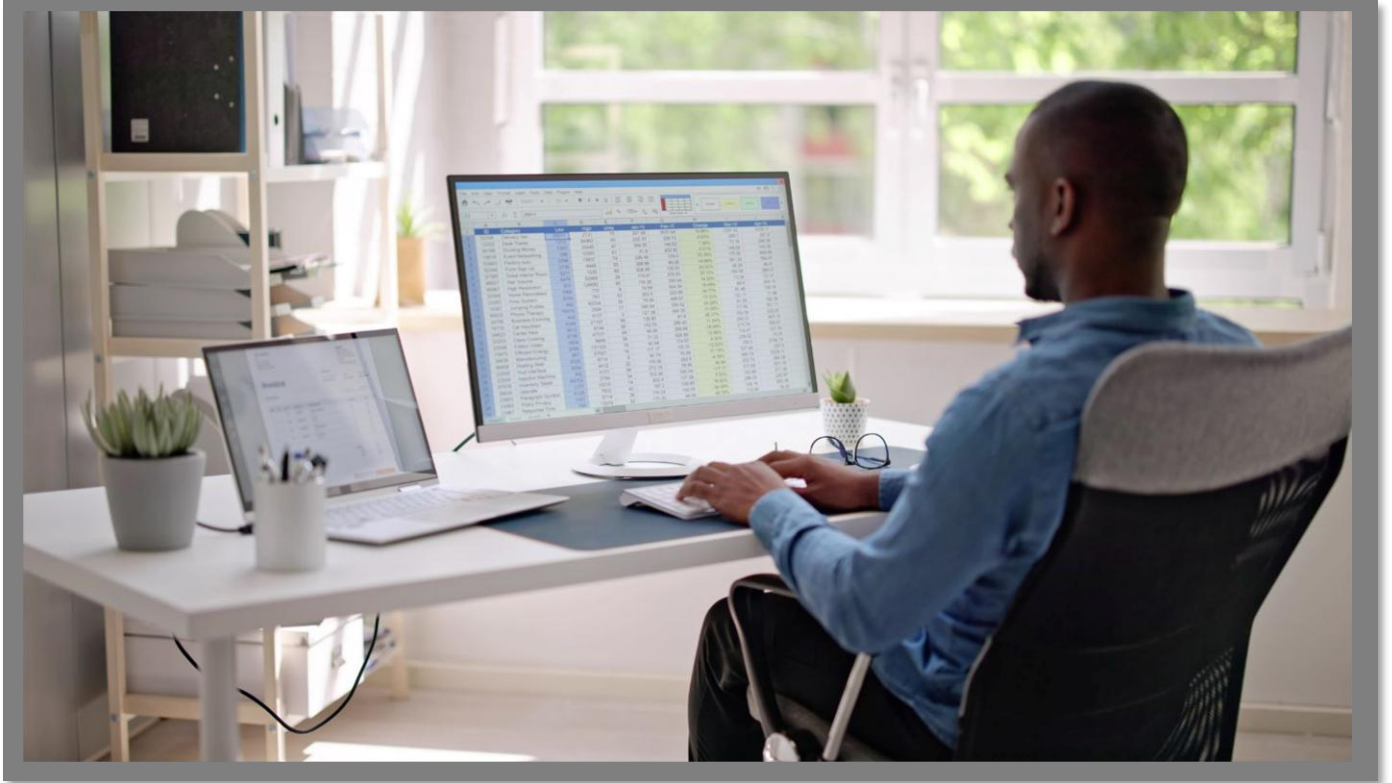


Arbutus Connectors

Dynamics 365 CONFIGURATION GUIDE



Arbutus Connectors

Contents

A. Introduction	1
B. About Dynamics 365	1
C. Determining if the Connector exists prior to configuring	2
D. Configuring the Connector after it has been installed	3
E. Editing the DSN properties – the basic and Advanced tabs .	6
E1. Editing the DSN properties in the Basic tab	6
E2. Editing the DSN properties in the Advanced tab	15
F. Other questions and/or request for assistance	17

Arbutus Connector – Dynamics 365

A. Introduction

The purpose of this Guide is to provide assistance with configuring the Arbutus Dynamics 365 Connector using the ODBC Data Source Administrator. The configuration process can involve several technical steps that require a good understanding of IT systems and database management.

To make the most of this guide, it's advisable to have a good understanding of database connectivity, driver installation, and system settings. The ODBC Data Source Administrator, which is used as part of the configuration process, allows for the setup and management of data sources, enabling applications to access data from various database systems.

Due to the complexity and potential impact of these configurations, it is recommended that only those individuals with IT or database expertise undertake this task. In addition, it should also be understood that each client's network environment is different. A one-size-fits-all approach is rarely effective, as what works well in one environment may not be suitable in another.

B. About Dynamics 365

Microsoft Dynamics 365 is a cloud-based business application platform that combines enterprise resource planning (ERP) and customer relationship management (CRM) capabilities. Organizations use Dynamics 365 to manage core business processes such as finance, sales, procurement, customer service, supply chain operations, and human resources. The platform stores business information in structured data entities that represent records such as customers, vendors, invoices, purchase orders, and general ledger transactions.

Arbutus Connectors

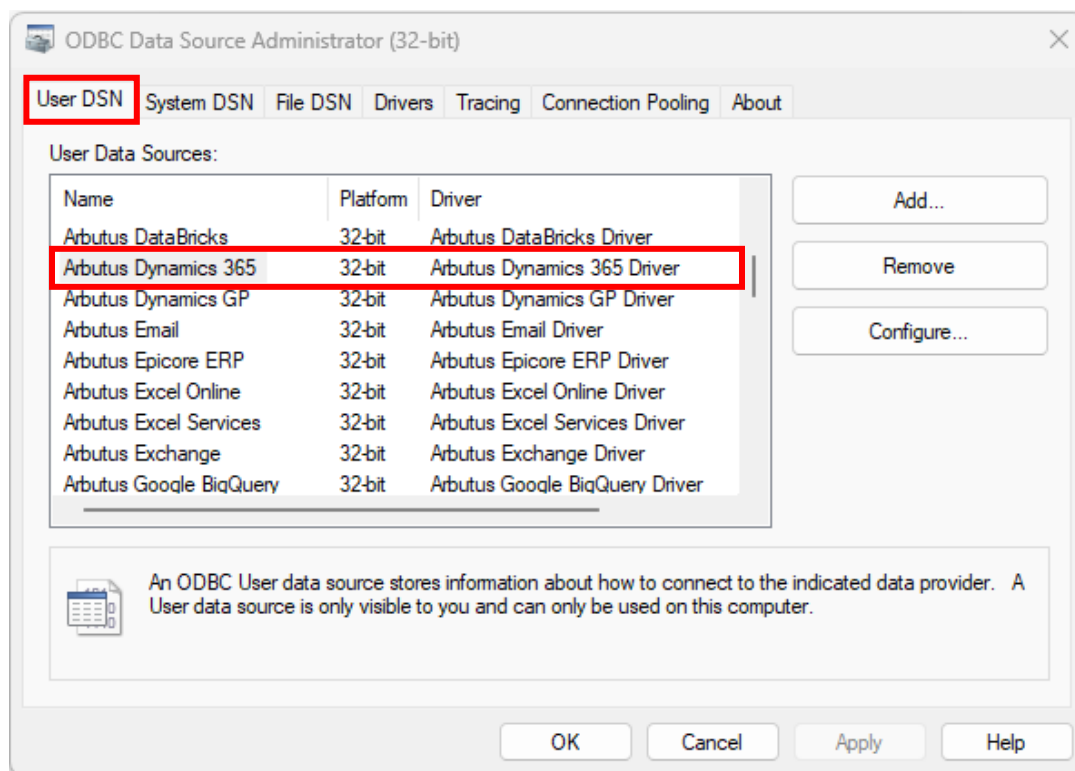
Dynamics 365 data is stored within Microsoft's cloud environment and organized into relational tables and entities that are linked through defined business relationships. Users and applications can access this data through secure APIs, reporting tools, and data connectors that support querying and analysis. This structure enables users to retrieve and examine business data while maintaining security controls and data integrity.

C. Determining if the Connector exists prior to configuring

Installation of the Arbutus Dynamics 365 Connector is done at the time of installing the Arbutus software. For more information on this, please see the **Overview Guide Document**.

Once the Connector has been installed, the next step is to configure it.

Prior to configuring it, you can check to see if the Connector has been installed by opening the **32-bit ODBC Data Source Administrator**, pictured below, and clicking the **User DSN** tab. Included below is information on how you can access the **ODBC Data Source Administrator**.



Arbutus Connectors

- If the Arbutus Dynamics 365 Connector appears in the list, it can be considered as installed.
- If it is not listed, it is likely that you did not select it during the installation or modification of the Arbutus software. In this case, it is recommended to reinstall the Arbutus software and choose the **Modify** option when prompted. For more details, please refer to the **Overview Guide Document**.

Below is the file path to access and run the **ODBC Data Source Administrator** application:

C:\Windows\SysWOW64\odbcad32.exe

Alternative, you can also try locating and opening the **ODBC Data Source Administrator** application by doing a search on your desktop application.

D. Configuring the Connector after it has been installed

Once you have verified that the Arbutus Connector has been installed, it is time to configure it.

This process is done using the **ODBC Data Source Administrator**. It can be described as “**editing the DSN configuration**”.

DSN, Drivers, and Data Sources

What is a DSN? DSN stands for Data Source Name, and is a unique name used to create a data connection to a database using open database connectivity (ODBC).

A DSN is a data structure that contains the information required to connect to a database. It is essentially a string that identifies the source database, including the driver details, the database name, and often authentication credentials and other necessary connection parameters. DSNs facilitate a standardized method for applications to access databases without needing hard-coded connection details, enhancing flexibility and scalability in database management.

Arbutus Connectors

- **Drivers** are the components that process ODBC requests and return data to the application. If necessary, drivers modify an application's request into a form that is understood by the data source. The **Drivers** tab in the **ODBC Data Source Administrator** dialog box lists all drivers installed on your computer, including the name, version, company, file name, and file creation date of each driver.
- **Data sources** are the databases of files accessed by a driver and are identified by a data source name (DSN). You use the ODBC Data Source Administrator to add, configure, and delete data sources from your system.

All ODBC connections require that a DSN be configured to support the connection. When a client application wants to access an ODBC-compliant database, it references the database using the DSN.

The types of DSNs are:

- **User DSN** – User DSNs are local to a computer and can be used only by the current user. They are registered in the HKEY_Current_USER registry subtree.
- **System DSN** – System DSNs are local to a computer rather than dedicated to a user. The system or any user with privileges can use a data source set up with a system DSN. System DSNs are registered in the HKEY_LOCAL_MACHINE registry subtree.
- **File DSN** – File DSNs are file-based sources that can be shared among all users who have the same drivers installed and therefore have access to the database. These data sources need not be dedicated to a user nor be local to a computer. File data source names are identified by a file name with a .dsn extension.

User and system data sources are collectively known as *machine* data sources because they are local to a computer.

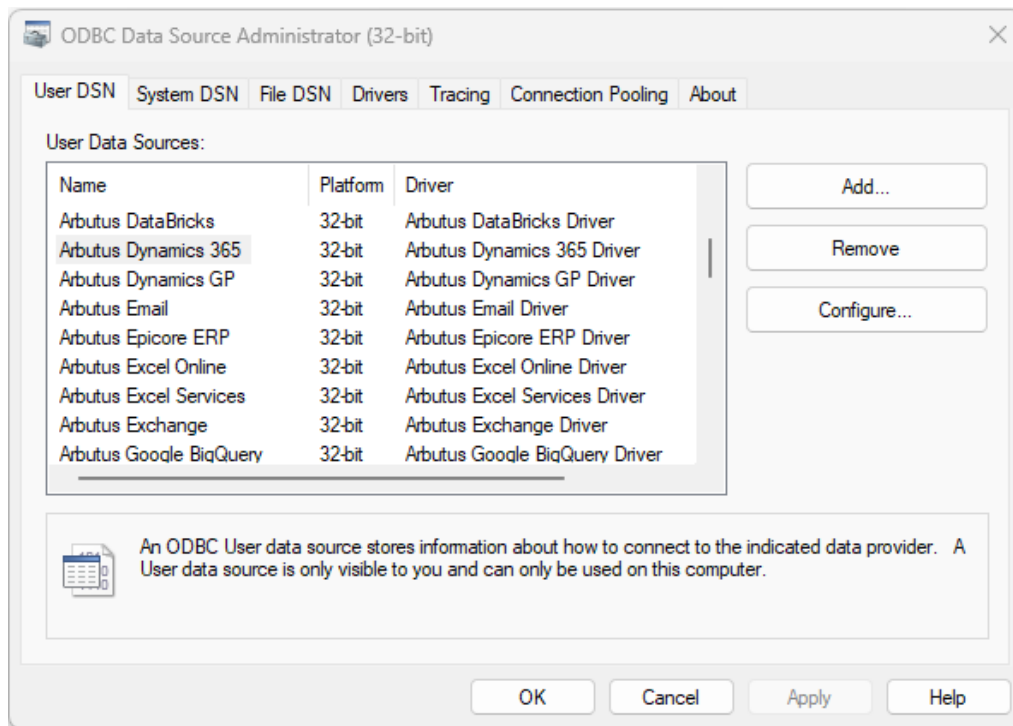
Each of these DSNs has a tab in the **ODBC Data Source Administrator** dialog.

The Arbutus ODBC Driver for Microsoft Dynamics 365 enables real-time access to Dynamics 365 data, directly from any applications that support ODBC connectivity, the most widely supported interface for connecting applications with data.

Arbutus Connectors

Follow these steps to edit the DSN configuration and configure the Connector.

1. First open the **ODBC Data Source Administrator**.



2. Click the **User DSN** tab.

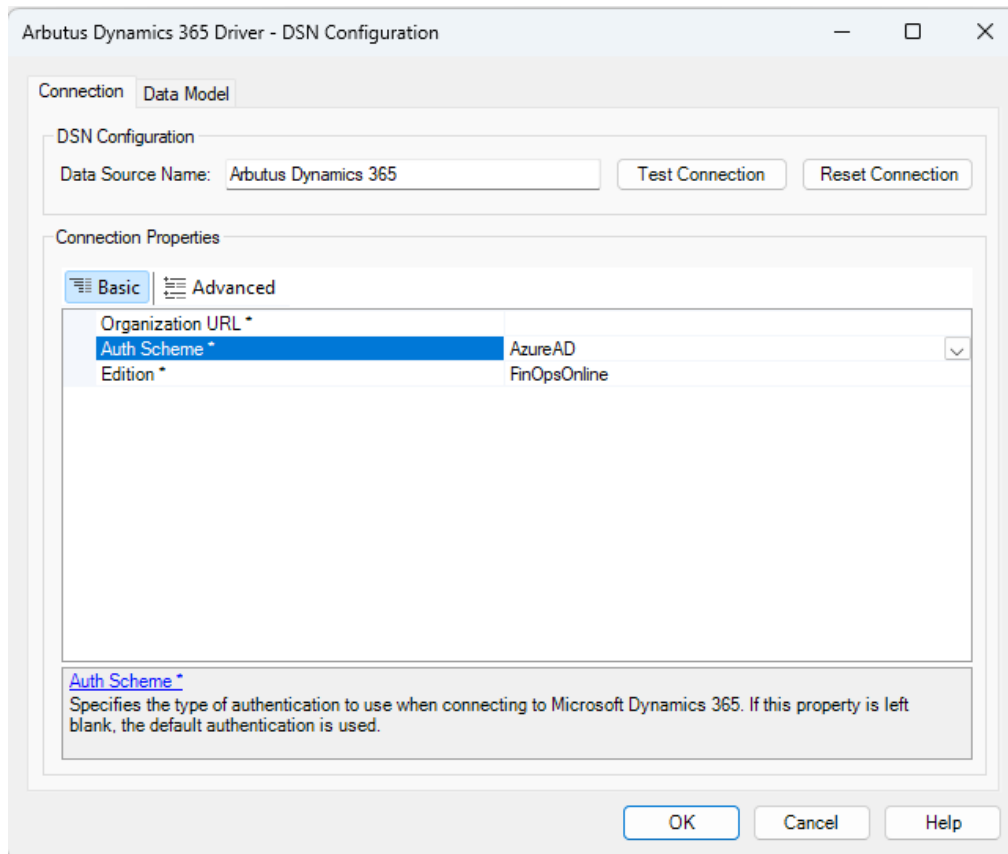
Selected data connectors are installed as **User DSN's** in Window's 32 Bit **ODBC Data Source Administrator**.

Also, each of the data connector's names is prefaced with Arbutus, for example, **Arbutus Dynamics 365**.

3. Select the Arbutus Connector, in this case it is **Arbutus Dynamics 365**.
4. Click **Configure**.

This opens the **Arbutus Dynamics 365 Driver – DSN Configuration** dialog.

Arbutus Connectors



E. Editing the DSN properties – the basic and Advanced tabs

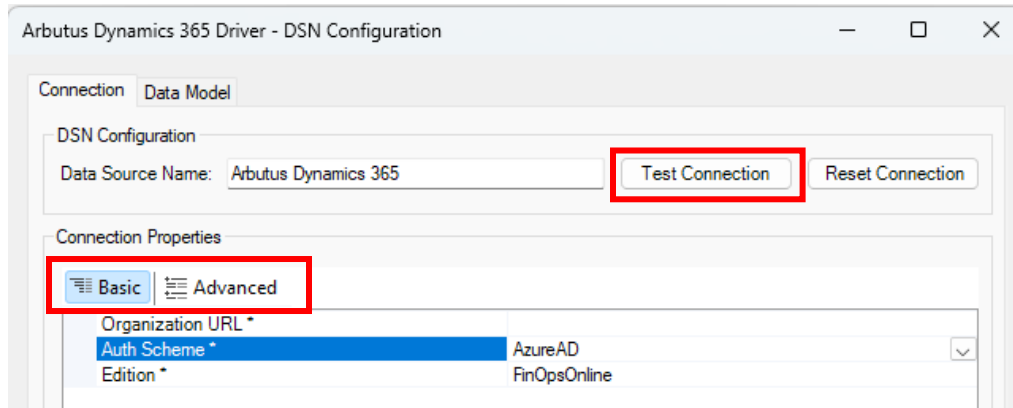
With the DSN Configuration dialog open, the next step is to edit the DSN properties, where necessary, in the **Basic** and **Advanced** tabs. For example, editing the **Schema** property (per screenshot below) to specify the type of schema to use.

E1. Editing the DSN properties in the Basic tab

The properties listed in the **Basic** tab are typically the ones that are most commonly used, and as such are designed to be more user-friendly and straightforward, allowing you to quickly make changes without needing in-depth technical knowledge.

Once you have completed editing the properties in the **Basic** tab, you can go ahead and try testing the connection to the Dynamics 365 system by clicking the **Test Connection** button, as highlighted in the screenshot below.

Arbutus Connectors



In the **Basic** tab, there are **three** main properties to review:

1. **Organization URL** – this is the URL you use to log into your Dynamics 365 organization; sometimes also referred to as the *resource*.

To find the correct URL for your Microsoft Dynamics 365 instance, within Dynamics 365, search **the Web Services page – click the Search icon and enter “Web Services”**. The resource URL format is similar to `https://abc123.cloudax.dynamics.com/`, except when the Edition is HumanResources. HumanResources URLs typically look like: `https://{cluster}.hr.talent.dynamics.com/namespaces/{namespace_guid}/`.

2. **Auth Scheme** – click the dropdown to select from the list the right authentication method to use when connecting to Dynamics 365. If this property is left blank, the default authentication is used.

The dropdown options available are:

- **AzureAD** – this is the default selection. Select this to perform Azure Active Directory (user-based) OAuth authentication.
- **AzureMSI** – select this when you want to automatically obtain Azure AD Managed Service Identity credentials when running on an Azure VM.

Arbutus Connectors

- **AzureServicePrincipal** – select this when you want to authenticate as an Azure Service Principal (role-based, application-based) using a Client Secret.

Selecting this property requires you to also specify the following:

- **Azure Tenant** – Identifies the Microsoft Dynamics 365 tenant being used to access data. Accepts either the tenant's domain name (for example, contoso.onmicrosoft.com) or its directory (tenant) ID.

A tenant is a digital container for your organization's users and resources, managed through Microsoft Entra ID (formerly Azure AD). Each tenant is associated with a unique directory ID, and often with a custom domain (for example, microsoft.com or contoso.onmicrosoft.com).

To find the directory (tenant) ID in the Microsoft Entra Admin Center, navigate to **Microsoft Entra ID > Properties** and copy the value labeled "**Directory (tenant) ID**".

This property is required in the following cases:

- When **AuthScheme** is set to **AzureServicePrincipal** or **AzureServicePrincipalCert**
- When **AuthScheme** is **AzureAD** and the user account belongs to multiple tenants

You can provide the tenant value in one of two formats:

- A domain name (for example, contoso.onmicrosoft.com)
- A directory (tenant) ID in GUID format (for example, c9d7b8e4-1234-4f90-bc1a-2a28e0f9e9e0)

Specifying the tenant explicitly ensures that the authentication request is routed to the correct directory, which is especially important when a user belongs to multiple

Arbutus Connectors

tenants or when using service principal-based authentication.

If this value is omitted when required, authentication may fail or connect to the wrong tenant. This can result in errors such as unauthorized or resource not found.

- **OAuth Client ID** – Specifies the client ID (also known as the consumer key) assigned to your custom OAuth application. This ID is required to identify the application to the OAuth authorization server during authentication.

This property is required in two cases:

- When using a custom OAuth application, such as in web-based authentication flows, service-based authentication, or certificate-based flows that require application registration.
- If the driver does not provide embedded OAuth credentials.

(When the driver provides embedded OAuth credentials, this value may already be provided by the driver and thus not require manual entry.)

OAuthClientId is generally used alongside other OAuth-related properties such as **OAuthClientSecret** and **OAuthSettingsLocation** when configuring an authenticated connection.

OAuthClientId is one of the key connection parameters that need to be set before users can authenticate via OAuth. You can usually find this value in your identity provider's application registration settings. Look for a field labeled **Client ID**, **Application ID**, or **Consumer Key**.

While the client ID is not considered a confidential value like a client secret, it is still part of your application's identity and

Arbutus Connectors

should be handled carefully. Avoid exposing it in public repositories or shared configuration files.

- **OAuth Client Secret** – Specifies the client secret assigned to your custom OAuth application. This confidential value is used to authenticate the application to the OAuth authorization server. (Custom OAuth applications only.).

This property (sometimes called the application secret or consumer secret) is required when using a custom OAuth application in any flow that requires secure client authentication, such as web-based OAuth, service-based connections, or certificate-based authorization flows. It is not required when using an embedded OAuth application.

The client secret is used during the token exchange step of the OAuth flow, when the driver requests an access token from the authorization server. If this value is missing or incorrect, authentication fails with either an *invalid_client* or an *unauthorized_client* error.

OAuthClientSecret is one of the key connection parameters that need to be set before users can authenticate via OAuth. You can obtain this value from your identity provider when registering the OAuth application.

Notes:

- This value should be stored securely and never exposed in public repositories, scripts, or unsecured environments.
- Client secrets may also expire after a set period. Be sure to monitor expiration dates and rotate secrets as needed to maintain uninterrupted access.

Arbutus Connectors

- **AzureServicePrincipalCert** – select this when you want to authenticate as an Azure Service Principal (role-based, application-based) using a Certificate.

Selecting this property requires you to also specify the following:

- **Azure Tenant** – Identifies the Microsoft Dynamics 365 tenant being used to access data. Accepts either the tenant's domain name (for example, contoso.onmicrosoft.com) or its directory (tenant) ID.

For more information, refer to the **Azure Tenant** section above – applies in this instance too.

- **OAuth Client Id** – Specifies the client ID (also known as the consumer key) assigned to your custom OAuth application. This ID is required to identify the application to the OAuth authorization server during authentication.

For more information, refer to the **OAuth Client Id** section above – applies in this instance too.

- **OAuth JWT Cert** - Supplies the name of the client certificate's JWT Certificate store.

The **OAuthJWTCertType** field specifies the type of the certificate store specified in **OAuthJWTCert**. If the store is password-protected, use **OAuthJWTCertPassword** to supply the password.

OAuthJWTCert is used in conjunction with the **OAuthJWTCertSubject** field in order to specify client certificates. If **OAuthJWTCert** has a value, and **OAuthJWTCertSubject** is set, the Arbutus ODBC Driver for Microsoft Dynamics 365 initiates a search for a certificate. For further information, see the **OAuthJWTCertSubject** section below.

Designations of certificate stores are platform-dependent.

Notes

- The most common **User** and **Machine** certificate stores in Windows include:
 - ❖ **MY**: A certificate store holding personal certificates with their associated private keys.
 - ❖ **CA**: Certifying authority certificates.
 - ❖ **ROOT**: Root certificates.
 - ❖ **SPC**: Software publisher certificates.
 - In Java, the certificate store normally is a file containing certificates and optional private keys.
 - When the certificate store type is **PFXFile**, this property must be set to the name of the file.
 - When the type is **PFXBlob**, the property must be set to the binary contents of a PFX file (i.e. **PKCS12** certificate store).
- **OAuth JWT Cert Type** - Identifies the type of key store containing the JWT Certificate.

This is a dropdown selection containing the following values for selection:

- **USER** – A certificate store owned by the current user.
- **MACHINE** – A machine store
- **PFXFILE** – A PFX (PKCS12) file containing certificates
- **PFXBLOB** – A string (base-64-encoded) representing a certificate store in PFX (PKCS12) format
- **JKSFILE** – A Java key store (JKS) file containing certificates
- **JKSBLOB** - A string (base-64-encoded) representing a certificate store in Java key store (JKS) format
- **PEMKEY_FILE** – A PEM-encoded file that contains a private key and an optional certificate

Arbutus Connectors

- PEMKEY_BLOB – A string (base64-encoded) that contains a private key and an optional certificate
- PUBLIC_KEY_FILE – A file that contains a PEM- or DER-encoded public key certificate
- PUBLIC_KEY_BLOB – A string (base-64-encoded) that contains a PEM- or DER-encoded public key certificate
- SSHPUBLIC_KEY_FILE – A file that contains an SSH-style public key
- SSHPUBLIC_KEY_BLOB – A string (base-64-encoded) that contains an SSH-style public key
- P7BFILE – A PKCS7 file containing certificates
- PPKFILE – A file that contains a PPK (PuTTY Private Key)
- XMLFILE – A file that contains a certificate in XML format
- XMLBLOB – A string that contains a certificate in XML format
- BCFKSFIL – A file that contains an Bouncy Castle keystore
- BCFKSBLOB - A string (base-64-encoded) that contains a Bouncy Castle keystore

The default is **USER**.

- [OAuth JWT Cert Password](#) - Provides the password for the OAuth JWT certificate used to access a password-protected certificate store. If the certificate store does not require a password, leave this property blank.
- [OAuth JWT Cert Subject](#) - Identifies the subject of the OAuth JWT certificate used to locate a matching certificate in the store. Supports partial matches and the wildcard '*' to select the first certificate.

The value of this property is used to locate a matching certificate in the store. The search process works as follows:

- If an exact match for the subject is found, the corresponding certificate is selected.

Arbutus Connectors

- If no exact match is found, the store is searched for certificates whose subjects contain the property value.
- If no match is found, no certificate is selected.

You can set the value to '*' to automatically select the first certificate in the store. The certificate subject is a comma-separated list of distinguished name fields and values. For example: CN=www.server.com, OU=test, C=US, E=support@cdata.com.

Common fields include:

Field	Meaning
CN	Common Name. This is commonly a host name like www.server.com
O	Organization
OU	Organization Unit
L	Locality
S	State
C	Country
E	Email Address

3. **Edition** – This is a dropdown selection and specifies the Microsoft Dynamics 365 edition in use. If not specified, the default (FinOpsOnline) is assumed.

The dropdown options available are:

- **CustomerService** - Connect to Dynamics 365 Customer Service environments, used for managing customer support, case management, and service operations
- **FieldService** - Connect to Dynamics 365 Field Service environments, used for scheduling, dispatching, and managing onsite work orders and field technicians
- **FinOpsOnline** - Connect to Dynamics 365 Finance and Operations (cloud-based ERP) environments, used for financial management, procurement, supply chain, and core business operations

Arbutus Connectors

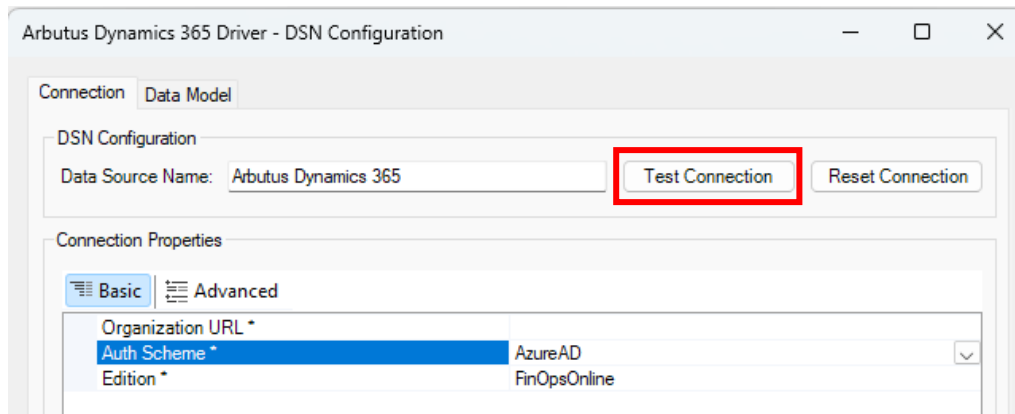
- [FinOpsOnPremise](#) - Connect to on-premise Dynamics 365 Finance and Operations environments, used for ERP processes hosted within the organization's own infrastructure
- [HumanResources](#) - Connect to Dynamics 365 Human Resources environments, used for managing employee data, HR processes, benefits, and workforce administration
- [Marketing](#) - Connect to Dynamics 365 Marketing environments, used for campaign management, customer journeys, and marketing automation
- [ProjectOperations](#) - Connect to Dynamics 365 Project Operations environments, used for managing project planning, resource scheduling, and project financials
- [Sales](#) - Connect to Dynamics 365 Sales environments, used for managing leads, opportunities, accounts, and sales pipelines
- [Commerce](#) - Commerce – Connect to Dynamics 365 Commerce environments, used for retail operations, point-of-sale (POS), e-commerce, and omnichannel customer experiences

E2. Editing the DSN properties in the [Advanced](#) tab

This tab includes more detailed and technical properties. It is intended for those users who need more control over the configuration and are comfortable with more complex options. The **Advanced** tab often includes properties that can fine-tune the behaviour of the system feature.

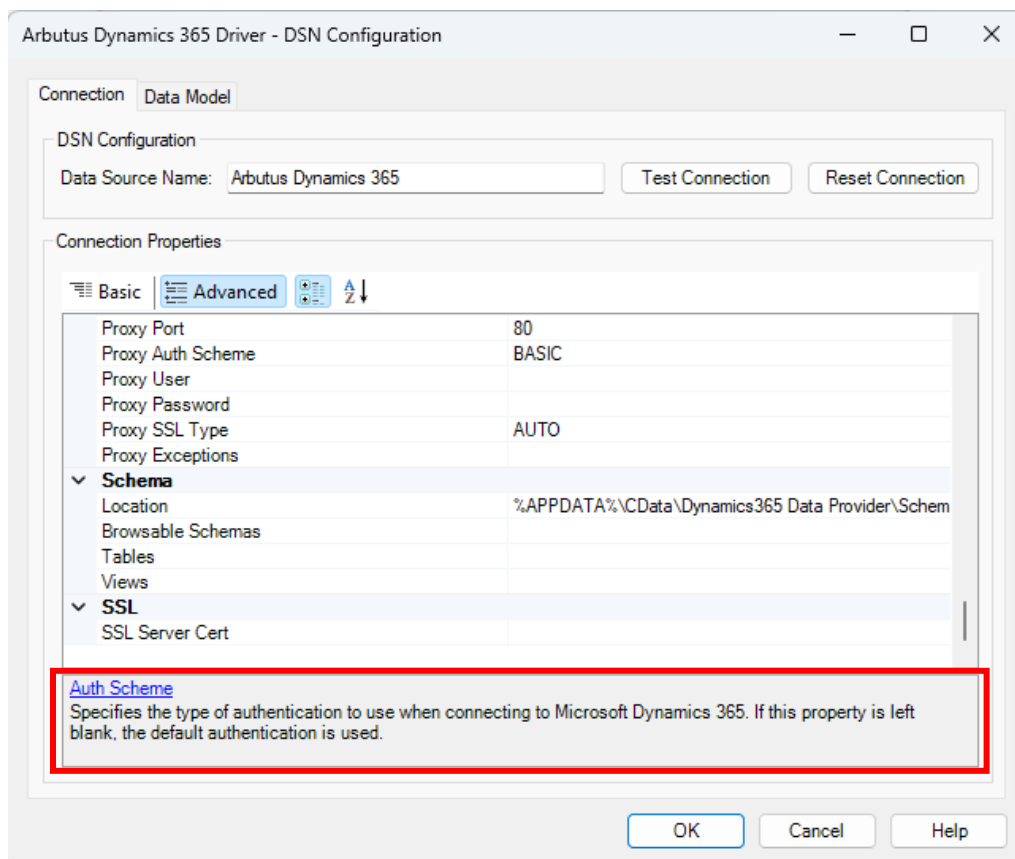
If you have already completed editing the properties in the **Basic** tab, as required, you do not necessarily need to also complete editing the properties in the **Advanced** tab. Instead, once you have completed editing the properties in the **Basic** tab, you may opt to proceed to testing the connection to the Dynamics 365 system by clicking the **Test Connection** button.

Arbutus Connectors



There are a lot more properties included for editing in the **Advanced** tab.

However, it is useful to know that each property does provide a short description of it and as such serves as a guide in terms of what to edit and/or enter. This short description can be seen at the bottom of the **DSN Configuration** dialog box, as seen in the screenshot below.



Arbutus Connectors

If it is deemed necessary to complete some/all the properties in the **Advanced** tab, it is recommended that you refer to the description shown for any of the properties being edited and/or entered.

If required, more information on the properties listed in the **Advanced** tab can also be provided.

F. Other questions and/or request for assistance

There may be times when you need to consult with the technical support team at Arbutus Software. If so, please send an email request to support@ArbutusSoftware.com.

For more information, please refer to the [CONTACT US](#) page on our website.