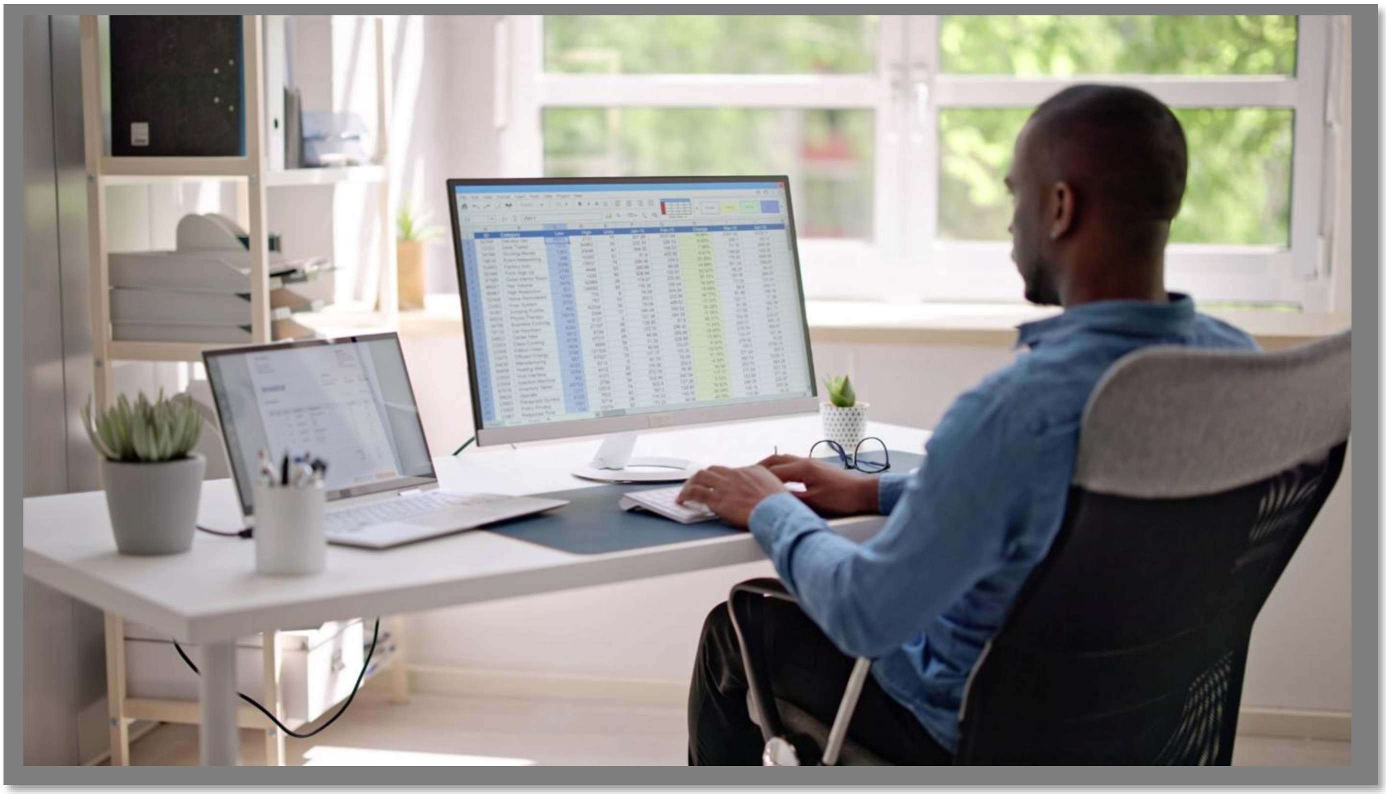
Arbutus Connectors

SharePoint

CONFIGURATION GUIDE



ARBUTUS

Powerful Analytics Simplified

Contents

Arbutus Connector – SharePoint

A. Introduction

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

SharePoint is a web-based collaboration platform developed by Microsoft. It allows organizations to create websites for sharing information, managing documents, and collaborating on projects. Key features include document storage and management, intranet portals, social networking, and business intelligence tools. SharePoint integrates seamlessly with Microsoft Office and other Microsoft services.

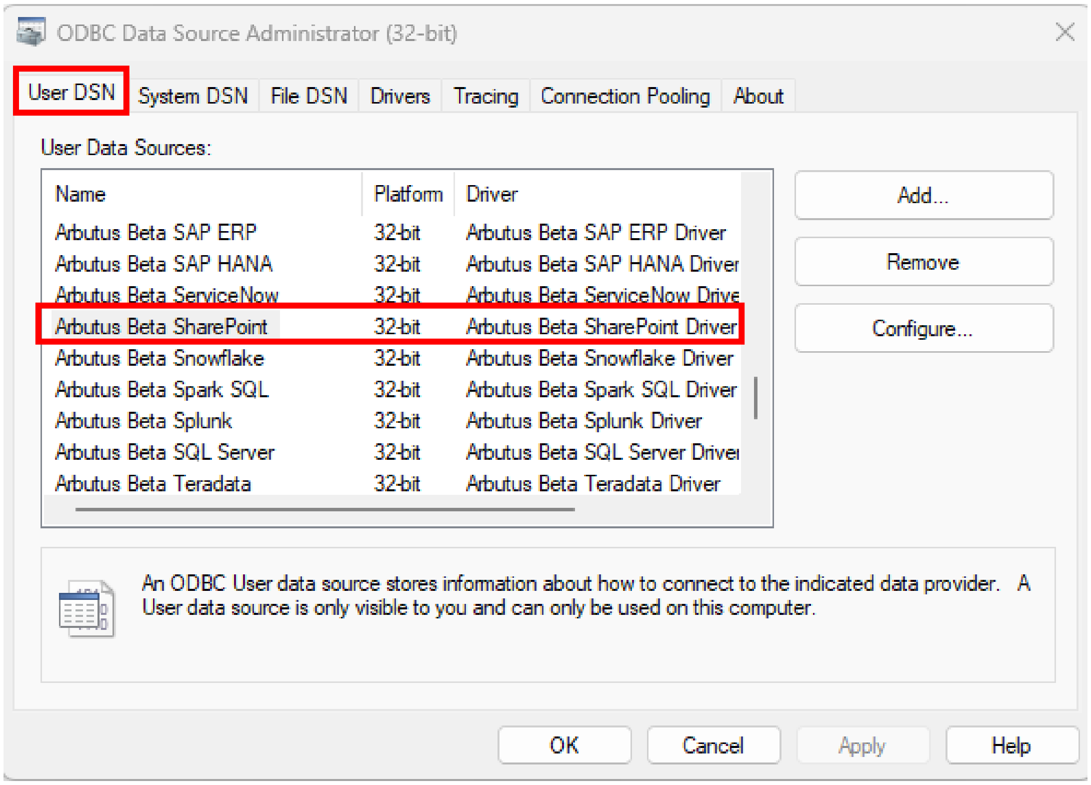
Data in SharePoint is stored in databases. Specifically, SharePoint uses SQL Server databases to store its data. For SharePoint Online, data is also stored in Azure SQL Database and Azure Blob Storage.

C. Determining if the Connector exists prior to configuring

Installation of the Arbutus SharePoint 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**.



Name	Platform	Driver
Arbutus Beta SAP ERP	32-bit	Arbutus Beta SAP ERP Driver
Arbutus Beta SAP HANA	32-bit	Arbutus Beta SAP HANA Driver
Arbutus Beta ServiceNow	32-bit	Arbutus Beta ServiceNow Drive
Arbutus Beta SharePoint	32-bit	Arbutus Beta SharePoint Driver
Arbutus Beta Snowflake	32-bit	Arbutus Beta Snowflake Driver
Arbutus Beta Spark SQL	32-bit	Arbutus Beta Spark SQL Driver
Arbutus Beta Splunk	32-bit	Arbutus Beta Splunk Driver
Arbutus Beta SQL Server	32-bit	Arbutus Beta SQL Server Drive
Arbutus Beta Teradata	32-bit	Arbutus Beta Teradata Driver

An ODBC User data source stores information about how to connect to the indicated data provider. A User data source is only visible to you and can only be used on this computer.

- If the Arbutus SharePoint 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.

- ***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.

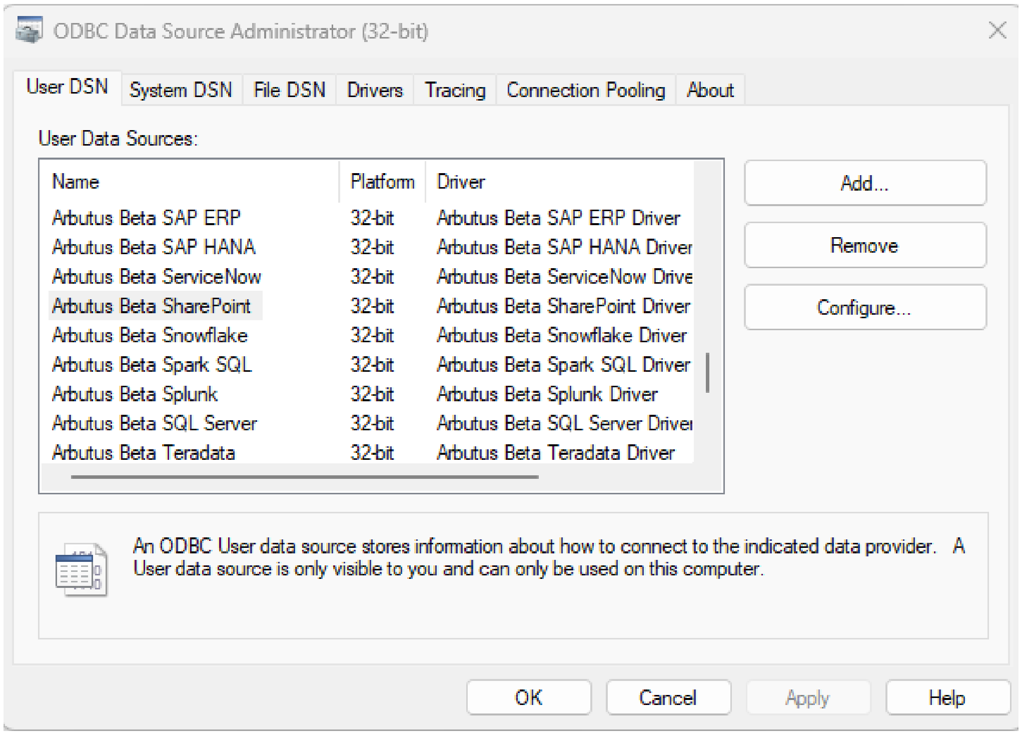
Each of these DSNs has a tab in the **ODBC Data Source Administrator** dialog.

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



Name	Platform	Driver
Arbutus Beta SAP ERP	32-bit	Arbutus Beta SAP ERP Driver
Arbutus Beta SAP HANA	32-bit	Arbutus Beta SAP HANA Driver
Arbutus Beta ServiceNow	32-bit	Arbutus Beta ServiceNow Drive
Arbutus Beta SharePoint	32-bit	Arbutus Beta SharePoint Driver
Arbutus Beta Snowflake	32-bit	Arbutus Beta Snowflake Driver
Arbutus Beta Spark SQL	32-bit	Arbutus Beta Spark SQL Driver
Arbutus Beta Splunk	32-bit	Arbutus Beta Splunk Driver
Arbutus Beta SQL Server	32-bit	Arbutus Beta SQL Server Driver
Arbutus Beta Teradata	32-bit	Arbutus Beta Teradata Driver

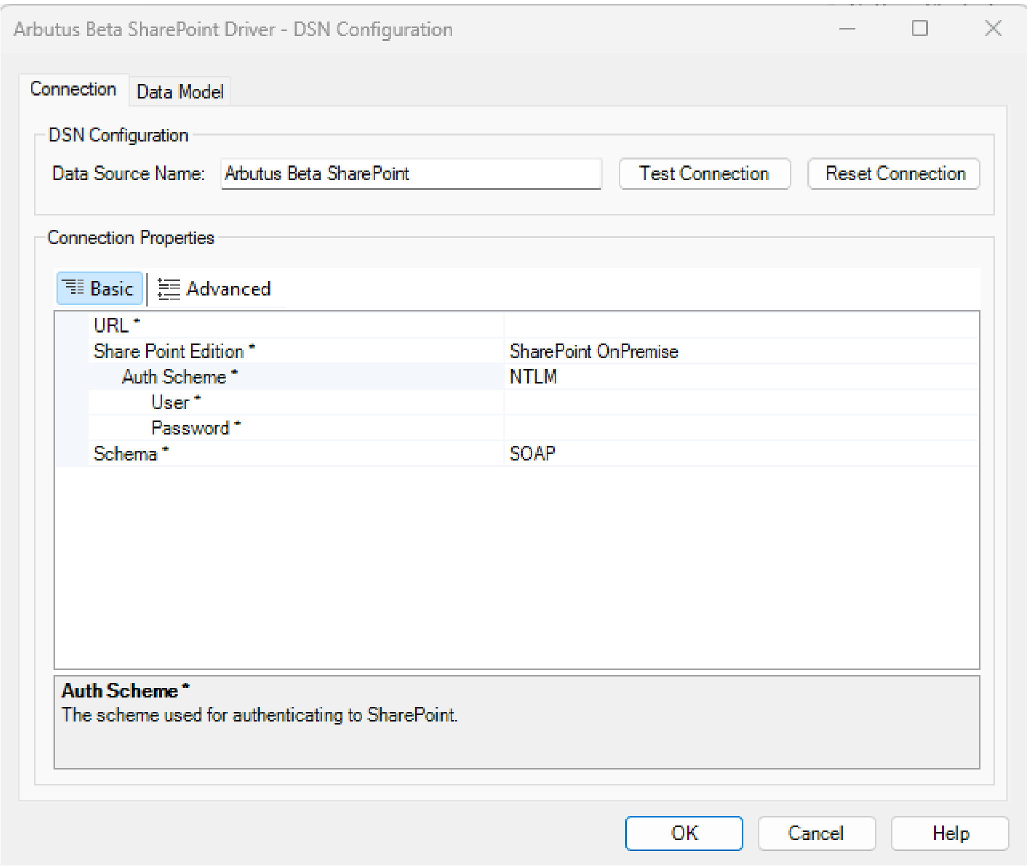
An ODBC User data source stores information about how to connect to the indicated data provider. A User data source is only visible to you and can only be used on this computer.

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 SharePoint.**

3. Select the Arbutus Connector, in this case it is **Arbutus SharePoint**.
4. Click **Configure**.
   This opens the **Arbutus SharePoint Driver – DSN Configuration** dialog.



Arbutus Beta SharePoint Driver - DSN Configuration

DSN Configuration

Data Source Name: Arbutus Beta SharePoint

Connection Properties

URL *	
Share Point Edition *	SharePoint OnPremise
Auth Scheme *	NTLM
User *	
Password *	
Schema *	SOAP

Auth Scheme *
The scheme used for authenticating to SharePoint.

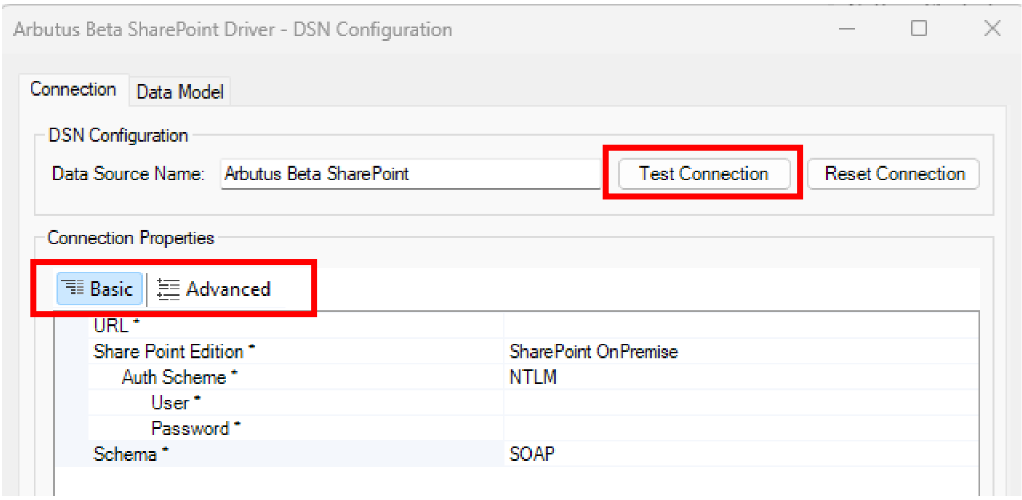
E. Editing the DSN properties – the Basic and Advanced tabs

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



Data Source Name: Arbutus Beta SharePoint

URL *	
Share Point Edition *	SharePoint OnPremise
Auth Scheme *	NTLM
User *	
Password *	
Schema *	SOAP

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

1. **URL** – this is the base URL for the site. The following are examples of valid URLs:
   - http://server/SharePoint/
   - http://server/Sites/mysite/
   - http://server:90/

2. **Share Point Edition** – click the dropdown to select from the list the edition of SharePoint being used. The options available are:
   - ○ SharePoint OnPremise – select this when you are connecting to a SharePoint environment that is hosted on your organization's local servers, rather than in the cloud.

   - ○ SharePoint Online – select this when you are connecting to a SharePoint environment that is hosted in the cloud, specifically through Microsoft's SharePoint Online service.

The default value is **SharePoint OnPremise**.

For both these properties, you have to specify the scheme used for authenticating to SharePoint. This is done via the **Auth Scheme** property.

If **SharePoint OnPremise** is selected, there are five different authenticating schemes you could chose from:

- NTLM (Windows NT LAN Manager - **default**) – select this when you want to use your Windows credentials for authentication to a SharePoint environment. This setup is typically chosen for environments where integrated Windows authentication is preferred.

  Selecting **NTLM** requires you to specify the User and Password.

  - User – this is the SharePoint user account used to authenticate.

    Together with **Password**, this field is used to authenticate against the SharePoint server.

    For SharePoint OnPremise, User should include the domain and will look similar to the following: DOMAIN\Username.

  - Password – this is the password used to authenticate the user.

    The **User** and **Password** are together used to authenticate with the server.

- Negotiate – select this when you want to use **Kerberos authentication** for your SharePoint environment. This setup is typically chosen for its strong security features and ability to support single sign-on (SSO).

Selecting **Negotiate** requires you to specify the User and Password.

- User – this is the SharePoint user account used to authenticate.

  Together with **Password**, this field is used to authenticate against the SharePoint server.

  For SharePoint OnPremise, User should include the domain and will look similar to the following: DOMAIN\Username.

- 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** for your SharePoint environment. This setup is typically chosen for accessing public sites or environments where no authentication is required.

○ Basic – select this when you want to use **HTTP Basic authentication** for your SharePoint environment. This setup is typically chosen for its simplicity and ease of use, especially in environments where security requirements are not stringent.

Selecting **Basic** requires you to specify the User and Password.

- User – this is the SharePoint user account used to authenticate.

  Together with **Password**, this field is used to authenticate against the SharePoint server.

For SharePoint OnPremise, User should include the domain and will look similar to the following: DOMAIN\Username.

- Password – this is the password used to authenticate the user.

  The **User** and **Password** are together used to authenticate with the server.

- ADFS (Active Directory Federation Services) – select this when you are using **ADFS** as your Single Sign-On (SSO) provider for SharePoint. This setup is typically chosen for enhanced security and streamlined user authentication.

  Selecting **ADFS** requires you to specify the User, Password, and SSO Domain.

  - User – this is the SharePoint user account used to authenticate.

    Together with **Password**, this field is used to authenticate against the SharePoint server.

    For SharePoint OnPremise, User should include the domain and will look similar to the following: DOMAIN\Username.

  - Password – this is the password used to authenticate the user.

    The **User** and **Password** are together used to authenticate with the server.

  - SSO Domain – this is the domain of the user when using single sign-on (SSO).

If **SharePoint Online** is selected, there are twelve different authenticating schemes you could chose from:

- OAuth (**default**) – select this when you want to use **OAuth 2.0** for authentication to a SharePoint Online environment. This setup is typically chosen for its robust security features and ability to support modern authentication methods.

- AzureAD – select this when you want to use **Azure Active Directory (Azure AD)** for authentication to a SharePoint Online environment. This setup is typically chosen for its robust security features and seamless integration with Microsoft's cloud services.

- Azure Password – select this when you want to use your **Azure credentials directly** for authentication to a SharePoint Online environment. This setup is typically chosen for its simplicity and direct use of Azure AD credentials.

  Selecting **Azure Password** requires you to specify the User, Password, and the Azure Tenant.

  - User – this is the SharePoint user account used to authenticate.

    Together with **Password**, this field is used to authenticate against the SharePoint server.

    For SharePoint Online, User will look similar to the following: username@domain.onmicrosoft.com

  - Password – this is the password used to authenticate the user.

    The **User** and **Password** are together used to authenticate with the server.

    - 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 JWT – select this when you want to use **OAuth 2.0 with JSON Web Tokens (JWT)** for authentication to a SharePoint Online environment. This setup is typically chosen for its robust security features and ability to support modern authentication methods.

Selecting **OAuth JWT** requires you to specify the following:

- Azure Tenant – this is the Microsoft Online tenant being used to access data. If not specified, your default tenant is used.

  For more information, please see the **Azure Tenant** section above in the **Azure Password** section.

- OAuth JWT Cert – this is the JWT Certificate store.

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

  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

  The default value is **USER**.

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

        - OAuth JWT Issuer – this is the issuer of the Java Web Token.

          In most cases, this takes the value of the OAuth App Id (Client Id) connection property and does not need to be individually set.

        - OAuth JWT Cert Password – this is the password of 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.

    - AzureMSI – select this when you want to use **Azure Managed Service Identity** for authentication to a SharePoint Online environment. This setup is typically chosen for its seamless integration with Azure services and enhanced security features.

      To configure this, you need to set the **Auth Scheme to AzureMSI**. The MSI credentials are automatically obtained for authentication, so no additional user credentials are required.

    - Ping Federate – select this when you are using **PingFederate** as your Single Sign-On (SSO) provider for SharePoint Online. This setup is typically chosen for enhanced security and streamlined user authentication.

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

Selecting **Ping Federate** requires you to specify the following:

- User – this is the SharePoint user account used to authenticate.

  Together with **Password**, this field is used to authenticate against the SharePoint server.

  For SharePoint Online, User will look similar to the following: username@domain.onmicrosoft.com

- Password – this is the password used to authenticate the user.

  The **User** and **Password** are together used to authenticate with the server.

- SSO Domain – this is the domain of the user when using single sign-on (SSO).

  This property is only applicable when using single sign-on (**AuthScheme** is configured to use an SSO authentication scheme) and if the domain of the User (e.g. user@mydomain.com) is different than the domain configured within the SSO service (e.g. user@myssodomain.com).

  This property may be required when using the ADFS, OneLogin, or OKTA SSO services.

○ ADFS – select this when you are using **ADFS** as your Single Sign-On (SSO) provider for SharePoint Online. This setup is typically chosen for enhanced security and streamlined user authentication.

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

- User – this is the SharePoint user account used to authenticate.

  Together with **Password**, this field is used to authenticate against the SharePoint server.

  For SharePoint Online, User will look similar to the following: username@domain.onmicrosoft.com

- Password – this is the password used to authenticate the user.

  The **User** and **Password** are together used to authenticate with the server.

- SSO Domain – this is the domain of the user when using single sign-on (SSO).

  For more information, please see the **SSO Domain** section above in the **Ping Federate** section.

○ OneLogin – select this when you are using **OneLogin** as your Single Sign-On (SSO) provider for SharePoint Online. This setup is typically chosen for enhanced security and streamlined user authentication.

Selecting **One Login** requires you to specify the following:

- User – this is the SharePoint user account used to authenticate.

  Together with **Password**, this field is used to authenticate against the SharePoint server.

  For SharePoint Online, User will look similar to the following: username@domain.onmicrosoft.com

- Password – this is the password used to authenticate the user.

  The **User** and **Password** are together used to authenticate with the server.

- SSO Domain – this is the domain of the user when using single sign-on (SSO).

  For more information, please see the **SSO Domain** section above in the **Ping Federate** section.

- OKTA – select this when you are using Okta as your Single Sign-On (SSO) provider for SharePoint Online. This setup is typically chosen for enhanced security and streamlined user authentication.

  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.

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

  - User – this is the SharePoint user account used to authenticate.

    Together with **Password**, this field is used to authenticate against the SharePoint server.

    For SharePoint Online, User will look similar to the following: username@domain.onmicrosoft.com

- Password – this is the password used to authenticate the user.

  The **User** and **Password** are together used to authenticate with the server.

- SSO Domain – this is the domain of the user when using single sign-on (SSO).

  For more information, please see the **SSO Domain** section above in the **Ping Federate** section.

- SharePointOAuth – select this when you want to use **OAuth 2.0** specifically tailored for SharePoint Online. This setup is typically chosen for its robust security features and ability to support modern authentication methods.

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

  - 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**.

  - 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**, 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.

    - OAuth Grant Type – this is the grant type for the OAuth flow. This is a dropdown selection containing the following possible values:
      a. CODE
      b. PASSWORD
      c. SAML_1
      d. CLIENT

      You should base your selection on the specific use case and security requirements of your application. For example, use **CODE** for user-facing applications, **PASSWORD** for trusted first-party apps, **SAML_1** for SAML-based SSO integration, and **CLIENT** for server-to-server communication.

      The default value is **CODE**.

  - NTLM (Windows NT LAN Manager) – select this when you want to use your Windows credentials for authentication to a SharePoint environment. However, NTLM is typically used for on-premise SharePoint environments rather than SharePoint Online.

    For SharePoint Online, other authentication schemes like **AzureAD**, **OAuth**, or **SAML** are more commonly used due to their compatibility with cloud environments.

    Selecting **NTLM** requires you to specify the following:
    - User – this is the SharePoint user account used to authenticate.

      Together with **Password**, this field is used to authenticate against the SharePoint server.

      For SharePoint Online, User will look similar to the following: username@domain.onmicrosoft.com

- 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** for your SharePoint Online environment. This setup is typically chosen for its simplicity and ease of use, especially in environments where security requirements are not stringent.

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

  - User – this is the SharePoint user account used to authenticate.

    Together with **Password**, this field is used to authenticate against the SharePoint server.

    For SharePoint Online, User will look similar to the following: username@domain.onmicrosoft.com

  - Password – this is the password used to authenticate the user.

    The **User** and **Password** are together used to authenticate with the server.

3. **Schema** – this is a dropdown selection containing the following two possible values to identify the type of schema to use.
   - SOAP (Simple Object Access Protocol) - If you are working with older systems or applications that were built using SOAP, it might be necessary to select this option for compatibility.

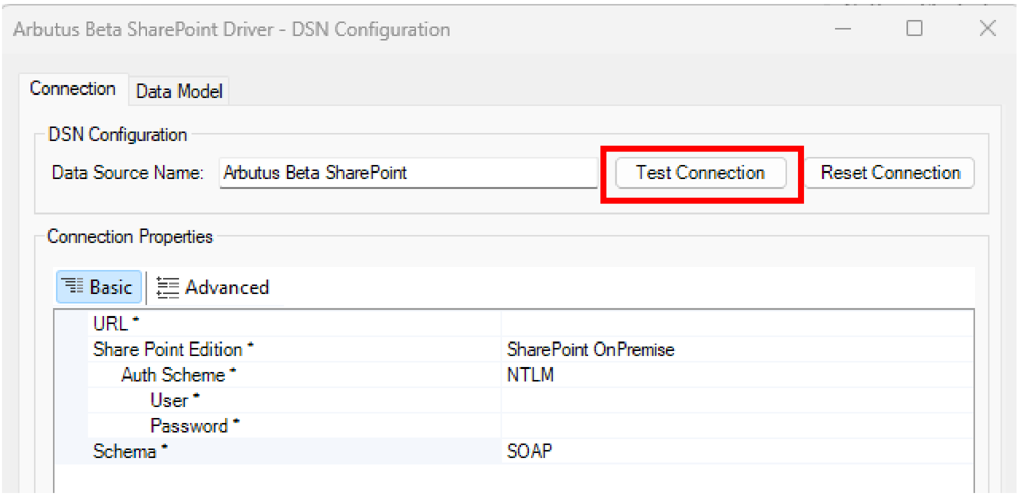
- REST (Representative State Transfer) - If you are working with modern applications and services, REST is often preferred due to its simplicity and ease of use.

In summary, consider choosing **SOAP** for legacy systems, formal standards, and complex operations, and choosing **REST** for modern applications, lightweight interactions, and direct access to SharePoint objects.

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 SharePoint system by clicking the **Test Connection** button.

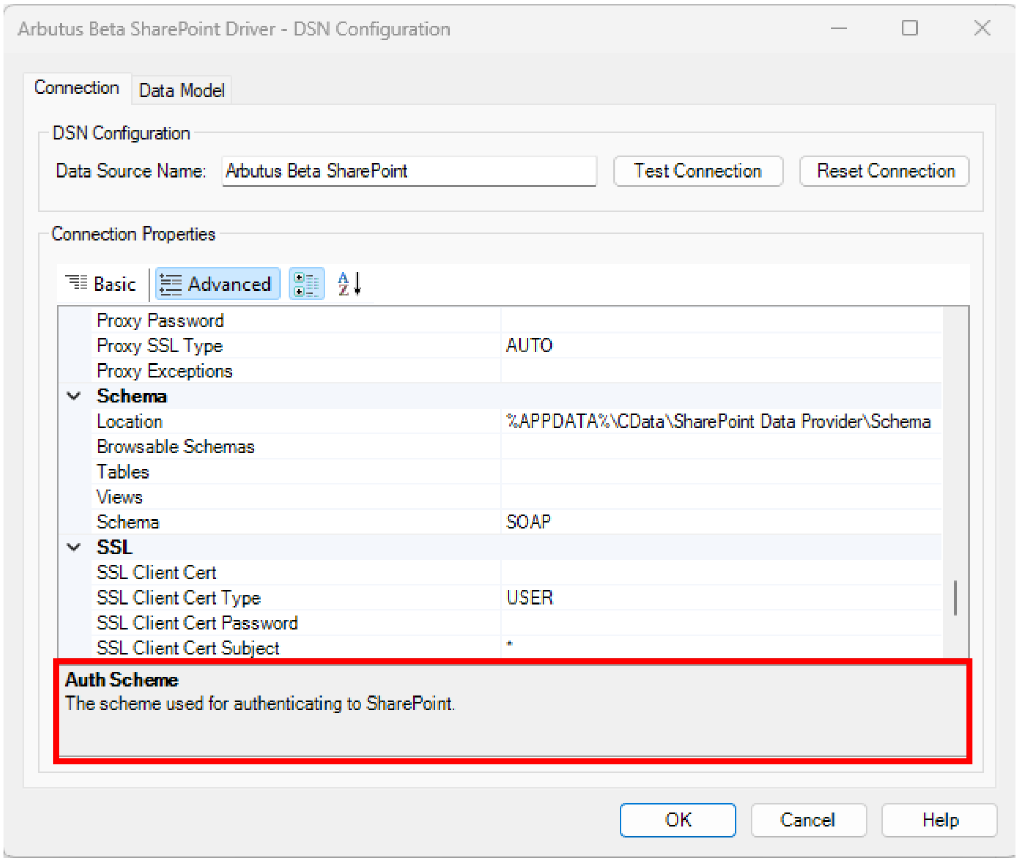


Data Source Name: Arbutus Beta SharePoint

URL *	
Share Point Edition *	SharePoint OnPremise
Auth Scheme *	NTLM
User *	
Password *	
Schema *	SOAP

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 Beta SharePoint Driver - DSN Configuration

DSN Configuration

Data Source Name: Arbutus Beta SharePoint

Connection Properties

Proxy Password	
Proxy SSL Type	AUTO
Proxy Exceptions	
Schema	
Location	%APPDATA%\CData\SharePoint Data Provider\Schema
Browsable Schemas	
Tables	
Views	
Schema	SOAP
SSL	
SSL Client Cert	
SSL Client Cert Type	USER
SSL Client Cert Password	
SSL Client Cert Subject	*

Auth Scheme
The scheme used for authenticating to SharePoint.

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.