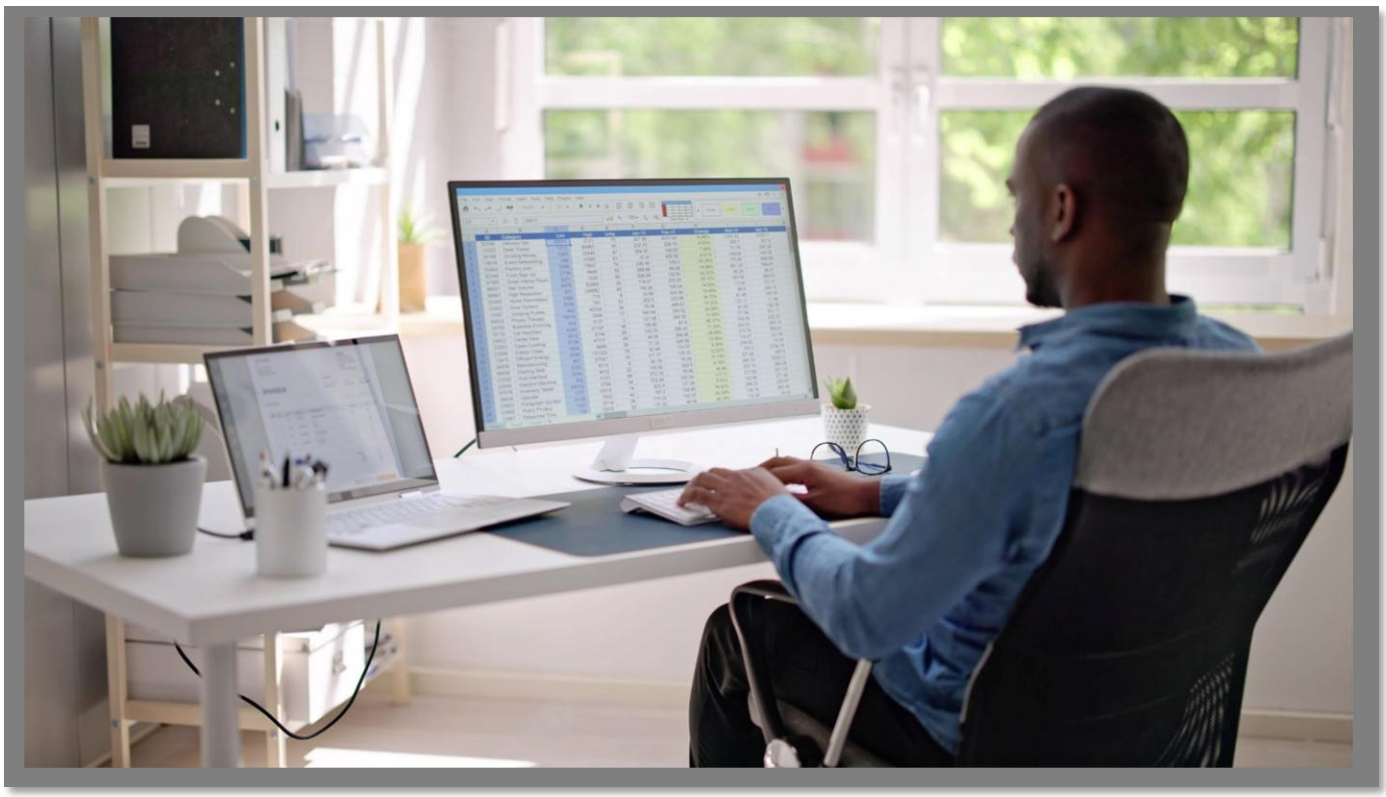
Arbutus Connectors

MS Exchange
CONFIGURATION GUIDE



ARBUTUS
Powerful Analytics Simplified

Contents

Arbutus Connector – MS Exchange

A. Introduction

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

Microsoft Exchange is a messaging platform that provides email, calendar, contacts, and tasks. It can be accessed from PCs, the web, and mobile devices. Exchange is often used in business and educational environments to manage communication and collaboration efficiently. It integrates with Microsoft 365 and can be hosted on-premises or used as a cloud service through Exchange Online. Where your data is stored depends on whether you are using**:**

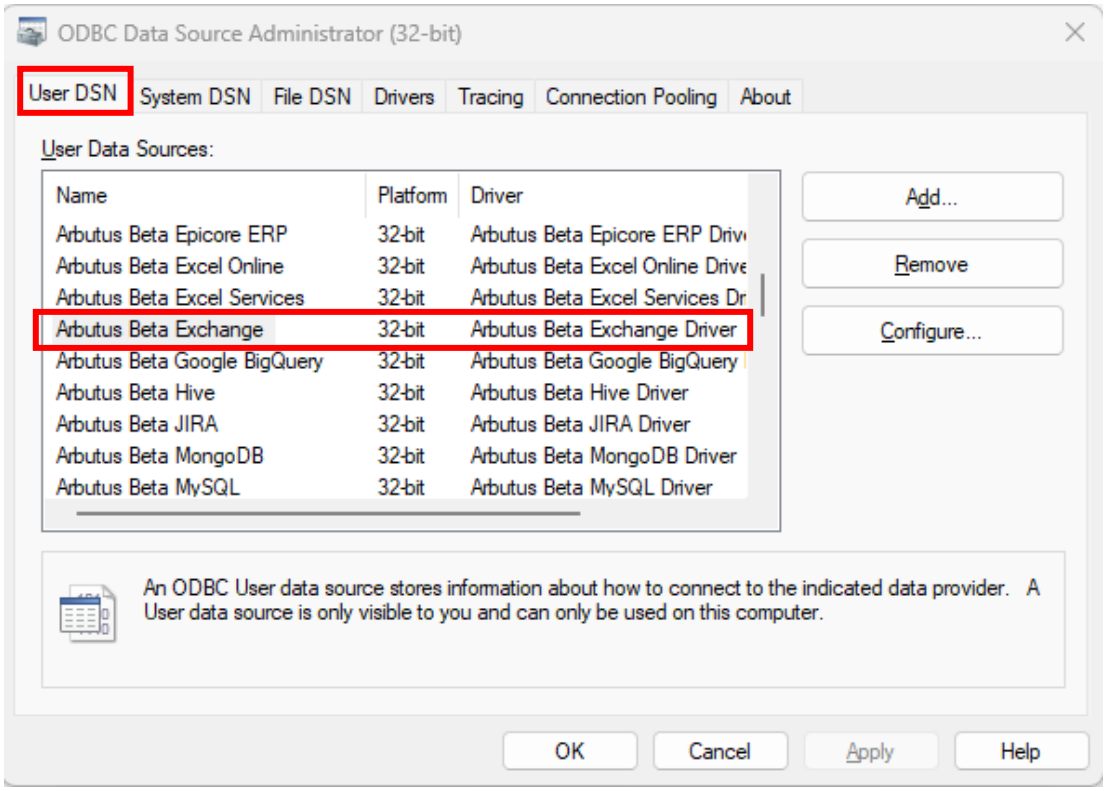
- **Exchange Online (Microsoft 365) -** data is stored in Microsoft's cloud data centres located worldwide. Microsoft determines the location based on your region and compliance requirements.
- **On-premise Exchange Server -** data is stored on your company's local servers or in a private cloud.

C. Determining if the Connector exists prior to configuring

Installation of the Arbutus Exchange 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 Exchange 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.

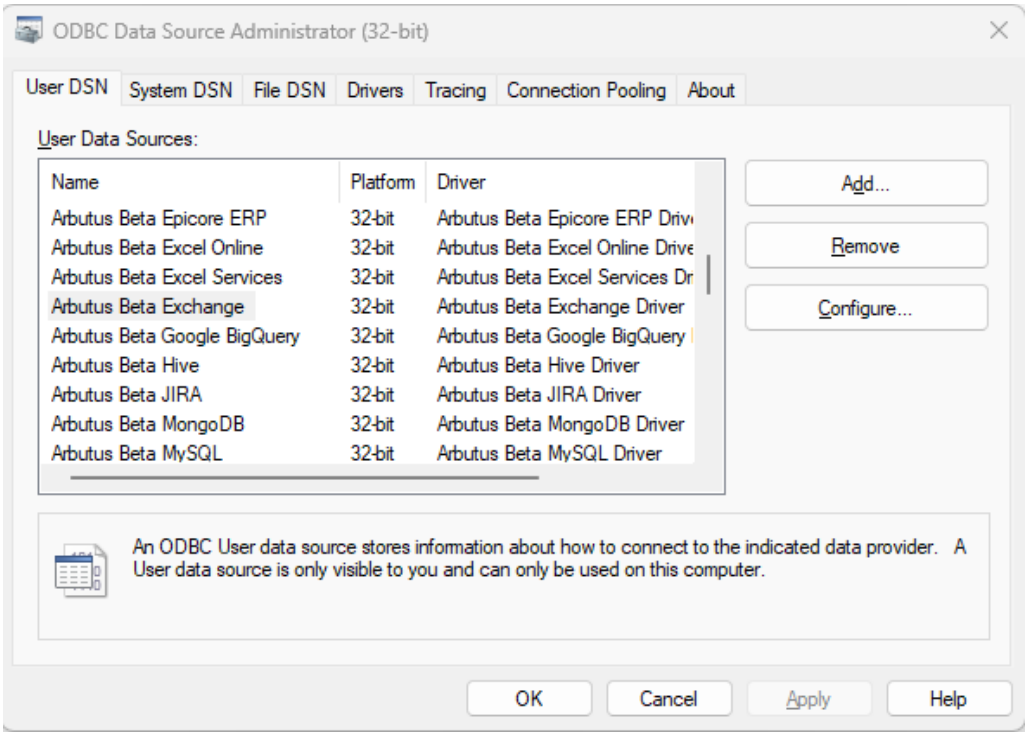
Each of these DSNs has a tab in the **ODBC Data Source Administrator** dialog.

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



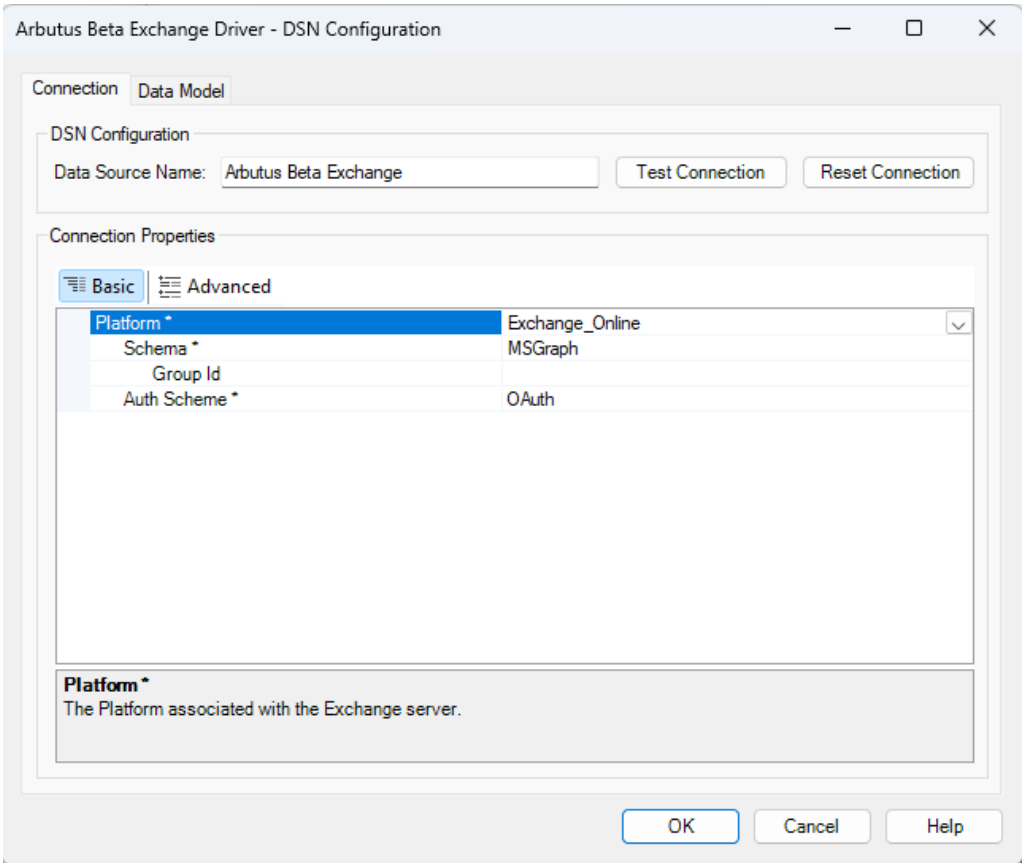
2. Click the **User DSN** tab.

   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 Exchange.**

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

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



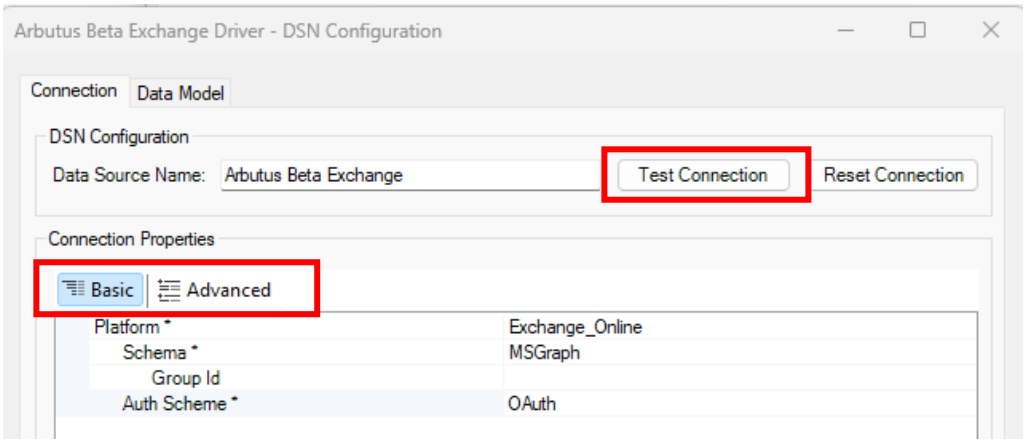
E. Editing the DSN properties – the Basic and Advanced tabs

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 **Auth Scheme** property (per screenshot below) to specify the scheme used for authentication.

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



In the **Basic** tab, there is **one** main property, with different underlying properties, to review:

1. **Platform** – this is the platform associated with the Exchange server. This is a dropdown selection consisting of the following eight possible platforms from which you can select:
   - Exchange Online
   - Exchange2007
   - Exchange2007 SP1
   - Exchange2010
   - Exchange2010 SP1
   - Exchange2010 SP2
   - Exchange2013
   - Exchange2013 SP1

   Each of the above have their own set of underlying properties for editing, and each of them are described below.

   The default value is **Exchange Online**.

If **Exchange Online** is selected, the following properties are listed for editing:

- Schema – specify the Microsoft Exchange schema. This is a dropdown selection consisting of the following two possible schemas that you can choose from:
  - MSGraph – select MSGraph when you want to use **Microsoft Graph API** for accessing and managing your Exchange Online data.

    Selecting **MSGraph** requires you to specify the following:
    - Group ID – specify this Group Id in order to access the OneNote documents for this group.

  - EWS – select EWS (Exchange Web Services) when you want to use EWS for accessing and managing your Exchange Online data. EWS is a robust API that allows you to interact with various Exchange Online features, such as email, calendar, contacts, and tasks.

    Selecting **EWS** requires you to specify the following
    - Server – this is the address of the Exchange server to which you are connecting.

  The default value is **EWS**.

- Auth Scheme – this is the scheme used for authentication. This is a dropdown selection consisting of the following five possible authentication schemes you can choose from:
  - OAuth – select this when you want to use **OAuth 2.0** for authentication. OAuth 2.0 provides a more secure authentication method by using tokens instead of handling user credentials directly. As it is part of modern authentication protocols, it supports multi-factor authentication (MFA).

    The default value is **OAuth**.

- AzureAD – select this when you want to use **Azure Active Directory (Azure AD)** for authentication. Azure AD provides advanced security features, such as multi-factor authentication (MFA) and conditional access policies, which help protect your data.

- AzureMSI – select this when you want to use **Azure Managed Service Identity (MSI)** for authentication. Azure MSI allows your application to automatically obtain and manage credentials, reducing the need for manual handling of secrets and credentials.

- AzureServicePrincipal – select this when you want to authenticate using an **Azure Service Principal.** Azure Service Principals are ideal for scenarios involving unattended scripts and automation, as they allow applications to authenticate without user interaction.

- AzureServicePrincipalCert – select this when you want to authenticate using an **Azure Service Principal with a certificate.** Using a certificate for authentication is more secure than using a client secret, as certificates are harder to compromise and can be managed more securely.

If **Exchange2007** is selected, the following properties are listed for editing:

- Schema - specify the Microsoft Exchange schema. This is a dropdown selection consisting of just a single schema that you can choose from:
  - EWS – select EWS (Exchange Web Services) when you want to use EWS for accessing and managing your Exchange Online data. EWS is a robust API that allows you to interact with various Exchange Online features, such as email, calendar, contacts, and tasks.

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

- Server – this is the address of the Exchange server to which you are connecting.

- Auth Scheme - this is the scheme used for authentication. This is a dropdown selection consisting of the following five possible authentication schemes you can choose from:
  - Basic – select this when you want to use **basic authentication**. Basic authentication is easy to set up and use, requiring only a username and password for access.

    However, it's important to note that basic authentication is less secure compared to modern authentication methods, as it involves sending credentials in plain text (though typically over a secure connection). For newer versions of Exchange or more secure environments, consider using modern authentication methods like OAuth.

    Selecting **Basic** requires you to specify the following:
    - User – this is the user who is authenticating to the Exchange site.
    - Password – this is the password used to authenticate to the Exchange site.

    The default value is **Basic**.

  - NTLM – select this when you want to use **NTLM (Windows NT LAN Manager)** authentication. NTLM is supported by Exchange 2007 and is often used in environments where older systems or applications are in place. NTLM allows for integrated Windows authentication, which can be useful in on-premises environments where users are already authenticated to the domain.

However, it's important to note that NTLM is considered less secure compared to modern authentication methods like OAuth. If possible, consider using more secure options for newer systems.

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

- ➢ User – this is the user who is authenticating to the Exchange site.

- ➢ Password – this is the password used to authenticate to the Exchange site.

- Digest – select this when you want to use **HTTP Digest** authentication. Digest authentication is more secure than basic authentication because it hashes the credentials before sending them over the network, reducing the risk of credential theft. Digest can be used in environments where integrated Windows authentication is required, providing a balance between security and ease of use.

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

  - ➢ User – this is the user who is authenticating to the Exchange site.

  - ➢ Password – this is the password used to authenticate to the Exchange site.

- Negotiate – select this when you want to use **Kerberos or NTLM** authentication. Kerberos, which is preferred by Negotiate, is more secure than NTLM and provides mutual authentication, ensuring both the client and server verify each other's identity. Negotiate allows for integrated Windows authentication, which can automatically select between Kerberos and NTLM based on what is available and configured in your environment.

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

- User – this is the user who is authenticating to the Exchange site.

- Password – this is the password used to authenticate to the Exchange site.

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

  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 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.

- None – select this when you do not require any authentication for accessing the Exchange server. An example of a scenario where this might be applicable is:
  - Internal testing - If you are setting up a test environment within a secure, isolated network where authentication is not necessary, you might use the None option to simplify the setup.

  However, it's important to note that using no authentication poses significant security risks and should be avoided in production environments. Always consider using more secure authentication methods whenever possible.

If **Exchange2007_SP1** is selected, the same set of properties as described in the section above under **Exchange2007** are listed for editing. Please refer to the **Exchange2007** section above for more information.

If **Exchange2010** is selected, the same set of properties as described in the section above under **Exchange2007** are listed for editing. Please refer to the **Exchange2007** section above for more information.

If **Exchange2010_SP1** is selected, the same set of properties as described in the section above under **Exchange2007** are listed for editing. Please refer to the **Exchange2007** section above for more information.

If **Exchange2010_SP2** is selected, the same set of properties as described in the section above under **Exchange2007** are listed for editing. Please refer to the **Exchange2007** section above for more information.

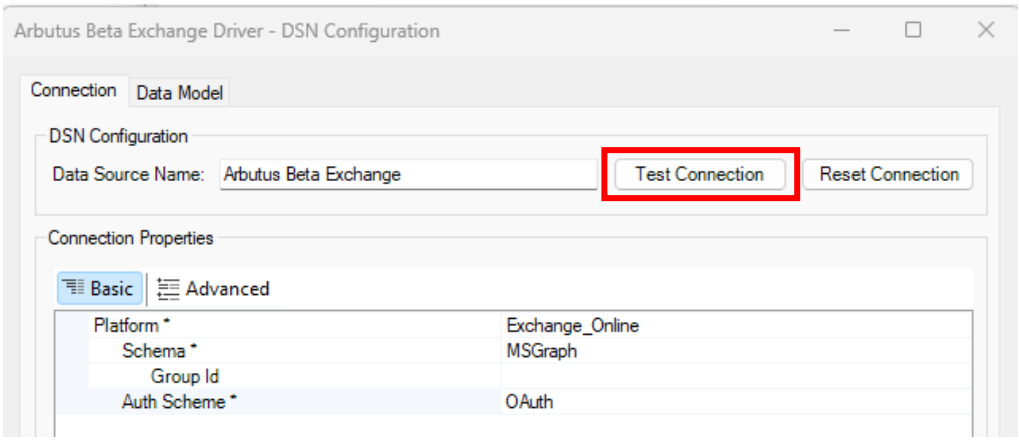
If **Exchange2013** is selected, the same set of properties as described above under **Exchange2007** are listed for editing. Please refer to the **Exchange2007** section above for more information.

If **Exchange2013_SP1** is selected, the same set of properties as described above under **Exchange2007** are listed for editing. Please refer to the **Exchange2007** section above for more information.

E2. Editing the DSN properties in the Advanced tab

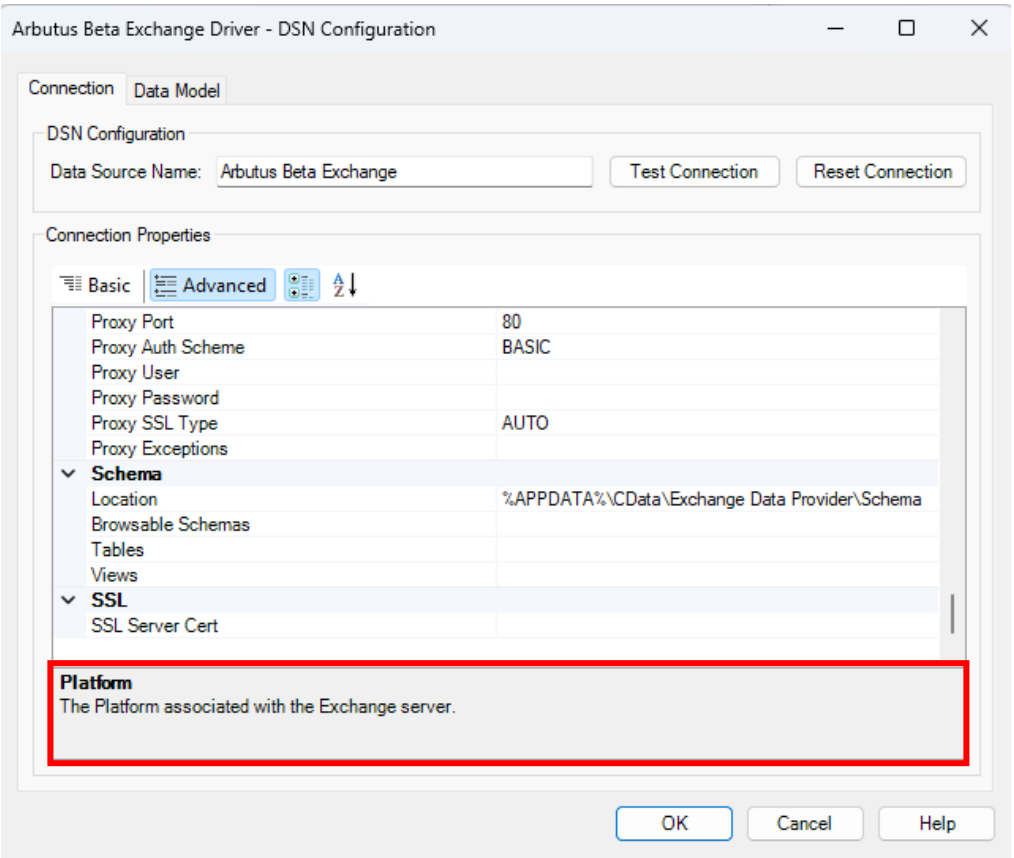
This tab includes more detailed and technical properties. It is intended for those users who need more control over the configuration and are comfortable with more complex options. The **Advanced** tab often includes properties that can fine-tune the behaviour of the system feature.

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 Microsoft Exchange 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.