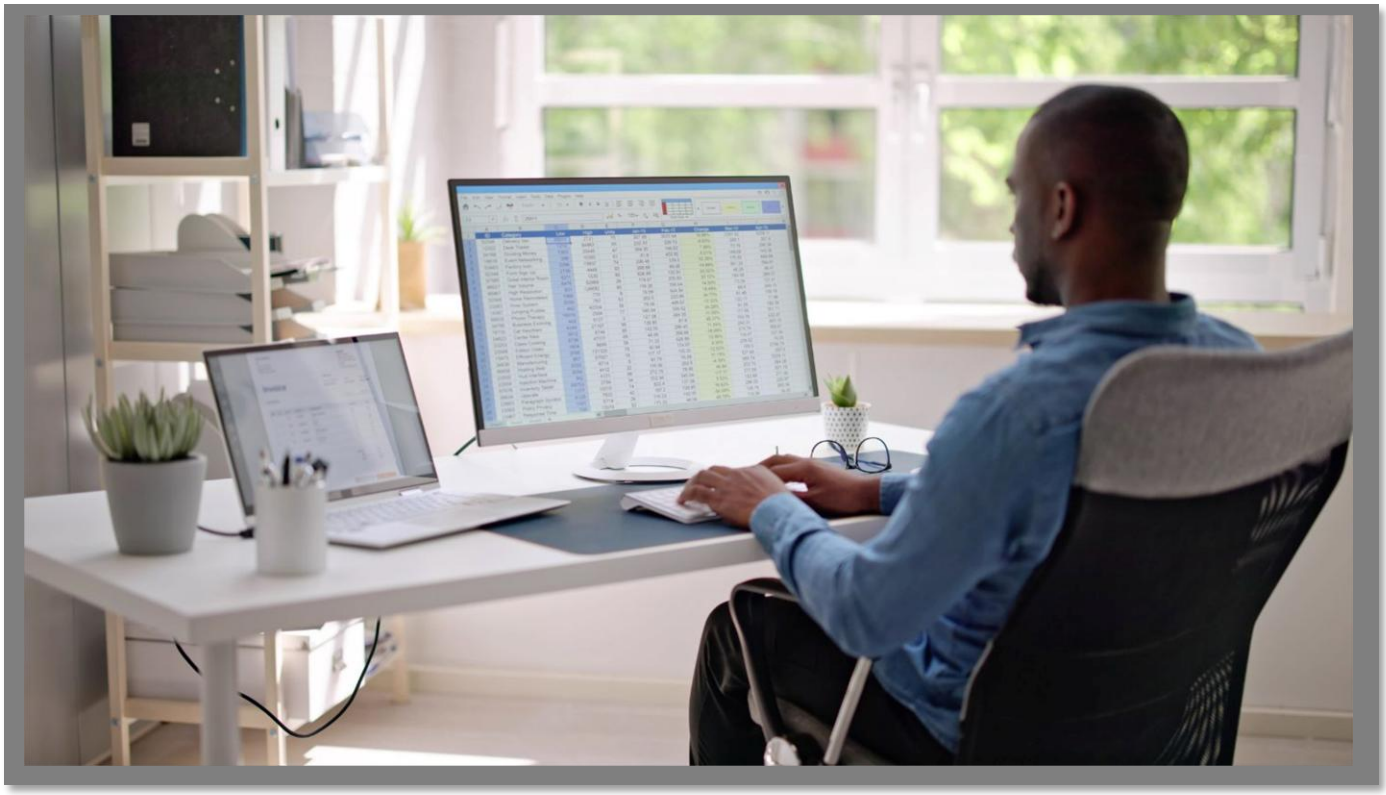
Arbutus Connectors

Dynamics 365 Great Plains (GP)

CONFIGURATION GUIDE



ARBUTUS

Powerful Analytics Simplified

Arbutus Connectors

Contents

Arbutus Connector – Dynamics Great Plains (GP)

A. Introduction

The purpose of this Guide is to provide assistance with configuring the Arbutus Dynamics Great Plains (GP) 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 GP

Dynamics GP is an ERP solution for small to mid-sized businesses, managing financials, supply chain, and operations. It streamlines processes, improves decision-making, and integrates with Microsoft tools.

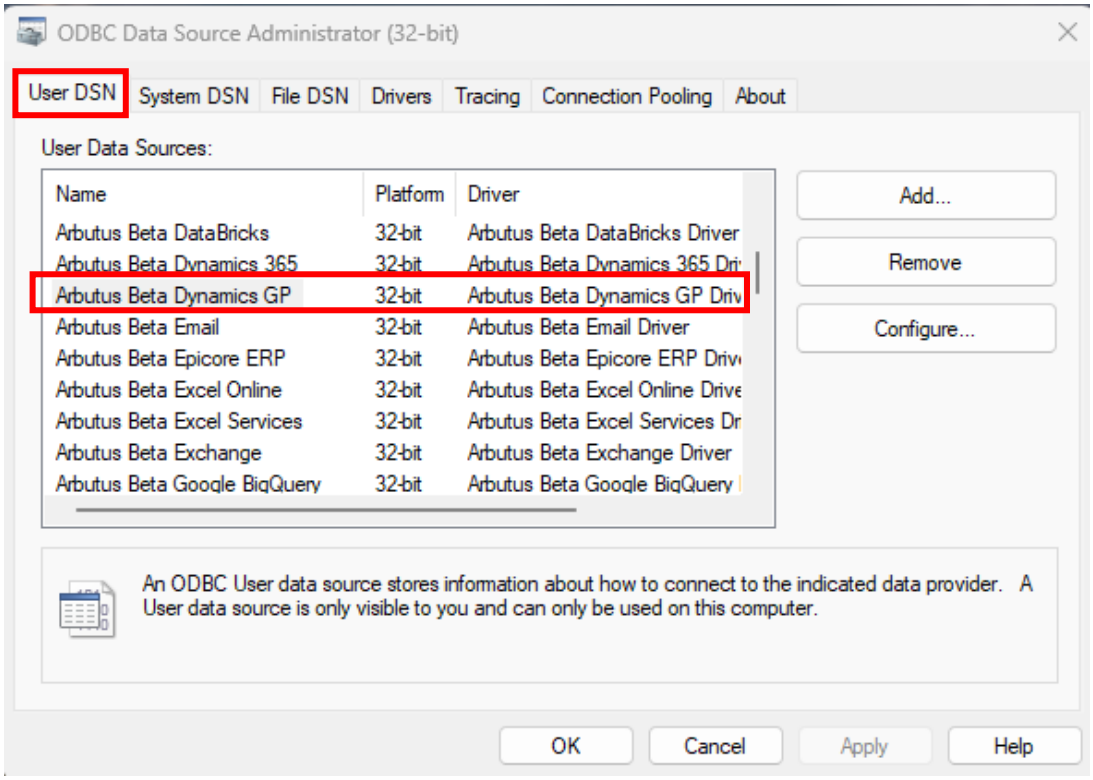
Dynamics GP stores data in a SQL Server database, where it organizes information into tables for various business functions like financials, inventory, and operations. The data is stored on-premises, providing secure and scalable access within the organization's infrastructure.

C. Determining if the Connector exists prior to configuring

Installation of the Arbutus Dynamics GP 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 GP 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.

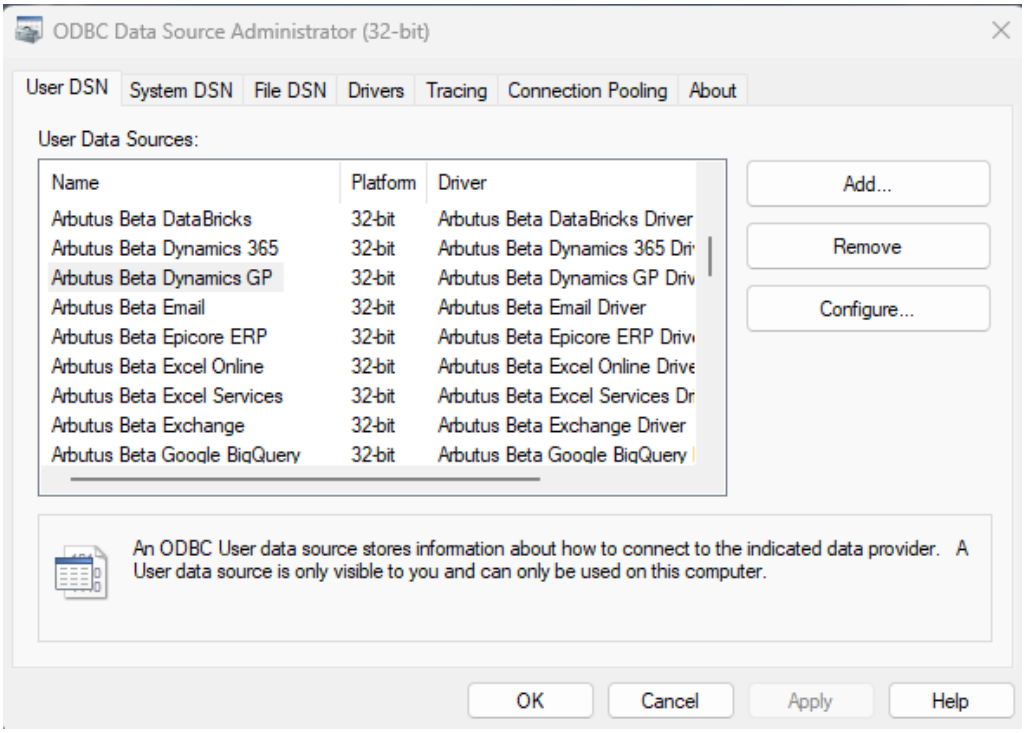
Each of these DSNs has a tab in the **ODBC Data Source Administrator** dialog.

The Arbutus ODBC Driver for Microsoft Dynamics GP enables real-time access to Dynamics GP 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**.



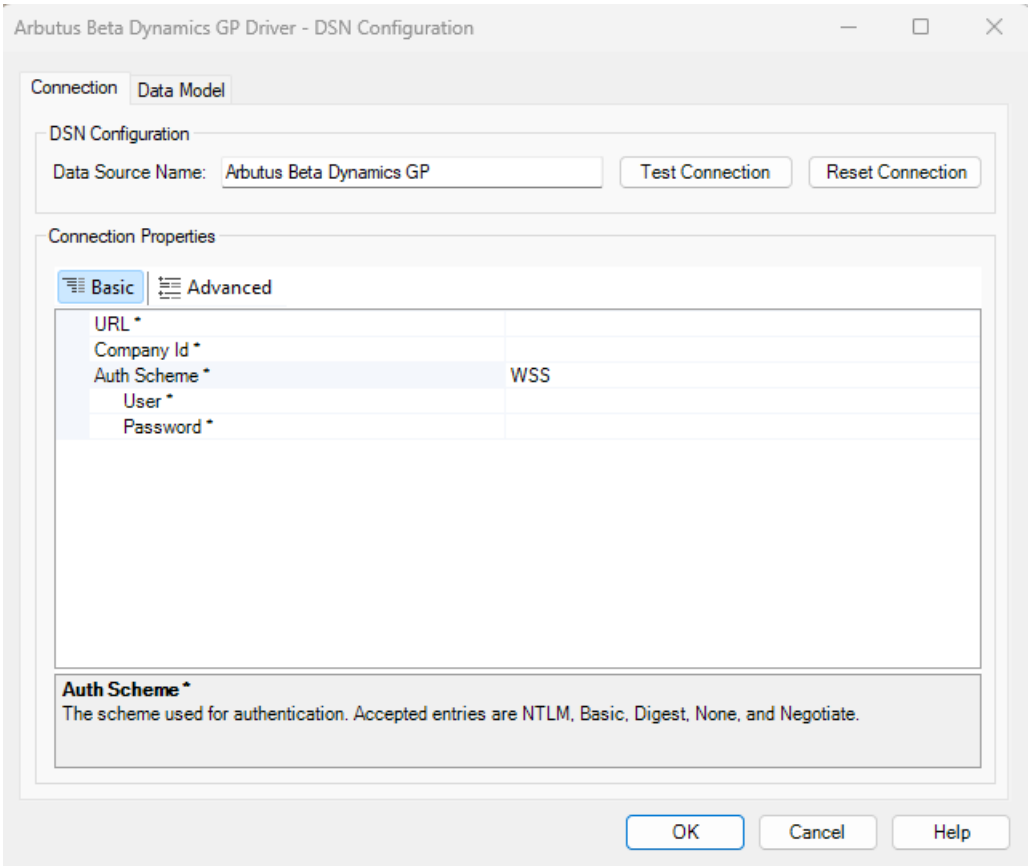
2. Click the **User DSN** tab.

   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 GP.**

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

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



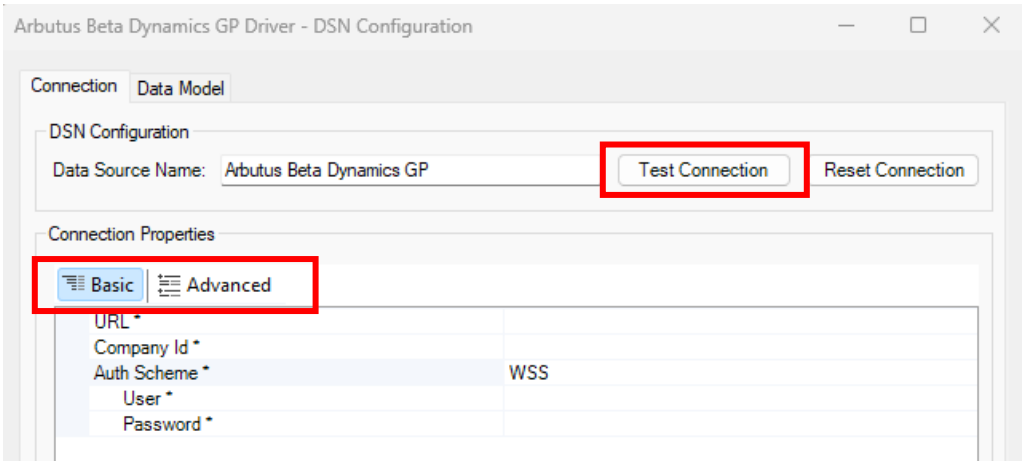
E. Editing the DSN properties – the Basic and Advanced tabs

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 GP 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. **URL** – this is the URL of the Dynamics GP server. This property is required to connect. The full path must be specified. A typical service URL follows the pattern: *http://{servername}:{port}/Dynamics/GPService*.

2. **Company Id** – this is the unique identifier of the company to access as a data source. This property is required to retrieve data for most of the tables. You can obtain this value by querying the Company table and leaving the property empty at first.

3. **Auth Scheme** – click the dropdown to select from the list the scheme used for authentication. The options available are:
   - WSS – select this when you want to use WS-SECURITY encryption for Simple Object Access Protocol (SOAP) messages.

     In the context of configuring the Dynamics GP Driver, using SOAP with WS-SECURITY ensures that the data exchanged between the client and server is secure and compliant with security standards.

     Choosing the WSS option helps ensure that your connection settings are optimized for secure and compliant data transmission.

     Selecting **WSS** requires you to specify the following:

     - User – this is the Microsoft Dynamics GP user account used to authenticate. Together with **Password** (see below), this field is used to authenticate against the Microsoft Dynamics GP server.

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

     The default value is **WSS**.

   - NTLM (Windows 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.

Selecting **NTLM** requires you to specify the following:

- User – this is the Microsoft Dynamics GP user account used to authenticate. Together with **Password** (see below), this field is used to authenticate against the Microsoft Dynamics GP server.

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

- Basic – select this when you want to use HTTP Basic Authentication.

  However, it is important to note that Basic Authentication sends credentials in an encoded form, not encrypted, which can be a security risk if not used over a secure connection (HTTPS). For production environments, consider using more secure authentication methods like NTLM or WS-SECURITY if possible.

  Selecting **Basic** requires you to specify the following:

  - User – this is the Microsoft Dynamics GP user account used to authenticate. Together with **Password** (see below), this field is used to authenticate against the Microsoft Dynamics GP server.

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

- Digest – select this when you want to use HTTP Digest Authentication. Choosing the Digest option helps ensure that your connection settings are optimized for secure and compliant data transmission.

Selecting **Digest** requires you to specify the following:

- User – this is the Microsoft Dynamics GP user account used to authenticate. Together with **Password** (see below), this field is used to authenticate against the Microsoft Dynamics GP server.

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

- None – select this when you want to use anonymous authentication.

  However, it's important to note that using anonymous authentication is not recommended for production environments due to the lack of security. For production, consider using more secure authentication methods like NTLM, Basic, Digest, or WS-SECURITY.

- 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.

  Selecting **Negotiate** requires you to specify the following:

  - User – this is the Microsoft Dynamics GP user account used to authenticate. Together with **Password** (see below), this field is used to authenticate against the Microsoft Dynamics GP server.

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

- Kerberos KDC – this is the Kerberos Key Distribution Center (KDC) service used to authenticate the user.

  The Kerberos properties are used when using SPNEGO or Windows Authentication. The driver will request session tickets and temporary session keys from the Kerberos KDC service. The Kerberos KDC service is conventionally collocated with the domain controller.

  If Kerberos KDC is not specified, the driver will attempt to detect these properties automatically from the following locations:
  - KRB5 Config File (krb5.ini/krb5.conf)
  - Domain Name and Host

- Kerberos Realm – this is the Kerberos Realm used to authenticate the user.

  The Kerberos properties are used when using SPNEGO or Windows Authentication. The Kerberos Realm is used to authenticate the user with the Kerberos Key Distribution Service (KDC). The Kerberos Realm can be configured by an administrator to be any string, but conventionally it is based on the domain name.

  If Kerberos Realm is not specified, the driver will attempt to detect these properties automatically from the following locations:
  - KRB5 Config File (krb5.ini/krb5.conf)
  - Domain Name and Host

- Kerberos SPN – this is the service principal name (SPN) for the Kerberos Domain Controller.

  If the SPN on the Kerberos Domain Controller is not the same as the URL that you are authenticating to, use this property to set the SPN.

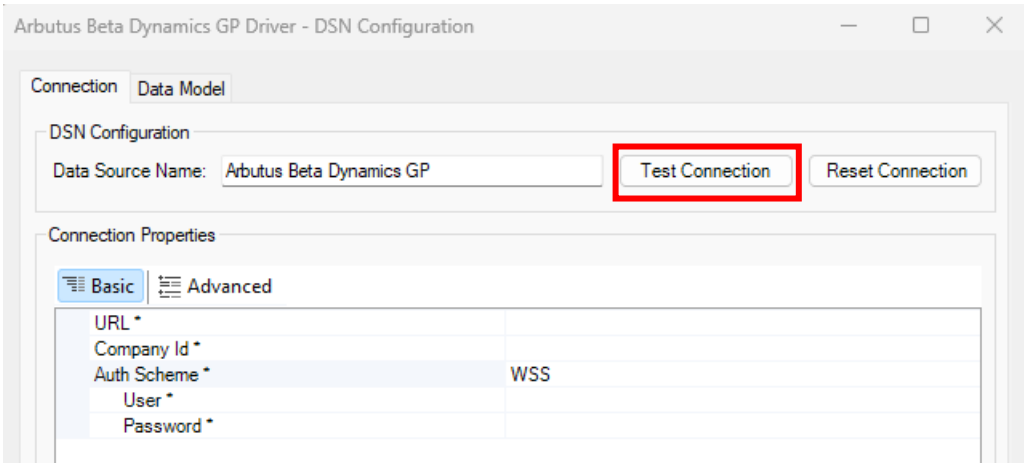
- Kerberos Keytab File – this is the Keytab file containing your pairs of Kerberos principals and encrypted keys.

- Kerberos Ticket Cache – this is the full file path to an MIT Kerberos credential cache file. This property can be set if you wish to use a credential cache file that was created using the MIT Kerberos Ticket Manager or kinit command.

E2. Editing the DSN properties in the Advanced tab

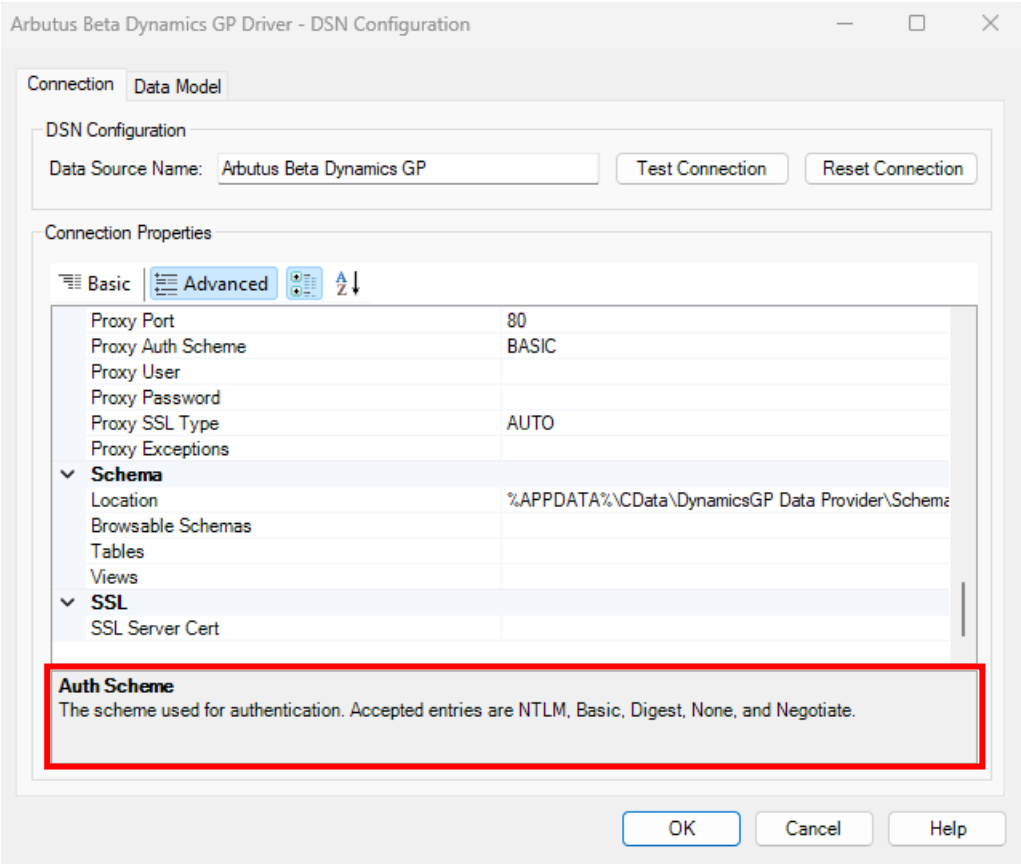
This tab includes more detailed and technical properties. It is intended for those users who need more control over the configuration and are comfortable with more complex options. The **Advanced** tab often includes properties that can fine-tune the behaviour of the system feature.

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 GP 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.