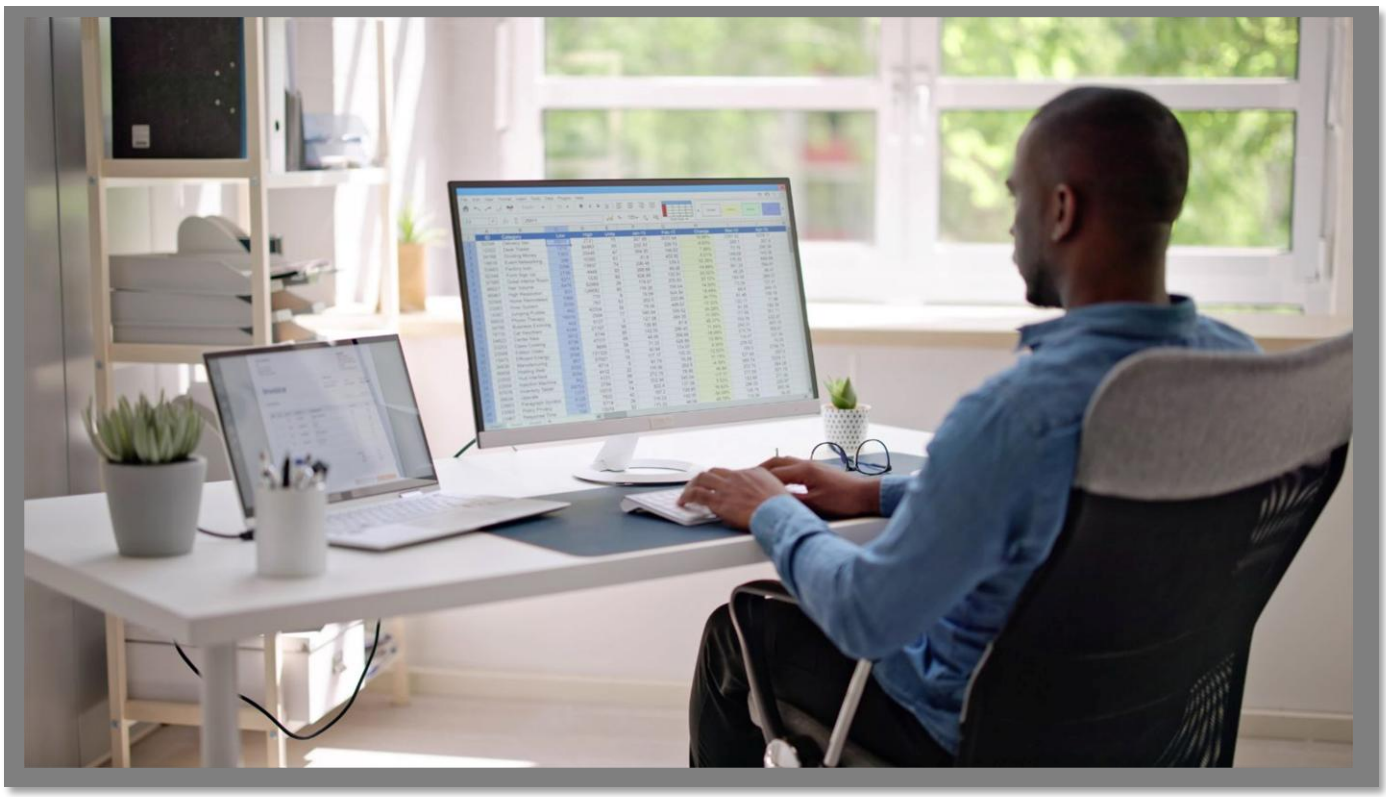
Arbutus Connectors

ServiceNow
CONFIGURATION GUIDE



ARBUTUS
Powerful Analytics Simplified

Contents

Arbutus Connector – ServiceNow

A. Introduction

The purpose of this Guide is to provide assistance with configuring the Arbutus ServiceNow 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 ServiceNow

ServiceNow is a cloud-based platform that helps businesses manage their work more efficiently and streamlining their processes. It automates routine tasks and centralizes operations, making it easier for different departments like IT, HR, and customer service to work together. For example, automating IT services such as incident, problem, and change management, streamlining HR processes such as employee onboarding, enhancing customer support by providing tools for managing customer inquiries, issues, and service requests, monitoring and managing IT infrastructure, identifying and responding to security threats, and so on.

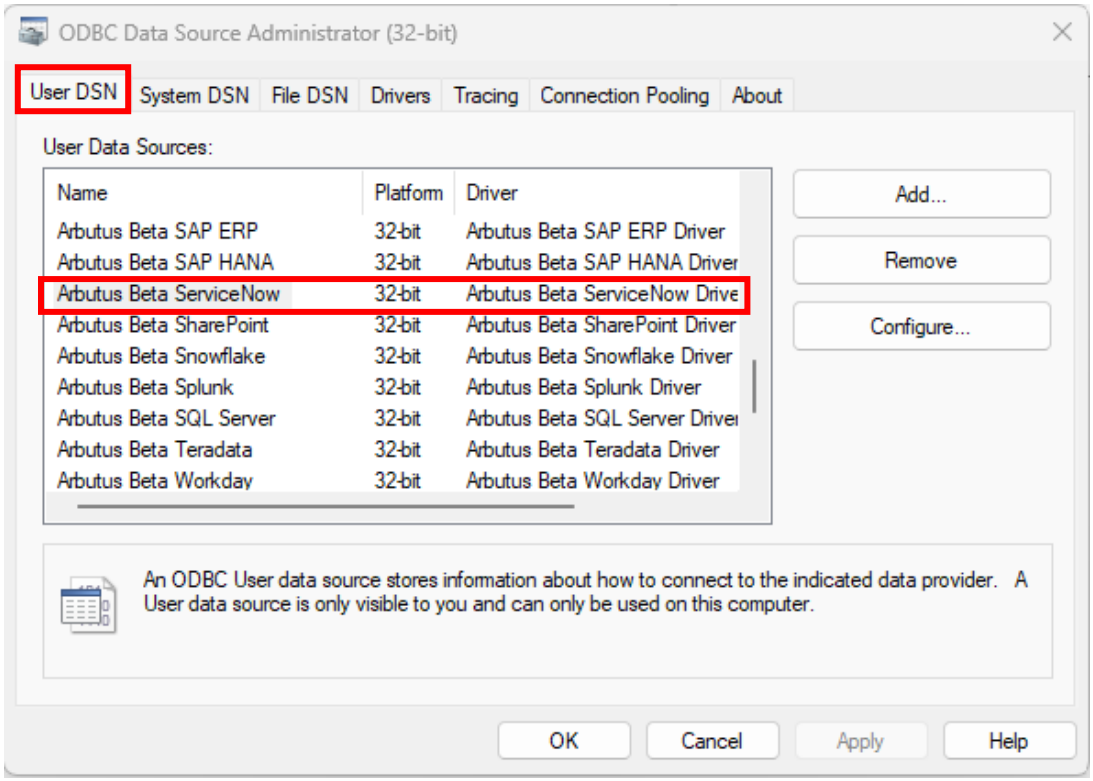
ServiceNow stores structured data in a relational database, where data is organized into tables.

C. Determining if the Connector exists prior to configuring

Installation of the Arbutus ServiceNow 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 ServiceNow 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.

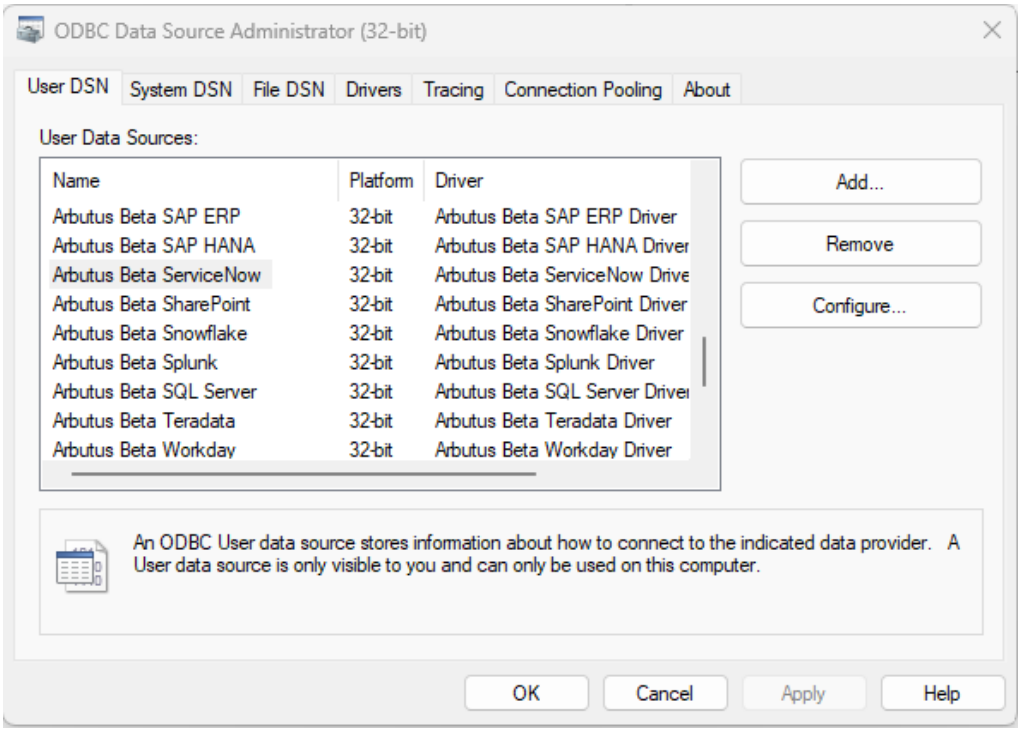
Each of these DSNs has a tab in the **ODBC Data Source Administrator** dialog.

The Arbutus ODBC Driver for ServiceNow enables real-time access to ServiceNow 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**.



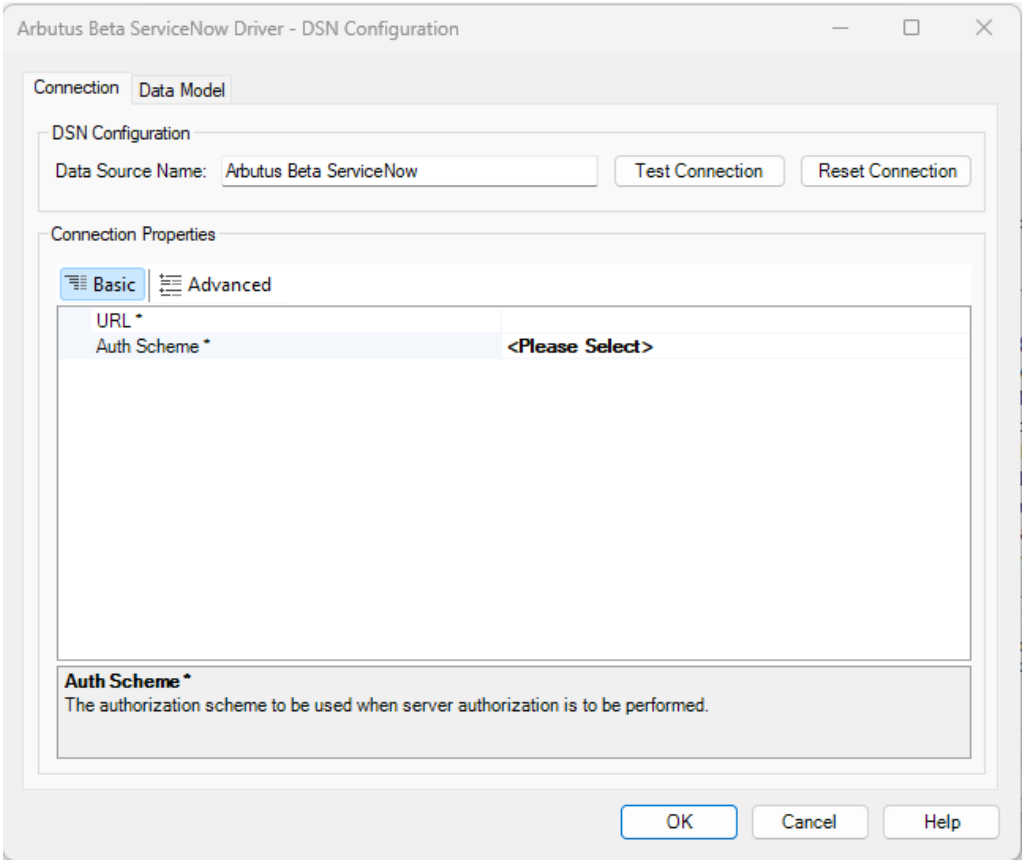
2. Click the **User DSN** tab.

   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 ServiceNow**

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

This opens the **Arbutus ServiceNow Driver – DSN Configuration** dialog.



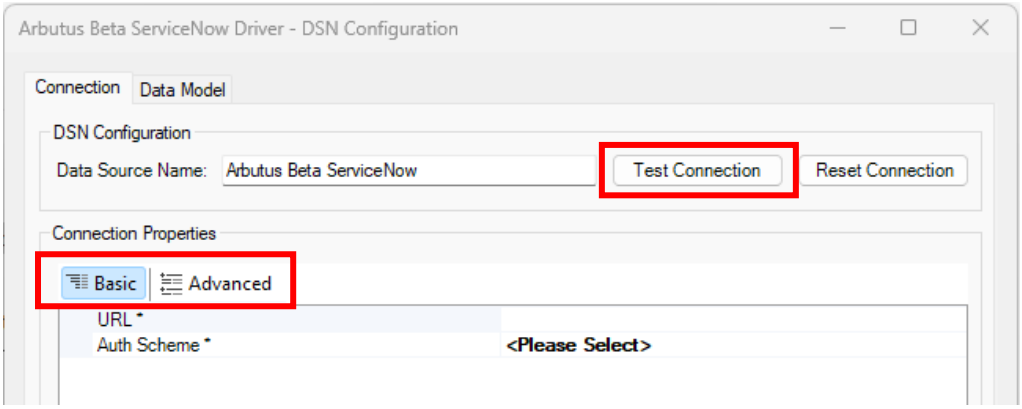
E. Editing the DSN properties – the Basic and Advanced tabs

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 **URL** (per screenshot below) to match the URL of the ServiceNow instance.

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



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

1. **URL** – this is the base URL of your ServiceNow instance. For example: https://dev47813.service-now.com/.

2. **Auth Scheme** – select from the dropdown list the appropriate authorization scheme to be used when server authorization is to be performed. The options available for selection are as follows:
   - Basic – select this when you want to authenticate using a **username and password** combination. This method is straightforward and commonly used for connecting to ServiceNow instances, especially when you have user credentials set up with the necessary permissions to access the instance.

     This approach is suitable for many scenarios, including local development and environments where you manage user credentials directly.

- OAuth – select this when you want to use **OAuth 2.0** for authentication. This method is particularly useful if you want to leverage token-based authentication, which provides enhanced security and allows for seamless integration with various identity providers. OAuth 2.0 is commonly used for single sign-on (SSO) and can help manage access tokens securely.

  This approach is beneficial in scenarios where you need to authenticate users through a third-party identity provider or when you want to avoid managing passwords directly.

- OAuth Password – select this when you want to use **OAuth 2.0** authentication with the **password grant type**. This method is useful if you want to leverage token-based authentication while still using a username and password to obtain the OAuth token. It provides enhanced security by using tokens instead of directly managing passwords for each session

  This approach is beneficial in scenarios where you need to authenticate users through a third-party identity provider that supports OAuth 2.0, and you want to avoid managing passwords directly.

- OKTA – select this when you want to use **Okta** for authentication. This is particularly useful if your organization uses Okta for single sign-on (SSO) and identity management. By using Okta, you can leverage its security features, such as multi-factor authentication (MFA), to enhance the security of your ServiceNow connections.

This method allows users to authenticate with their Okta credentials, providing a seamless and secure login experience.

Note:
Okta is a widely used cloud-based identity and access management (IAM) service that provides secure identity management and Single Sign-On (SSO) solutions. It helps organizations manage user authentication and authorization across various applications and services, ensuring secure access and streamlined user experience.

- ADFS – select this when you want to use **Active Directory Federation Services (ADFS)** for authentication. This is particularly useful if your organization uses ADFS for single sign-on (SSO) and identity management. By using ADFS, you can leverage its security features to enhance the security of your ServiceNow connections.

  This method allows users to authenticate with their ADFS credentials, providing a seamless and secure login experience.

- OneLogin – select this when you want to use **OneLogin** for authentication. This is particularly useful if your organization uses OneLogin for single sign-on (SSO) and identity management. By using OneLogin, you can leverage its security features, such as multi-factor authentication (MFA), to enhance the security of your ServiceNow connections.

  This method allows users to authenticate with their OneLogin credentials, providing a seamless and secure login experience.

- Ping Federate- select this when you want to use **Ping Identity PingFederate** for authentication. This is particularly useful if your organization uses PingFederate for single sign-on (SSO) and identity management. By using PingFederate, you can leverage its security features to enhance the security of your ServiceNow connections.

This method allows users to authenticate with their PingFederate credentials, providing a seamless and secure login experience.

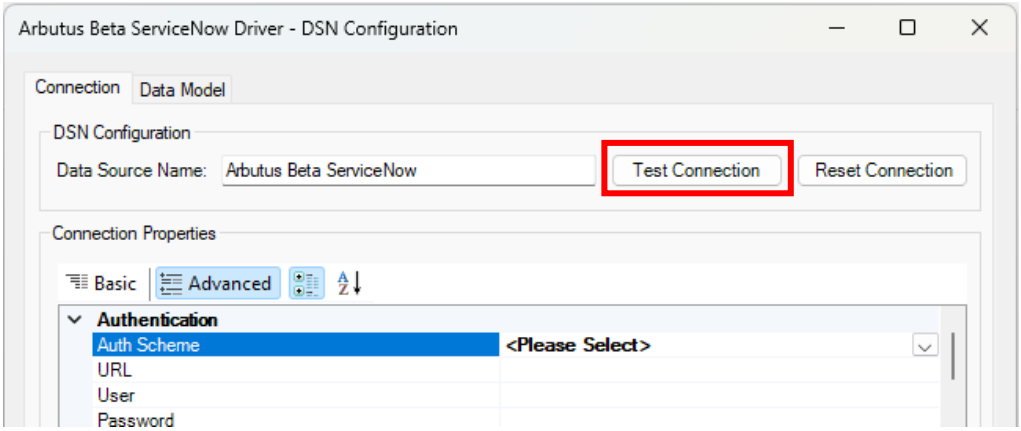
Note:
PingFederate is a highly regarded enterprise federation server that specializes in user authentication and providing standardized single sign-on (SSO) solutions.

The default value is **Basic**.

E2. Editing the DSN properties in the Advanced tab

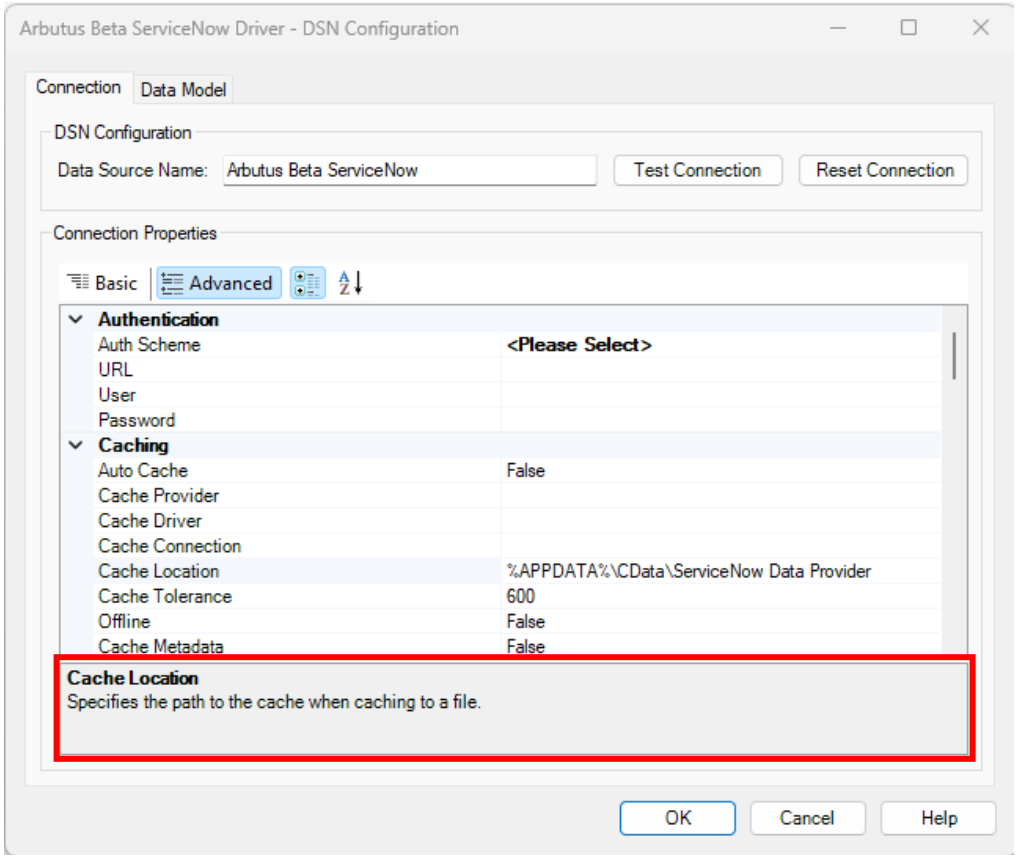
This tab includes more detailed and technical properties. It is intended for those users who need more control over the configuration and are comfortable with more complex options. The **Advanced** tab often includes properties that can fine-tune the behaviour of the system feature.

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 ServiceNow 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.