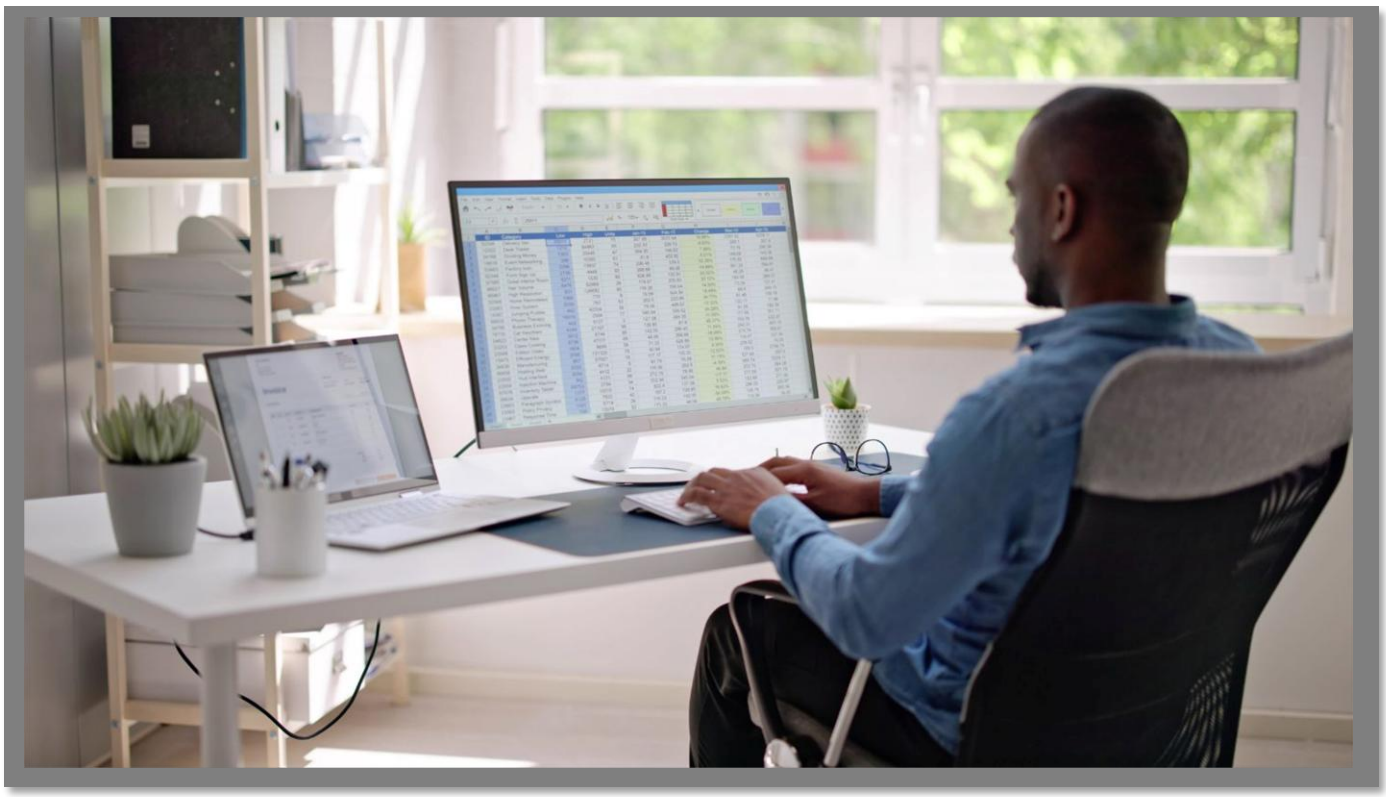
Arbutus Connectors

Dynamics 365 Business Central

CONFIGURATION GUIDE



ARBUTUS

Powerful Analytics Simplified

Arbutus Connectors

Contents

Arbutus Connector – Dynamics 365 Business Central

A. Introduction

The purpose of this Guide is to provide assistance with configuring the Arbutus Dynamics 365 Business Central 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 Business Central

Dynamics 365 Business Central is a cloud-based ERP solution for small to medium-sized businesses. It integrates finance, sales, supply chain, inventory, and customer management into one platform, helping businesses automate processes, gain insights, and streamline operations.

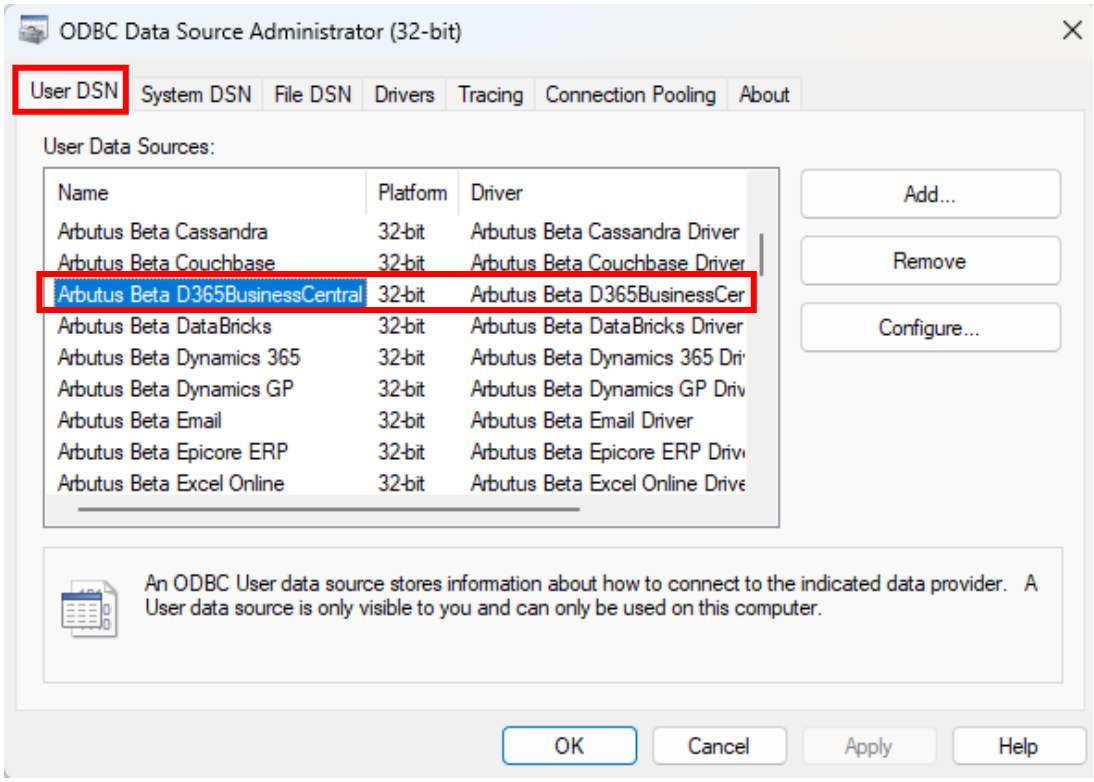
Data is stored in the cloud on Microsoft Azure. Business Central uses SQL Server databases to manage structured data, ensuring scalability and security. The data is organized into tables, which represent different business entities (e.g., customers, orders, inventory).

C. Determining if the Connector exists prior to configuring

Installation of the Arbutus Dynamics 365 Business Central 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**.



- If the Arbutus Dynamics 365 Business Central 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.

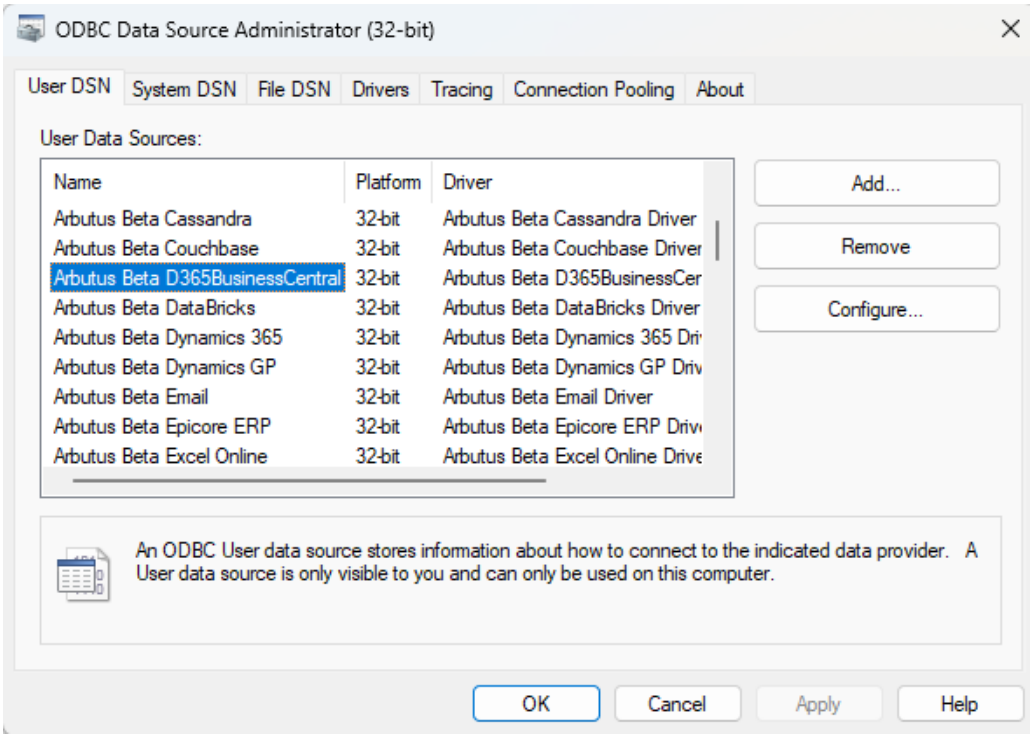
Each of these DSNs has a tab in the **ODBC Data Source Administrator** dialog.

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**.



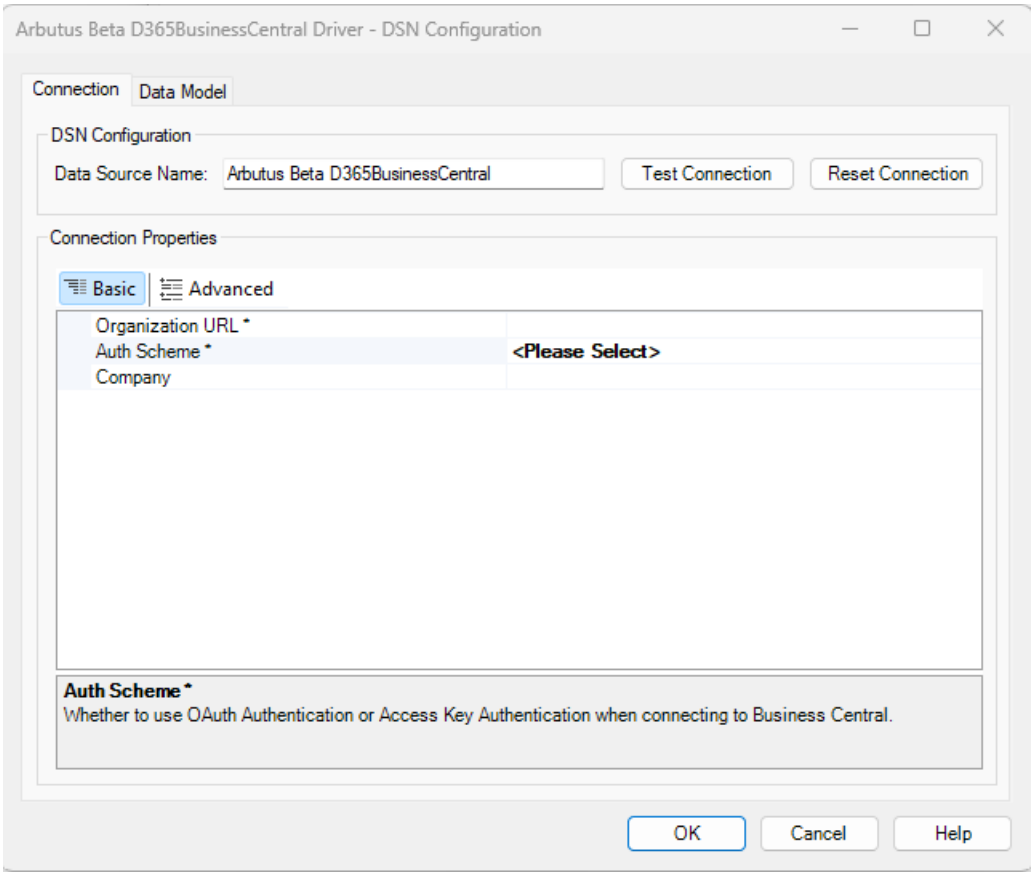
2. Click the **User DSN** tab.

   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 Business Central.**

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

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



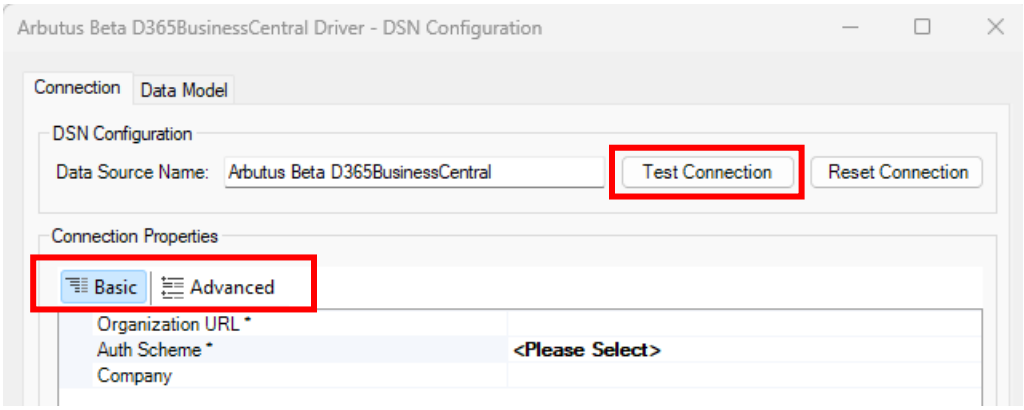
E. Editing the DSN properties – the basic and Advanced tabs

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 Business Central system by clicking the **Test Connection** button, as highlighted in the screenshot below.



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 called the *resource*. For instance, https://businesscentral.dynamics.com/abc123/.

   To find the correct URL for your Microsoft Dynamics 365 Business Central instance. This may also be known as the resource. To find this click the **Search** icon and enter "Web Services". Monitor the OData v4 URL. The end value should be the web service endpoint (minus the **Company** – see below).

2. **Auth Scheme** – click the dropdown to select from the list the right authentication method to use when connecting to Business Central – whether to use OAuth Authentication or Access Key Authentication. The options available are:
   - AccessKey – select this when you want to authenticate using a web service access key in Dynamics 365 Business Central.

     To obtain an access key, you typically need to log into your Dynamics 365 Business Central instance, navigate to the Users page, and either copy an existing web service access key or generate a new one.

     This property requires you to also specify the following:

     - User – this is the username of the Dynamics 365 OnPremise account to authenticate to the Microsoft Dynamics 365 Business Central server.

       Together with **Access Key** (see below), this field is used to authenticate to the Microsoft Dynamics 365 Business Central server.

     - Access Key – this is the access key used to authenticate to the Microsoft Dynamics 365 Business Central server.

       Together with User, this field is used to authenticate against the Microsoft Dynamics 365 Business Central server.

   - AzureAD – select this when you want to authenticate using Azure Active Directory (Azure AD), now known as Microsoft Entra ID.

     Choosing the AzureAD option helps ensure that your connection settings are optimized for secure, efficient, and integrated authentication using Azure AD.

- AzureServicePrincipal – select this when you want to authenticate using a service principal in Azure Active Directory (Azure AD).

  This property requires you to also specify the following:

  - Azure Tenant – this is the Microsoft Online tenant being used to access data. If not specified, your default tenant is used.
    This value is the directory Id in the Azure Portal > Azure Active Directory > Properties.

    Typically it is not necessary to specify the Tenant. This can be automatically determined by Microsoft when using the **OAuth Grant Type** set to **CODE** (default). However, it may fail in the case that the user belongs to multiple tenants. For instance, if an Admin of domain A invites a user of domain B to be a guest user. The user will now belong to both tenants. It is a good practice to specify the Tenant, although in general things should normally work without having to specify it.

    The **AzureTenant** is required when setting **OAuth Grant Type** to **CLIENT**. When using client credentials, there is no user context. The credentials are taken from the context of the app itself. While Microsoft still allows client credentials to be obtained without specifying which Tenant, it has a much lower probability of picking the specific tenant you want to work with. For this reason, we require AzureTenant to be explicitly stated for all client credentials connections to ensure you get credentials that are applicable for the domain you intend to connect to.

- OAuth Client Id – this is the client Id assigned when you register your application with an OAuth authorization server.

  As part of registering an OAuth application, you will receive the **OAuth Client Id** value, sometimes also called a consumer key, and a client secret, the **OAuth Client Secret** (see below).

- OAuth Client Secret – this is the client secret assigned when you register your application with an OAuth authorization server.

  As part of registering an OAuth application, you will receive the **OAuth Client Id** (see above), also called a consumer key. You will also receive a client secret, also called a consumer secret. Set the client secret in the **OAuth Client Secret** property.

- AzureServicePrincipalCert – select this when you want to authenticate using a certificate-based service principal in Azure Active Directory (Azure AD).

  This property requires you to also specify the following:

  - Azure Tenant – for more information, please see this same property listed and described above (under the **AzureServicePrincipal** section).

  - OAuth Client ID – for more information, please see this same property listed and described above (under the AzureServicePrincipal section).

- OAuth JWT Cert – this is the JWT Certificate store for the client certificate.

  The **OAuth JWT Cert Type** field (see below) specifies the type of the certificate store specified by **OAuth JWT Cert**. If the store is password protected, specify the password in OAuthJWT Cert Password (see below).

  OAuth JWT Cert is used in conjunction with the **OAuth JWT Cert Subject** field (see below) in order to specify client certificates. If **OAuth JWT Cert** has a value, and **OAuth JWT Cert Subject** is set, a search for a certificate is initiated. Please refer to the **OAuth JWT Cert Subject** field for details.

  If required, more information on this setting and its properties can be provided.

- OAuth JWT Cert Type – this is the type of key store containing the JWT Certificate.

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

  > USER, MACHINE, PFXFILE, PFXBLOB, JKSFILE, JKSBLOB, PEMKEY_FILE, PEMKEY_BLOB, PUBLIC_KEY_FILE, PUBLIC_KEY_BLOB, SSHPUBLIC_KEY_FILE, SSHPUBLIC_KEY_BLOB, P7BFILE, PPKFILE, XMLFILE, XMLBLOB, BCFKSFILE, BCFKSBLOB

  If required, more information on this setting and its properties can be provided.

  The default is **USER**.

- OAuth JWT Cert Password – this is the password for the OAuth JWT certificate. If the certificate store is of a type that requires a password, this property is used to specify that password in order to open the certificate store.

- OAuth JWT Cert Subject – this is the subject of the OAuth JWT certificate.

  When loading a certificate the subject is used to locate the certificate in the store. If an exact match is not found, the store is searched for subjects containing the value of the property. If a match is still not found, the property is set to an empty string, and no certificate is selected.

  The special value "*" picks the first certificate in the certificate store.

  If required, more information on this setting and its properties can be provided.

- AzureMSI – select this when you want to use Managed Service Identity for authentication.

- NTLM (NT LAN Manager) – select this when you want to use your Windows credentials for authentication.

  Choosing the NTLM option helps ensure that your connection settings are optimized for environments where Windows-based authentication is preferred or required.

- Negotiate – select this when you want to use Kerberos authentication. Choosing the Negotiate option helps ensure that your connection settings are optimized for secure and efficient authentication using Kerberos.

This property requires you to also specify the following:

- User – this is the username of the Dynamics 365 OnPremise account to authenticate to the Microsoft Dynamics 365 Business Central server.

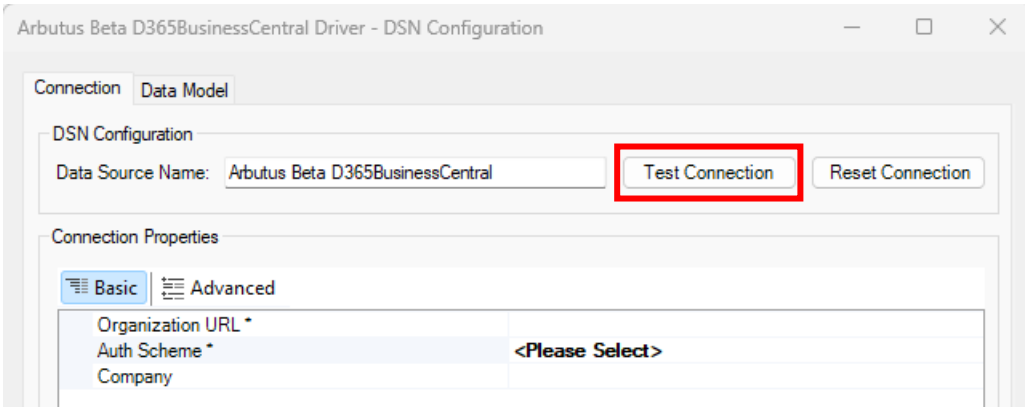
- Password – this is the password used to authenticate the user. The **User** and **Password** are together used to authenticate with the server.

3. **Company** – this is the name of the Microsoft Dynamics 365 Business Central company.

E2. Editing the DSN properties in the Advanced tab

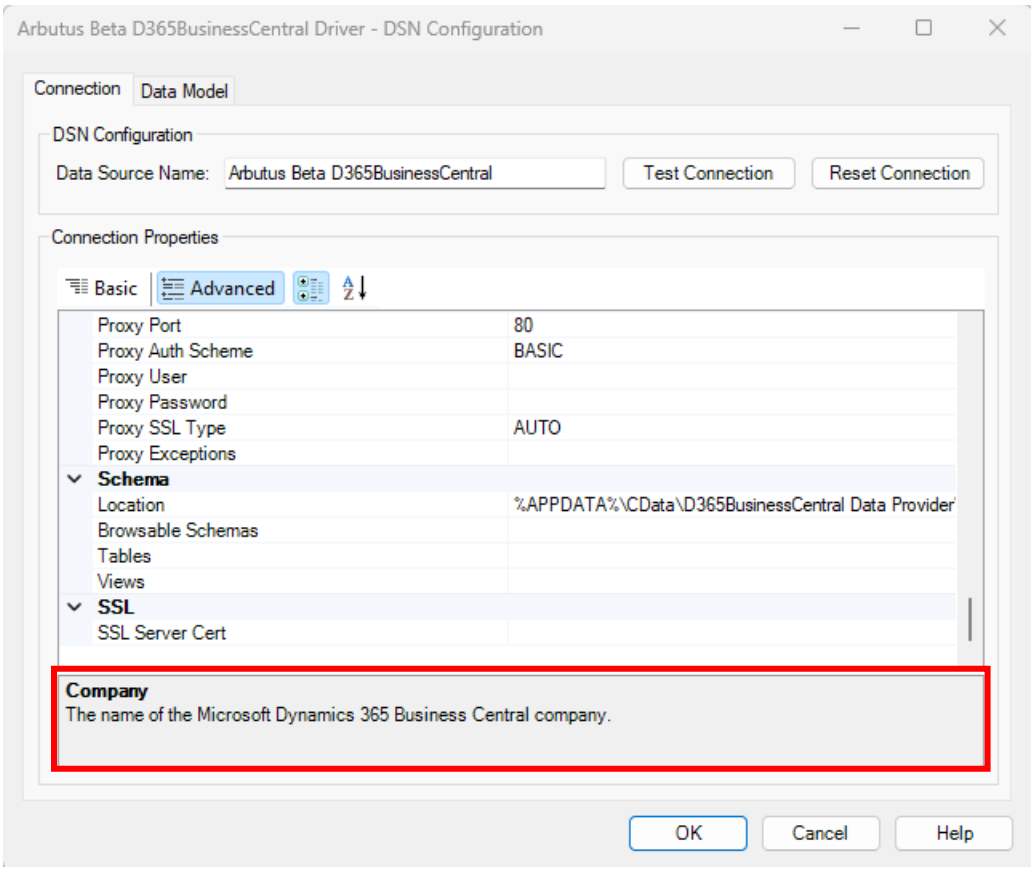
This tab includes more detailed and technical properties. It is intended for those users who need more control over the configuration and are comfortable with more complex options. The **Advanced** tab often includes properties that can fine-tune the behaviour of the system feature.

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 Business Central system by clicking the **Test Connection** button.



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.



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.