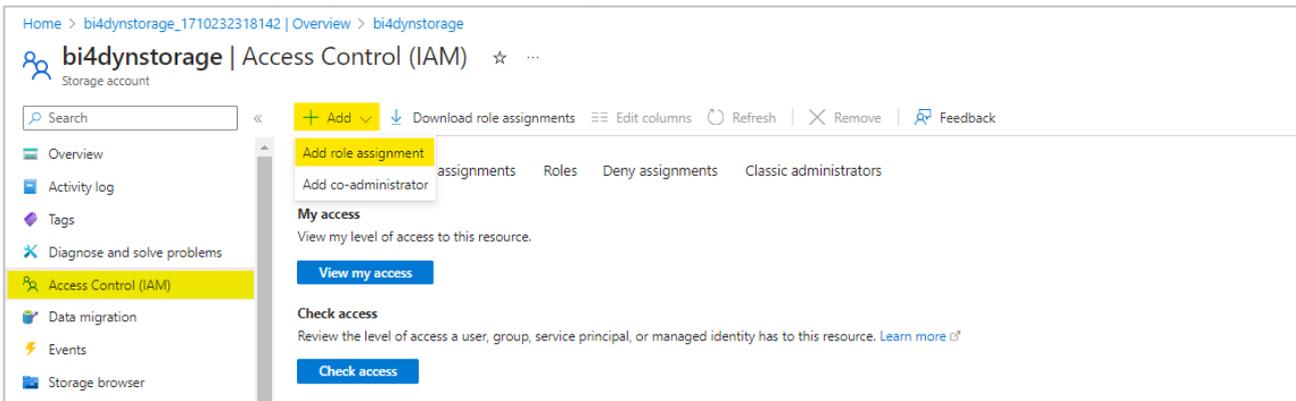
Create < Previous Next > [Download a template for automation](#)

2.2 Add Role Assignments to Data Lake Storage (Gen2) Account

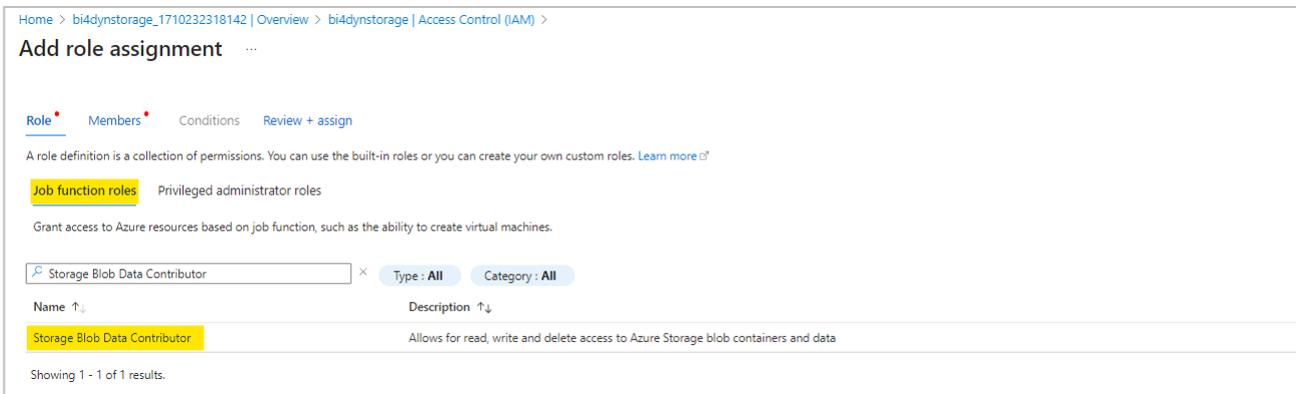
Once the resource is deployed, go to Storage Account:



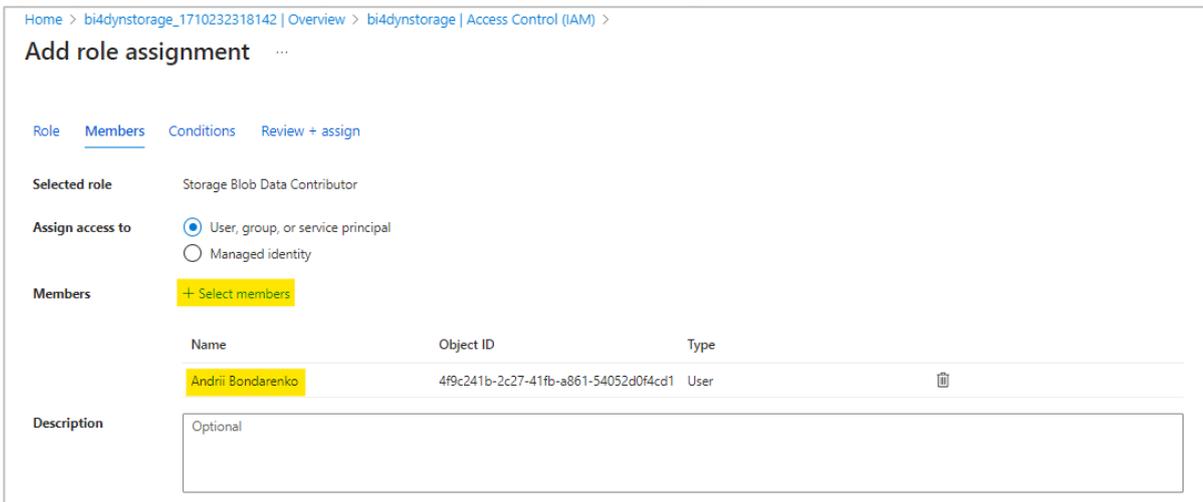
Under **Access Control (IAM)**, select **Add role assignment**:



Assign BI4Dynamics account with the role of **Storage Blob Data Contributor**:



Specify the user with the option **Select members** and assign the role:



Two roles cannot be assigned at the same time in Azure Portal. That is why similar actions should be performed for the role of **Owner**:

Home > bi4dynstorage_1710232318142 | Overview > bi4dynstorage | Access Control (IAM) >

Add role assignment

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles **Privileged administrator roles**

Grant privileged administrator access, such as the ability to assign roles to other users.

⚠ Can a job function role with less access be used instead?

Owner × Type: All Category: All

Name ↑↓	Description ↑↓
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.

Showing 1 - 1 of 1 results.

Once the role is selected, add the user:

Home > bi4dynstorage_1710232318142 | Overview > bi4dynstorage | Access Control (IAM) >

Add role assignment

Role Members Conditions Review + assign

Selected role Owner

Assign access to User, group, or service principal
 Managed identity

Members **+ Select members**

Name	Object ID	Type
Andrii Bondarenko	4f9c241b-2c27-41fb-a861-54052d0f4cd1	User

Description Optional

To assign the role of **Owner** conditions should be specified. As the user will not be assigning any additional roles for the resource, the second or third option can be used to avoid creating specific conditions for the role:

Home > bi4dynstorage_1710232318142 | Overview > bi4dynstorage | Access Control (IAM) >

Add role assignment

Role Members Conditions Review + assign

Selected role Owner

What user can do Allow user to only assign selected roles to selected principals (fewer privileges) ⓘ
 Allow user to assign all roles except privileged administrator roles Owner, UAA, RBAC (Recommended) ⓘ
 Allow user to assign all roles (highly privileged) ⓘ

Condition ⓘ

Preconfigured (All roles except privilege built-in roles)

Exclude roles:
Owner, User Access Administrator, Role Based Access Control Administrator

2.3 Create Synapse Workspace

Create a new **Synapse Workspace** in the same resource group and region as your **Dataverse Environment**. Under **Select Data Lake Storage (Gen2) Account**, select the **account** created in a previous step and specify a new file system name as **bi4dcontainer**. In the tab **Security**, create a password for the **SQL Server admin login** and save it.

Home > Azure Synapse Analytics > Create Synapse workspace

* Basics * Security Networking Tags Review + create

Create a Synapse workspace to develop an enterprise analytics solution in just a few clicks.

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

Subscription *

Resource group *

Managed resource group

Workspace details
Name your workspace, select a location, and choose a primary Data Lake Storage Gen2 file system to serve as the default location for logs and job output.

Workspace name *

Region *

Select Data Lake Storage Gen2 * From subscription Manually via URL

Account name *

File system name *

Information: We will automatically grant the workspace identity data access to the specified Data Lake Storage Gen2 account, using the **Storage Blob Data Contributor** role. To enable other users to use this storage account after you create your workspace, perform these tasks:

- Assign other users to the **Contributor** role on workspace
- Assign other users the appropriate **Synapse RBAC roles** using Synapse Studio
- Assign yourself and other users to the **Storage Blob Data Contributor** role on the storage account

Review + create < Previous Next Security >

Home > Create Synapse workspace

* Basics * Security Networking Tags Review + create

Configure security options for your workspace.

Authentication
Choose the authentication method for access to workspace resources such as SQL pools. The authentication method can be changed later on. [Learn more](#)

Authentication method Use both local and Microsoft Entra ID authentication Use only Microsoft Entra ID authentication

SQL Server admin login *

SQL Password

Confirm password

System assigned managed identity permission
Select to grant the workspace network access to the Data Lake Storage Gen2 account using the workspace system identity. [Learn more](#)

Allow network access to Data Lake Storage Gen2 account.

Workspace encryption
Double encryption configuration cannot be changed after opting into using a customer-managed key at the time of workspace creation.

Choose to encrypt all data at rest in the workspace with a key managed by you (customer-managed key). This will provide double encryption with encryption at the infrastructure layer that uses platform-managed keys. [Learn more](#)

Double encryption using a customer-managed key Enable Disable

Review + create < Previous Next Networking >

Under the properties on the **Networking** tab, select the option **Allow connections from all IP addresses**.

Home > Create Synapse workspace

* Basics * Security Networking Tags Review + create

Configure networking options for your workspace.

Managed virtual network
Choose whether to set up a dedicated Azure Synapse-managed virtual network for your workspace. [Learn more](#)

Managed virtual network Enable Disable

Firewall rules
Azure Synapse Studio and other client tools will only connect to the workspace endpoints if this setting is selected. Connections from specific IP addresses or all Azure services can be allowed or disallowed after the workspace is provisioned.

Allow connections from all IP addresses to your workspace's endpoints. You can restrict these permissions to just Azure datacenter IP addresses and/or specific IP address ranges after creating the workspace.

Allow connections from all IP addresses

Encrypted connections
Azure Synapse Analytics applies TLS1.2 encryption protocol for all network connections. [Learn more](#)

Minimum TLS version

Review + create < Previous Next Tags >

Home > Azure Synapse Analytics > Create Synapse workspace

Validation succeeded

* Basics * Security Networking Tags Review + create

Product Details
Azure Synapse Analytics workspace by Microsoft **4.68 EUR**

Terms
By clicking Create, I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. For additional details see [Azure Marketplace Terms](#).

Basics

Subscription	Customers POC
Resource group	dataverse
Region	North Europe
Workspace name	(new) bi4dmysynapse
Data Lake Storage Gen2 account	https://bi4dmystorage.dfs.core.windows.net
Data Lake Storage Gen2 file system	(new) bi4dcontainer
Managed resource group	None
Role assignments	The Storage Blob Data Contributor role will be assigned on the specified Data Lake Storage Gen2 account to the workspace managed identity.

Security

Authentication method	Use both local and Microsoft Entra ID authentication
SQL Server admin login	sqladminuser
SQL Password	*****
Double encryption	No

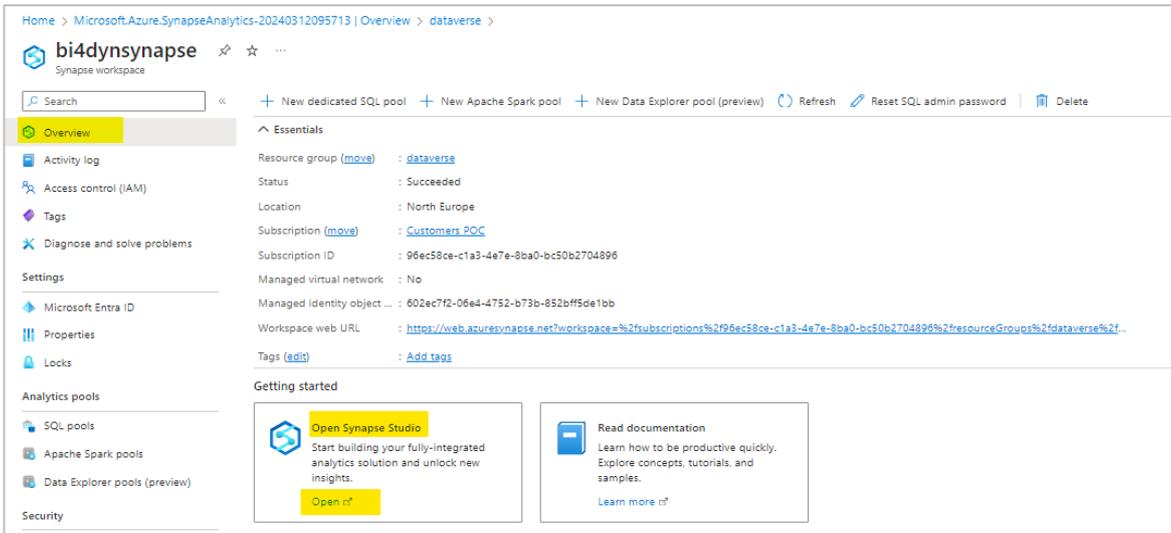
Networking

Managed virtual network	No
Allow connections from all IP addresses	Yes

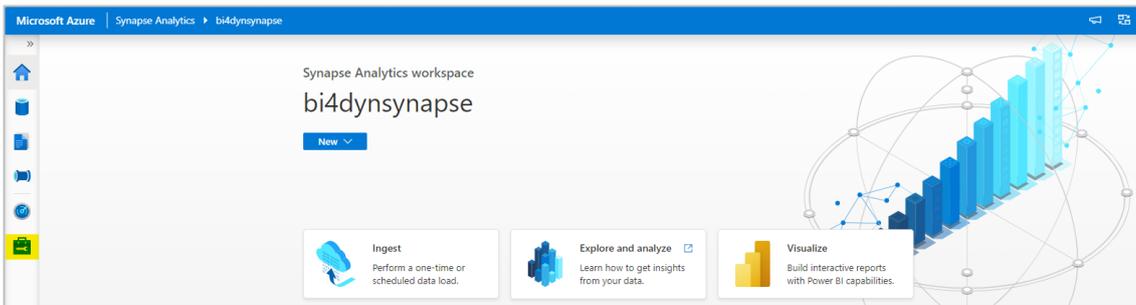
Create < Previous Next > [Download a template for automation](#)

2.4 Assign the role of Synapse Administrator in Synapse Studio

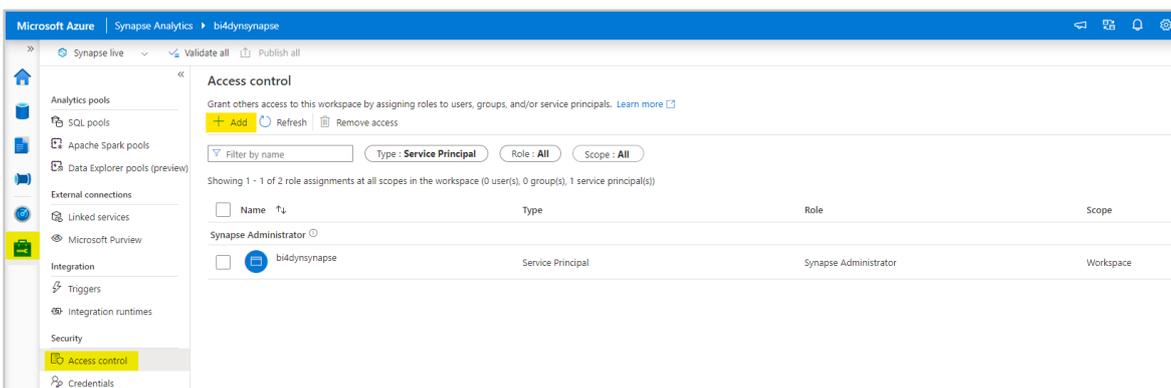
Navigate to **Overview** of Synapse Workspace and open **Synapse Studio**:



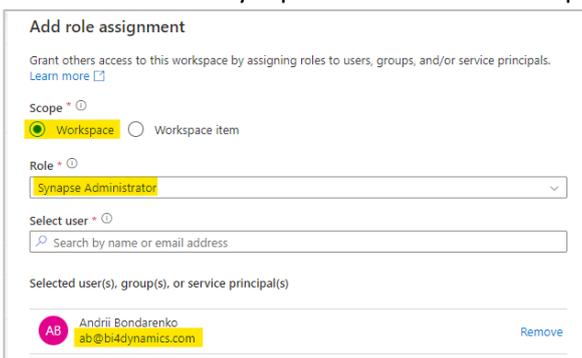
Synapse Studio will open in a separate window. Navigate to the tab **Manage** on the left side of the screen:



Select **Access Control** and click on **Add**:

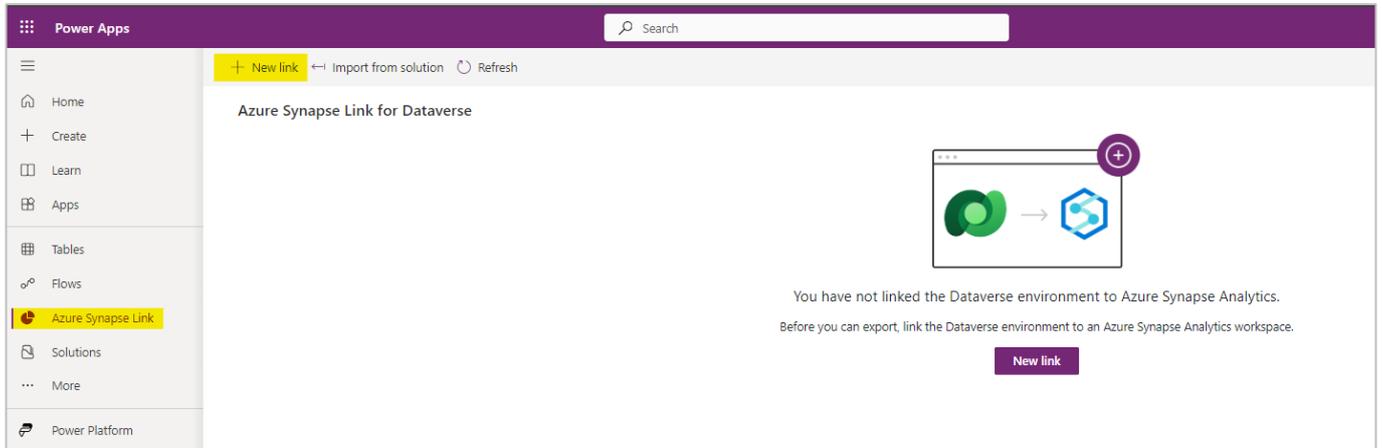


Select the roles of Synapse Administrator and specify the user:



3 Setting up Azure Synapse Link

Navigate to **Power Apps** and select **Azure Synapse Link**.

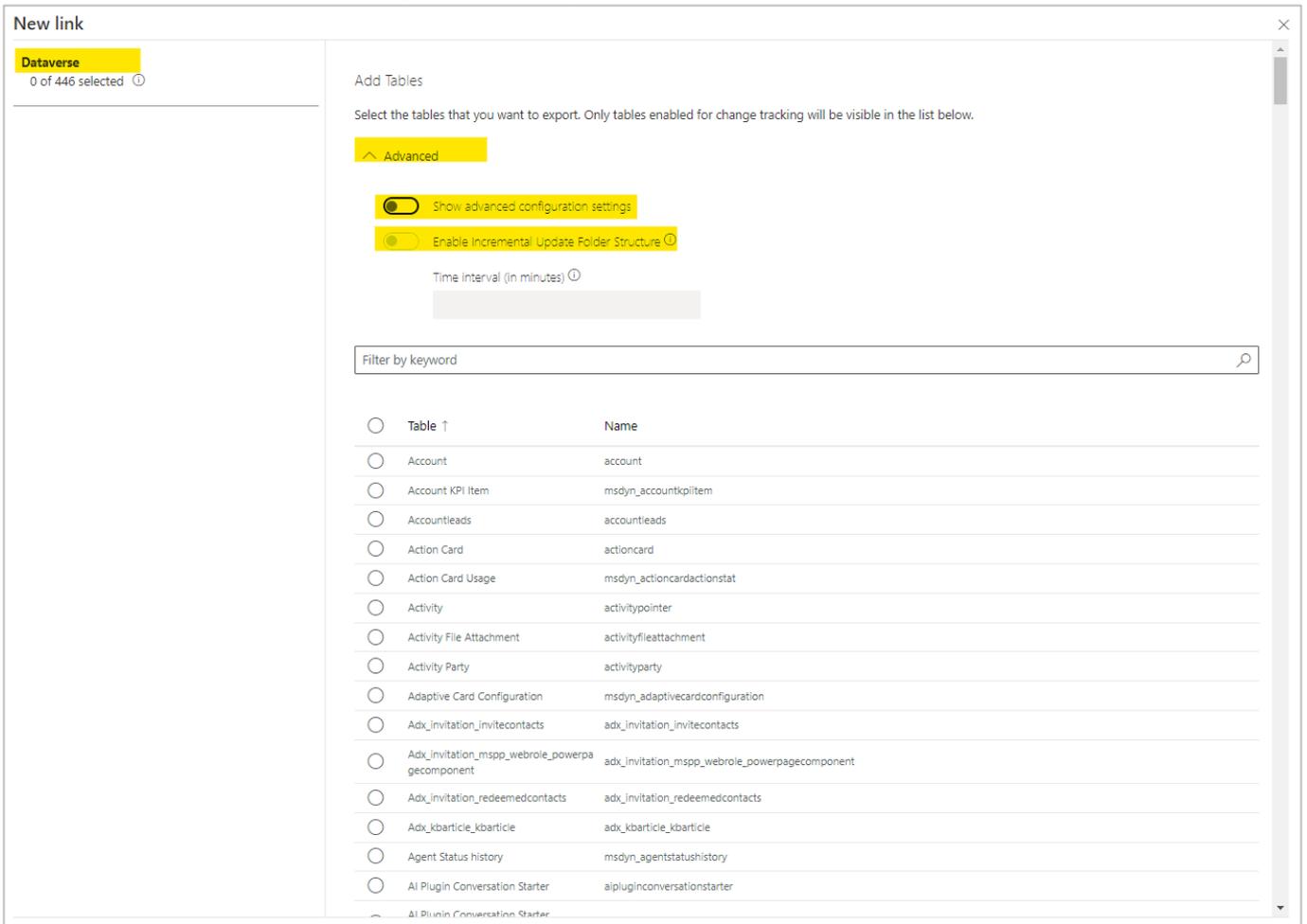


Set up a new link with the resources created in the previous chapter and click on **Next**:

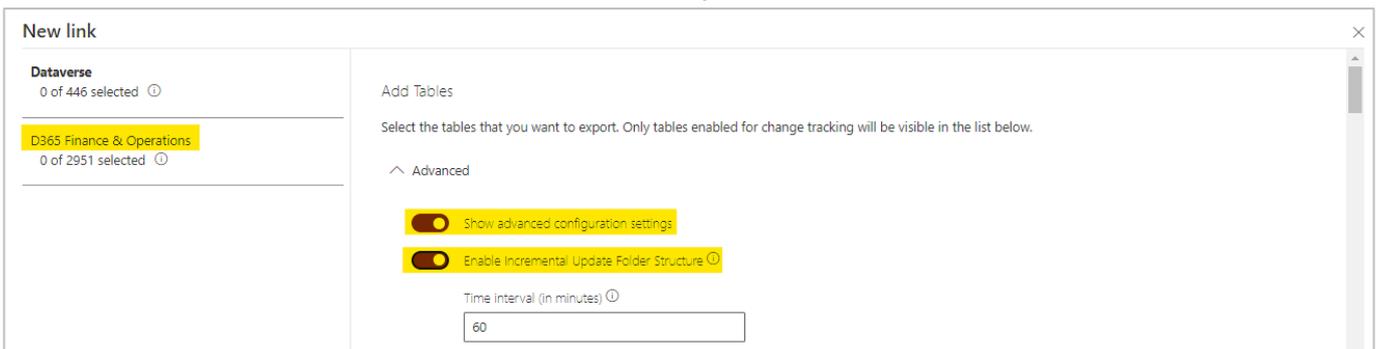
The 'New link' dialog is shown with the following configuration:

- Select Azure resource** (selected)
- Add Tables** (unselected)
- Select Azure resource** (Section header)
- Select the storage account and Azure Synapse workspace that you want link to the Dataverse environment. The storage account and Azure Synapse workspace must be in the same geography as your environment.**
- Your environment is located in: North Europe within the Azure geography: Europe**
- For optimal performance, we recommend attaching your Azure resource within the same region, preferably in one of the following location(s): North Europe**
- You may choose to attach your Azure resource within the same geography as your Dataverse environment: Europe. For more details on Azure geographies, click here.**
- Connect to your Azure Synapse Analytics workspace**
- Subscription ***: Microsoft Azure Sponsorship 1
- Resource group ***: DataverseSynapseLink
- Storage account ***: bi4dynstorage
- Select Enterprise Policy with Managed Service Identity**
- As part of linking the Dataverse environment to a data lake, you are granting the Azure Synapse Link service additional roles to your storage account. By using the Azure Synapse Link service, you agree that data may go outside of Power Apps' compliance boundary.**
- [For more information, see the Privacy Notice in the technical documentation for the service.](#)
- Buttons:** Back, Next (highlighted), Cancel

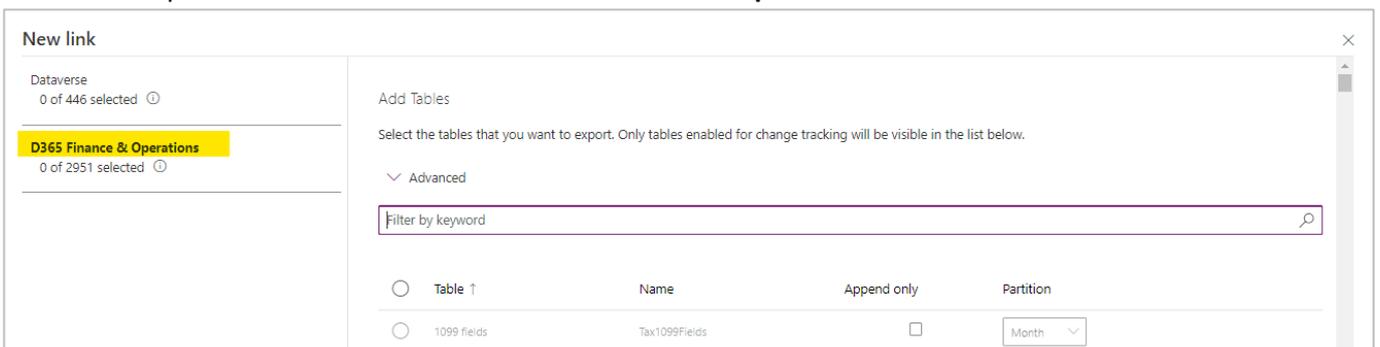
By default, only tables from Dataverse are available. Extend the option **Advanced** under the Dataverse and check the boxes on **Show advanced configuration settings** and **Enable Incremental Update Folder Structure**:



Once boxes are checked, the tab on the **D365 Finance & Operations** tables will be visible:



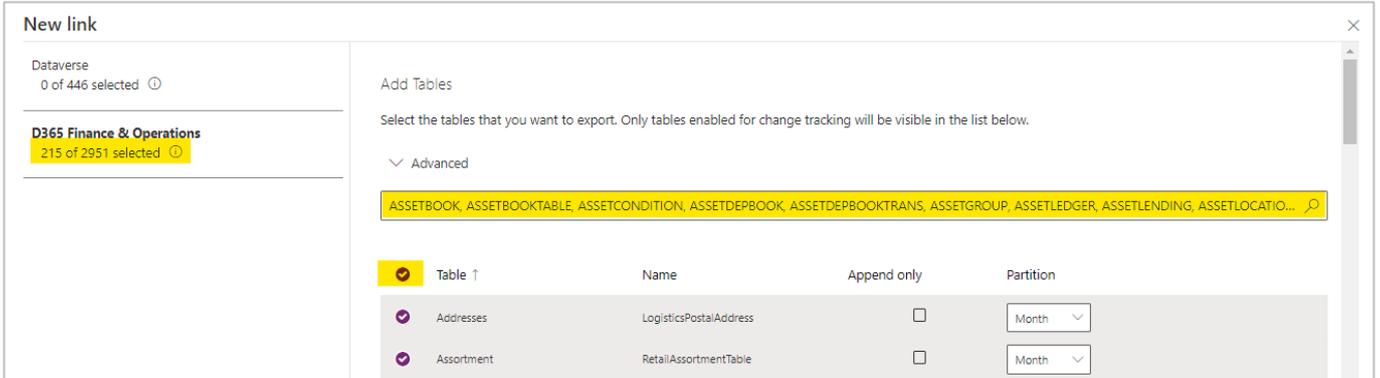
Click on this option to select the tables from **D365 Finance & Operations**:



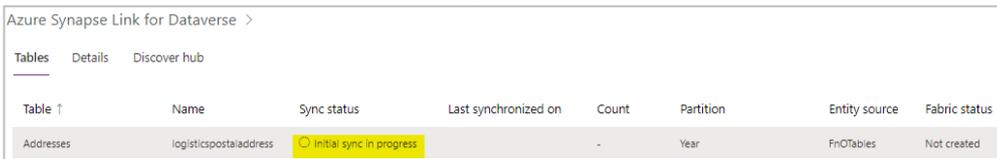
Copy the tables for export under **D365 Finance & Operations** from the attached list: [List of Tables](#)

These tables are used by BI4Dynamics solution to recreate the standard model in our Data Warehouse. In total, **up to 220 tables** should be selected from the solution (some tables might not be available in newer versions of FO).

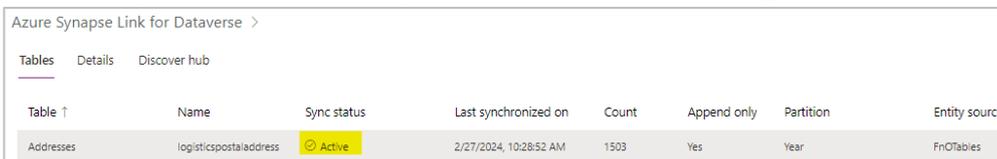
Leave the columns **Append Only** and **Partition** under the default setup as they will be automatically updated. **Append only** will be **checked** and **Partition** will be changed to **Year** for the FO tables right after creating the link.



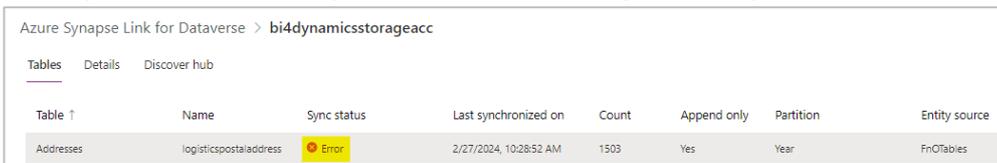
Once the selection is saved, the Initial synchronization will start:



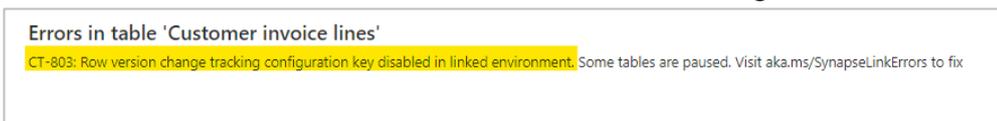
When the synchronization is completed, the status should change to Active:



If the synchronization fails, you will see the following icon on Sync status:



For the error details click on the icon. The detailed Error message will be shown:



For more details on the error message and its resolution, the following link can be used:

<https://learn.microsoft.com/en-us/power-apps/maker/data-platform/azure-synapse-link-troubleshooting-guide>

4 Adding Custom Tables to the Azure Synapse Link

Custom FO tables are not visible by default in Azure Synapse Link. Based on the official Microsoft documentation, custom tables require row version change tracking enabled manually:

Known limitations with finance and operations tables

Currently, there are limitations with finance and operations tables and Azure Synapse Link. We're working to address these limitations. To learn more about the upcoming roadmap and stay in touch with the product team, join the [preview Viva Engage group](#).

- You must create a new Azure Synapse Link profile. You can't add finance and operations apps tables to existing Azure Synapse Link profiles.
- Don't see all tables? Up to 2,750 Microsoft provided finance and operations apps tables are already enabled in Azure Synapse Link with application version 10.0.38. If you have a previous version of finance and operations apps, not all required tables can be enabled by default. You can enable more tables yourself by extending table properties and enabling the change tracking feature. For more information about how to enable change tracking, see [Enable row version change tracking for tables](#).
- **Don't see your custom tables? You must enable change tracking for them. More information: [Enable row version change tracking for tables](#). If you're using a cloud hosted environment (CHE), you must perform a database sync operation to reflect the changes.**
- You can select a maximum of 1,000 tables in an Azure Synapse Link profile. To enable more tables, create another Azure Synapse Link profile.
- If the table selected contains data columns that are secured via **AOS Authorization**, those columns are ignored and the exported data doesn't contain the column. For example in a custom table named *CustTable*, the column *TaxLicenseNum* has the metadata property **AOS Authorization** set to **Yes**. This column is ignored when *CustTable* data is exported with Azure Synapse Link.

In particular, the property **Allow Row Version Change Tracking** of the table has to be changed to **Yes**:

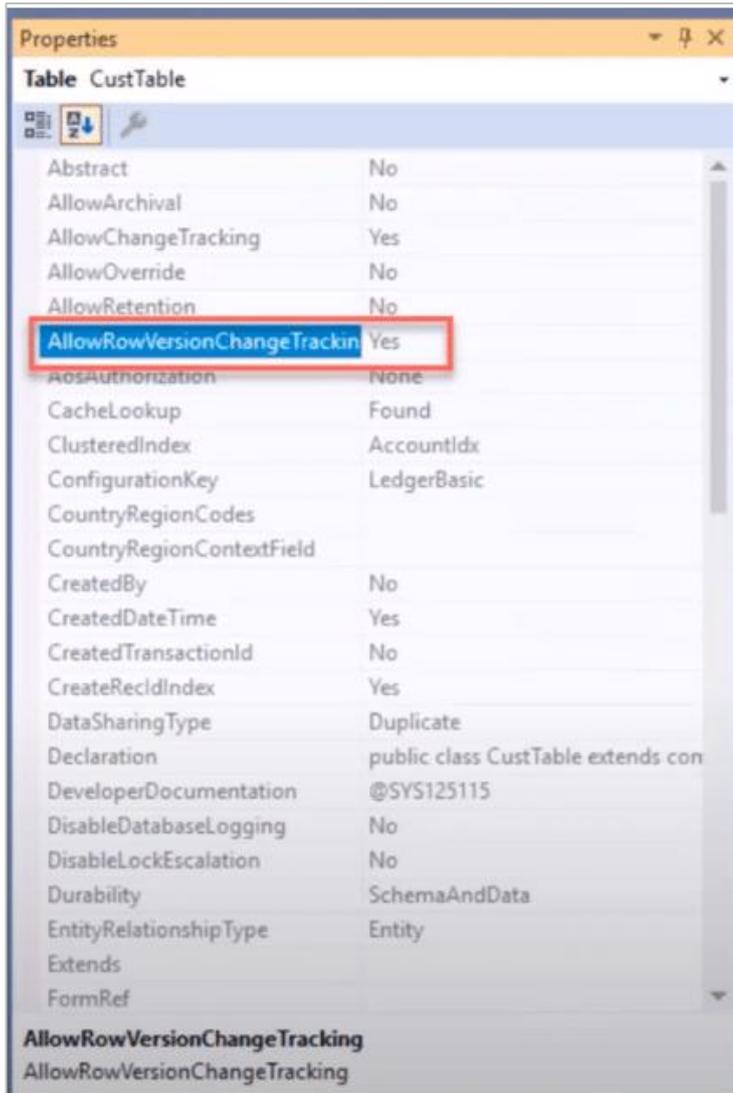
Enable row version change tracking for tables

To enable row version change tracking for a table, set the **Allow Row Version Change Tracking** property of the table to **Yes**. The table then gets a new system field of the **rowversion** type that's named **SysRowVersion**.

Note

Before version 10.0.34, while row version change tracking functionality was in preview, the row version column was named **SysRowVersionNumber**. In version 10.0.34, the **SysRowVersionNumber** column was replaced with a new **SysRowVersion** column. The **SysRowVersionNumber** column is now obsolete. In version 10.0.39, it's removed from the metadata of out-of-box tables. Don't make any dependencies for the **SysRowVersionNumber** column. If your code has a dependency on the older **SysRowVersionNumber** column, you are required to remove the dependency and test 10.0.39 in your sandbox environment before upgrading your production instance to 10.0.39.

The change is made in the table metadata accessed through Visual Studio.
The developer team or Microsoft partner should be engaged.



Please note that Synapse Link does not currently support derived columns in the FO tables. To get the data from a derived column, the base table for this column needs to be additionally selected in Azure Synapse Link:

- Table inheritance and derived tables are concepts in finance and operations apps. When choosing a derived table from finance and operations apps, fields from the corresponding base table currently aren't included. For example, if you choose `DirPerson` table, a table derived from `DirPartyTable` also known as the base table, exported data contains fields from the base table `DirPartyTable`. You need to select the base table in addition to the derived table if you need access to these fields. You can use this FastTrack solution [provided on GitHub](#). This solution creates views, which include columns from base tables.

5 Setting up Application for Metadata Connector

Metadata connector is used to get database metadata (AOT) directly from **D365 Finance and Operations**. With the connector, the BI4Dynamics application will be able to know the structure and properties of the database such as:

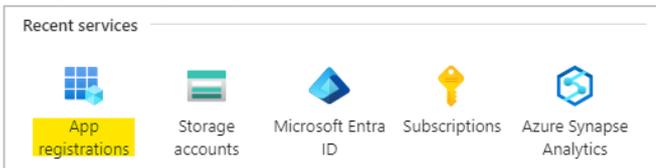
- list of tables and enums available in FO
- relationship between the tables
- profile, length, and type of each field in the tables

RecID	Profile	Table	TableName	Field	FieldName	FieldType	FieldLen	Data TypeName	FieldsDescription	EnumID	RelationTable	RelationTableName	RelationField	RelationFieldName
1	516528	1	1449	VENDINVOICEJOUR	61455	SYSSHARINGDATAAREID	UserType	100	String	1	-1	0	0	
2	516531	1	1449	VENDINVOICEJOUR	61458	SYSTARGETSCALEUNITID	UserType	100	String	1	-1	0	0	
3	516515	1	1449	VENDINVOICEJOUR	61442	MODIFIEDBY	UserType	100	String	1	-1	0	0	
4	516530	1	1449	VENDINVOICEJOUR	61457	SYSSCALEUNITID	UserType	100	String	1	-1	0	0	
5	516521	1	1449	VENDINVOICEJOUR	61448	DATAAREID	UserType	100	String	1	-1	0	0	
6	516519	1	1449	VENDINVOICEJOUR	61446	CREATEDBY	UserType	100	String	1	-1	0	0	
7	516438	1	1449	VENDINVOICEJOUR	70	NUMBERSEQUENCEGROUP	UserType	100	String	1	-1	0	0	
8	516442	1	1449	VENDINVOICEJOUR	75	PARMID	UserType	100	String	1	-1	0	0	
9	516443	1	1449	VENDINVOICEJOUR	76	PAYMDAYID	UserType	100	String	1	-1	0	0	
10	516444	1	1449	VENDINVOICEJOUR	77	PAYMENT	UserType	100	String	1	-1	0	0	
11	516445	1	1449	VENDINVOICEJOUR	78	PAYMENTSCHED	UserType	100	String	1	-1	0	0	
12	516447	1	1449	VENDINVOICEJOUR	80	POSTINGPROFILE	UserType	100	String	1	-1	0	0	
13	516452	1	1449	VENDINVOICEJOUR	85	PURCHID	UserType	100	String	1	-1	0	0	
14	516437	1	1449	VENDINVOICEJOUR	69	NUMBERSEQUENCECODE_LT	UserType	100	String	1	-1	0	0	
15	516370	1	1449	VENDINVOICEJOUR	73	ORDERACCOUNT	UserType	100	String	1	-1	0	0	
16	516439	1	1449	VENDINVOICEJOUR	71	OFFSESSIONID_RU	UserType	100	String	1	-1	0	0	
17	516457	1	1449	VENDINVOICEJOUR	90	RETURNITEMNUM	UserType	100	String	1	-1	0	0	
18	516480	1	1449	VENDINVOICEJOUR	114	VATNUM	UserType	100	String	1	-1	0	0	
19	516484	1	1449	VENDINVOICEJOUR	118	VENDGROUP	UserType	100	String	1	-1	0	0	

This information allows creating the customizations in the BI4Dynamics application only with a couple of clicks.

5.1 Register an app in the Azure Active Directory

Navigate to App Registrations:



Register a new application with **Any Azure AD Directory - Multitenant** account type:

Home > App registrations >

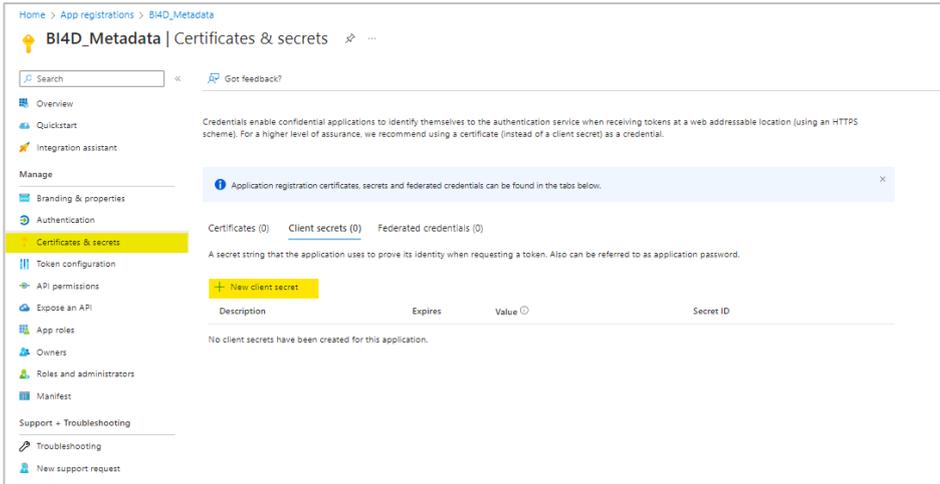
Register an application

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

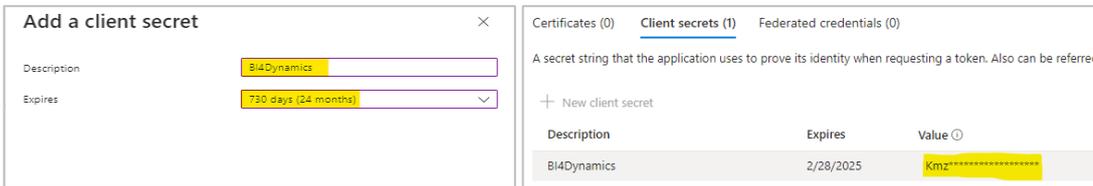
Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (BI4DYNAMICS d.o.o. only - Single tenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - 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:

Navigate to **Certificates & secrets** and create a new **Client Secret**:



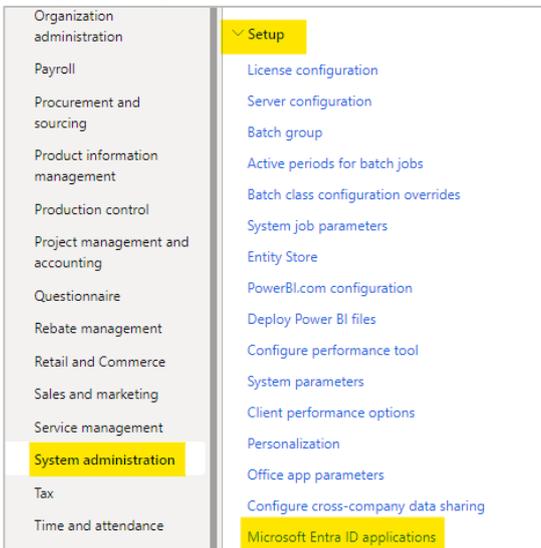
Set the expiration to 730 days. Copy and save the **Value of the Client Secret**:



The secret Value of the application is visible only immediately after the creation. Do not forget to **copy and save** it before leaving Azure Portal.

5.2 Add BI4Dynamics Application

Navigate to **System Administration > Setup > Microsoft Entra ID applications**.



Register a new application and insert the **Client ID** and **Name** of the app created in the previous step.

