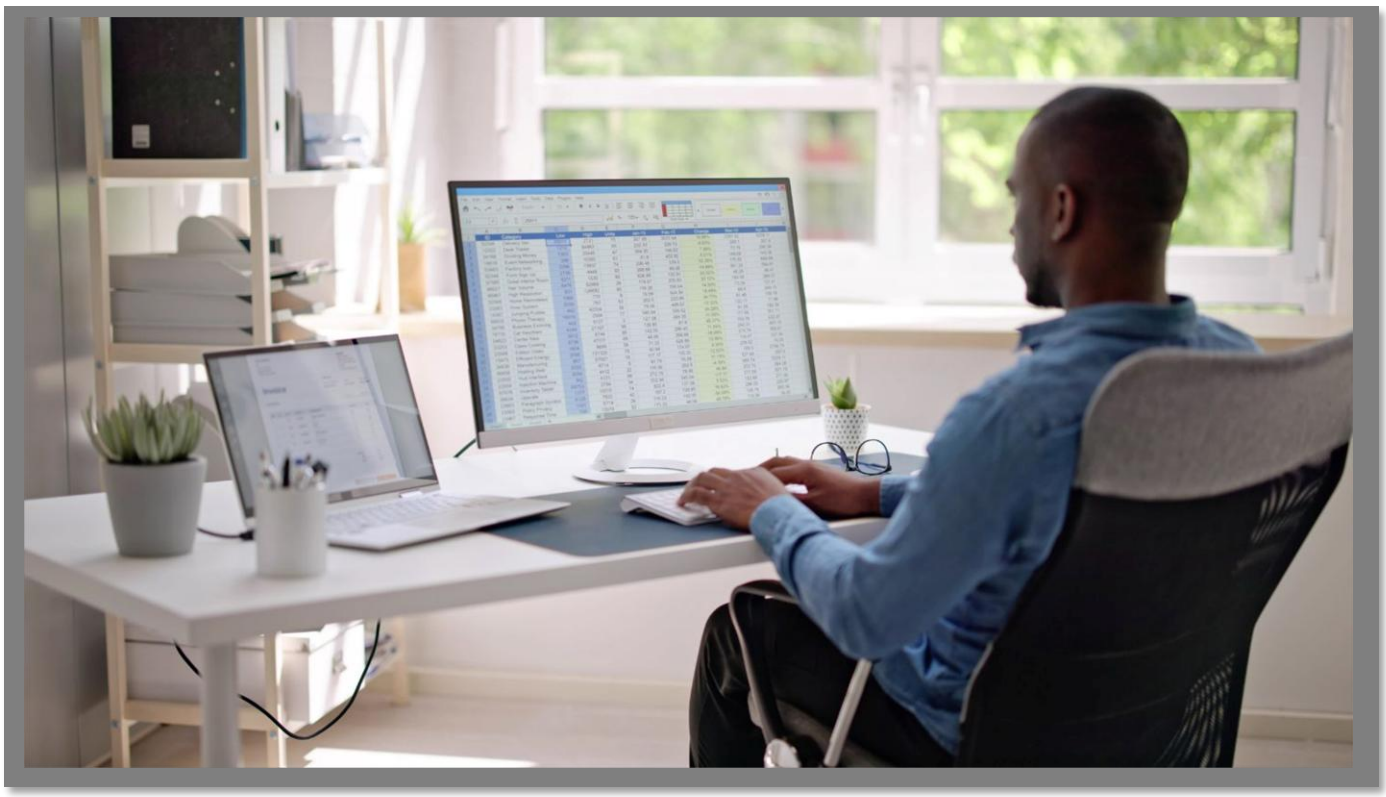
Arbutus Connectors

Active Directory
CONFIGURATION GUIDE



ARBUTUS
Powerful Analytics Simplified

Arbutus Connectors

Contents

Arbutus Connector – Active Directory

A. Introduction

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

Active Directory (AD) is a Microsoft service that provides centralized authentication and authorization to network resources – it authenticates and authorizes all users and computers in a Windows domain-type network. It is used in business environments to simplify user management, control access to data and enforce company security policies.

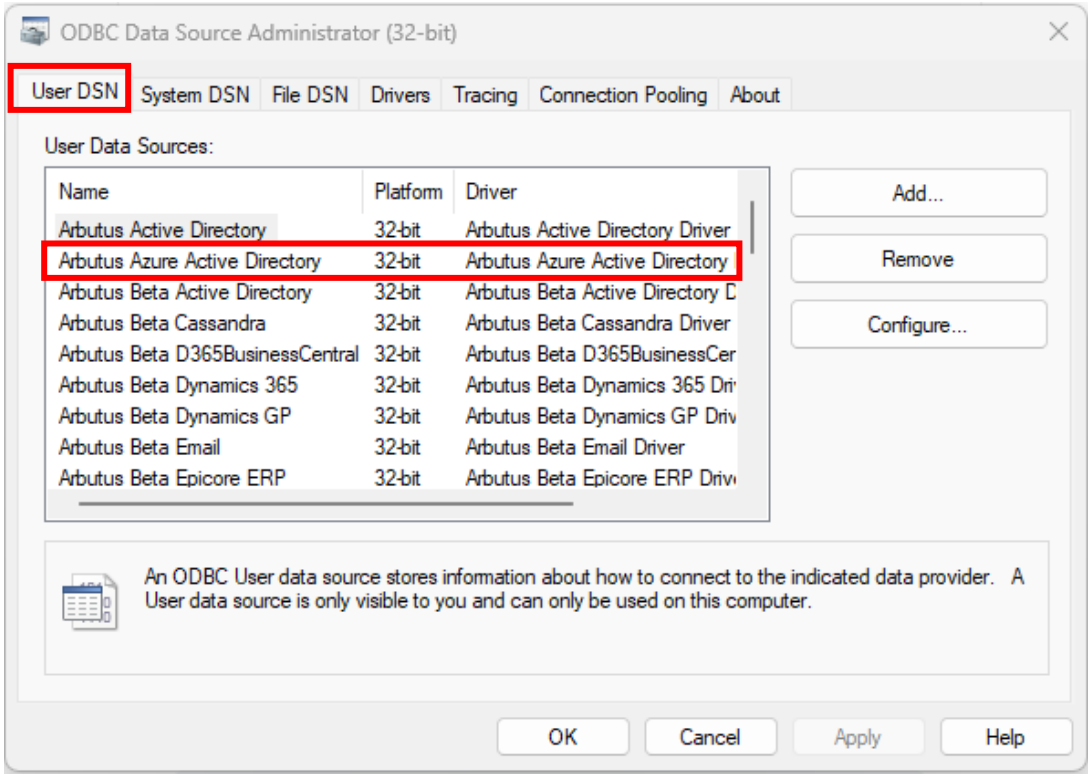
In Active Directory (AD), data is stored in a hierarchical structure within a database. Directory objects that are stored include, Users and Groups, Computers and Devices, Security Policies and Access Controls, and Group Policy Objects. The main AD database file is NTDS.DIT and contains all directory objects and attributes.

C. Determining if the Connector exists prior to configuring

Installation of the Arbutus Active Directory 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 Active Directory 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.

Arbutus Connectors

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.

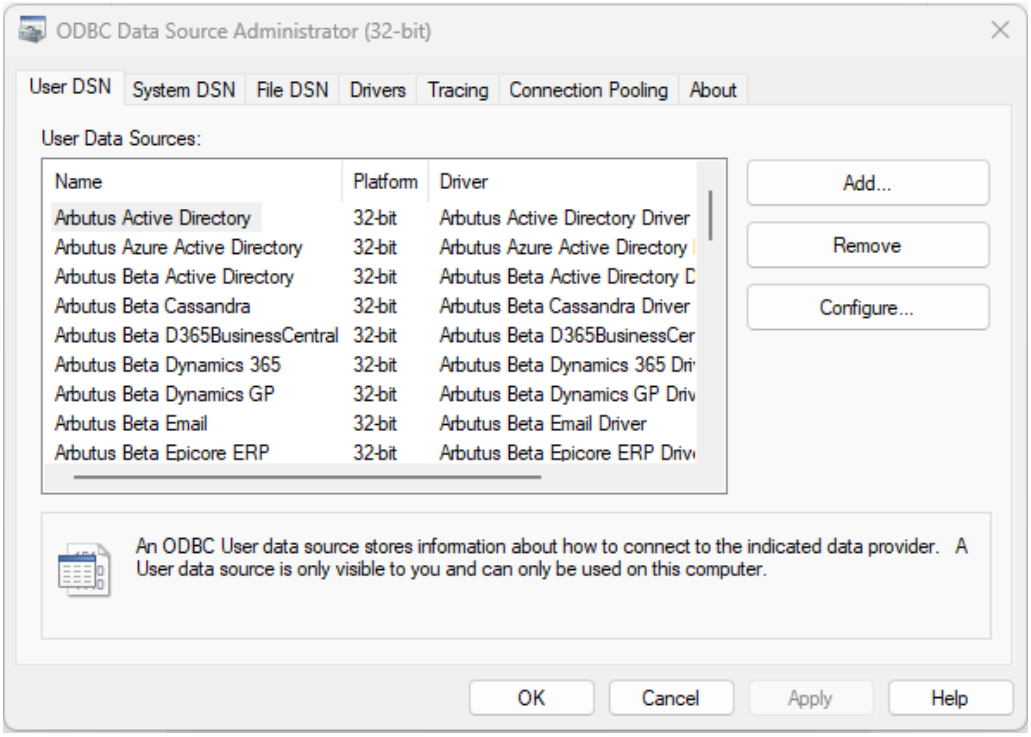
Each of these DSNs has a tab in the **ODBC Data Source Administrator** dialog.

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



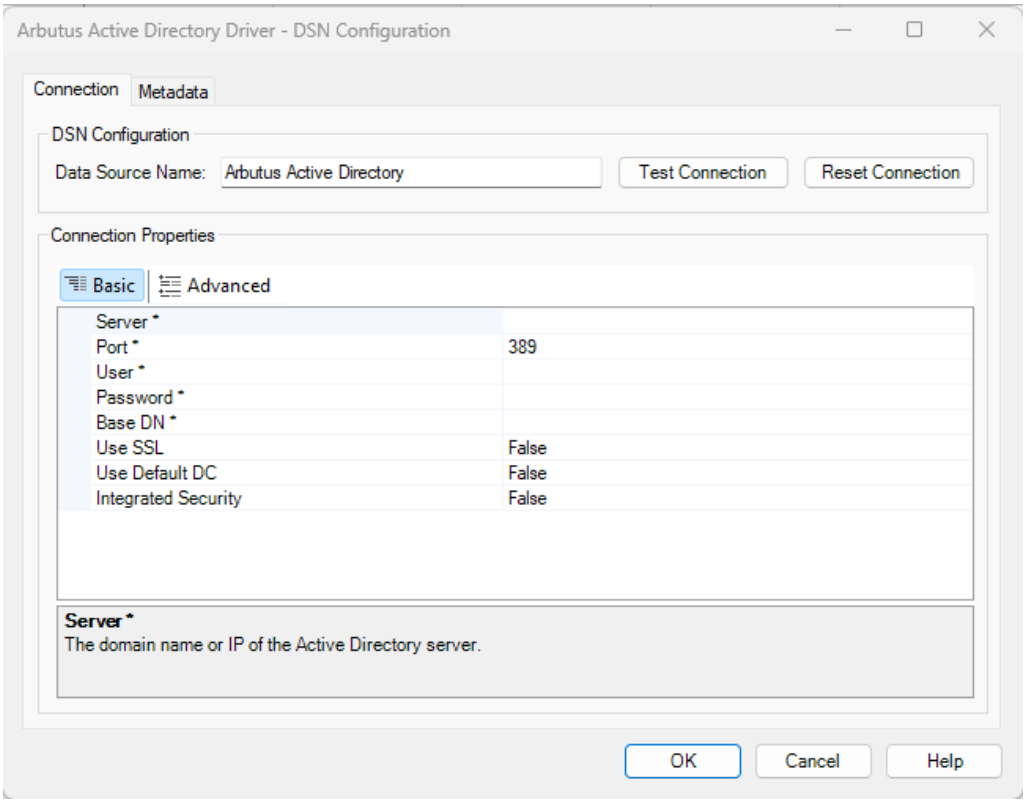
2. Click the **User DSN** tab.

   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 Active Directory.**

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

This opens the **Arbutus Active Directory Driver – DSN Configuration** dialog.



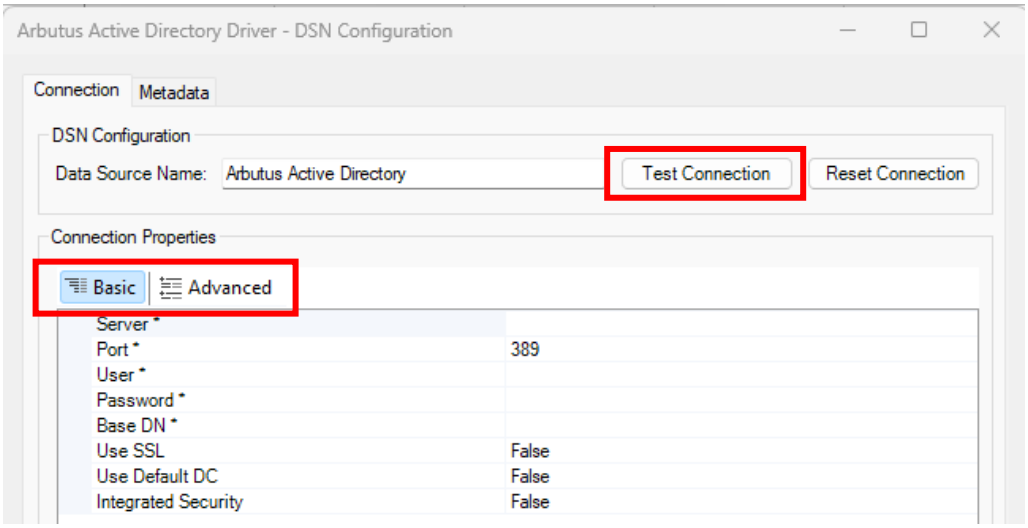
E. Editing the DSN properties – the Basic and Advanced tabs

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 **389** entry for the **Port** (per screenshot below) to match the number by which the target system is defined.

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 Active Directory by clicking the **Test Connection** button, as highlighted in the screenshot below.



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

1. **Server** – enter the domain name or IP of the Active Directory Server. This does not need to include the LDAP:\\ portion, only the server domain name or IP.

2. **Port** – enter the port the Active Directory Server is running on. The port the Active Directory server is running on. Together with **Server** (see above), this property is used to specify the Active Directory server.

   The default value is **389**.

3. **User** – enter the distinguished name of a user. Together with **Password** (see below), this field is used to authenticate against the Active Directory server.

4. **Password** – enter the password for the distinguished name of the specified user. Together with User (see above), this field is also used to authenticate against the Active Directory server

5. **Base DN** – enter the base portion of the distinguished name, used for limiting results to specific subtrees.

   You can specify a base DN to significantly improve performance when returning entries for large servers by limiting the number of entries that need to be examined.

6. **Use SSL** – specify through the dropdown selection (True / False) whether or not to use SSL to connect to the server. Note that a port of 636 will always use SSL.

   The default value is **False**.

7. **Use Default DC** - specify through the dropdown selection (True / False). Used to connect to the default Domain Controller and authenticate using the current user credentials.

   When True, the driver queries the system for the default Domain Controller and attempts to establish a connection with that server. The Server property does not need to be set separately in this case. Note: This functionality is only available in Windows.

   The default value is **False**.

8. **Integrated Security** - specify through the dropdown selection (True / False) whether or not to use the user's current context when logging in.

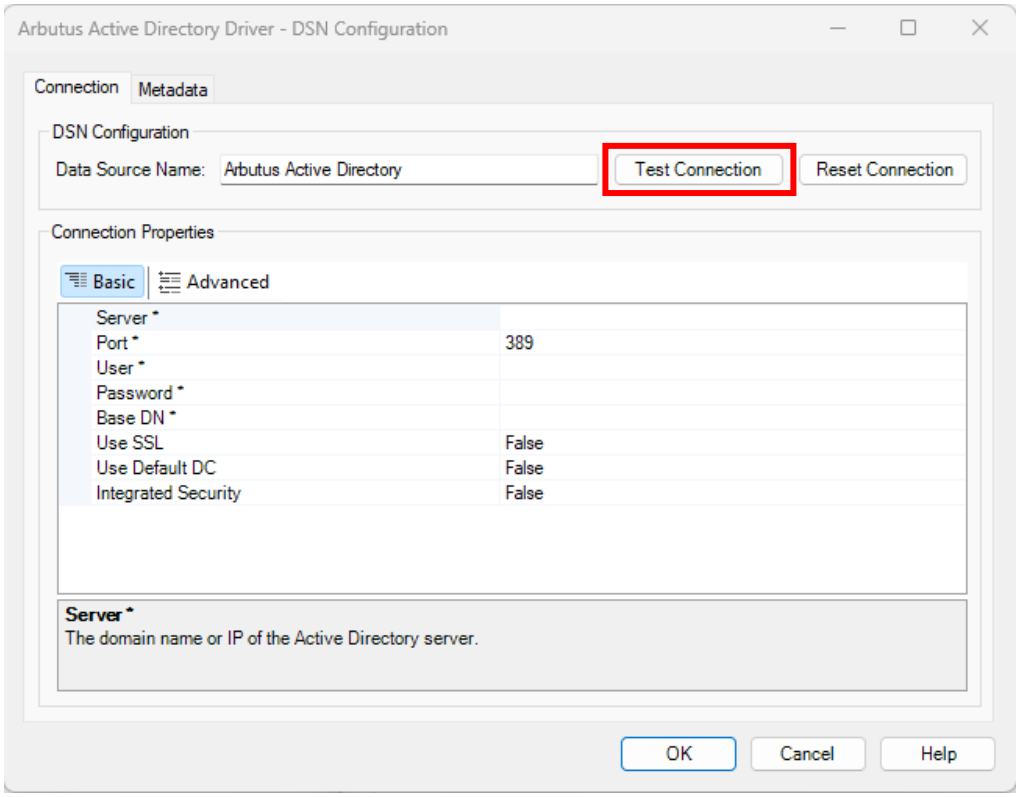
By default, the driver will use the provided **User** and **Password** when authenticating. If this option is enabled, then the driver will ignore the current User and Password and log in using the current user's context instead. This is only available when running on Windows.

The default value is **False**.

E2. Editing the DSN properties in the Advanced tab

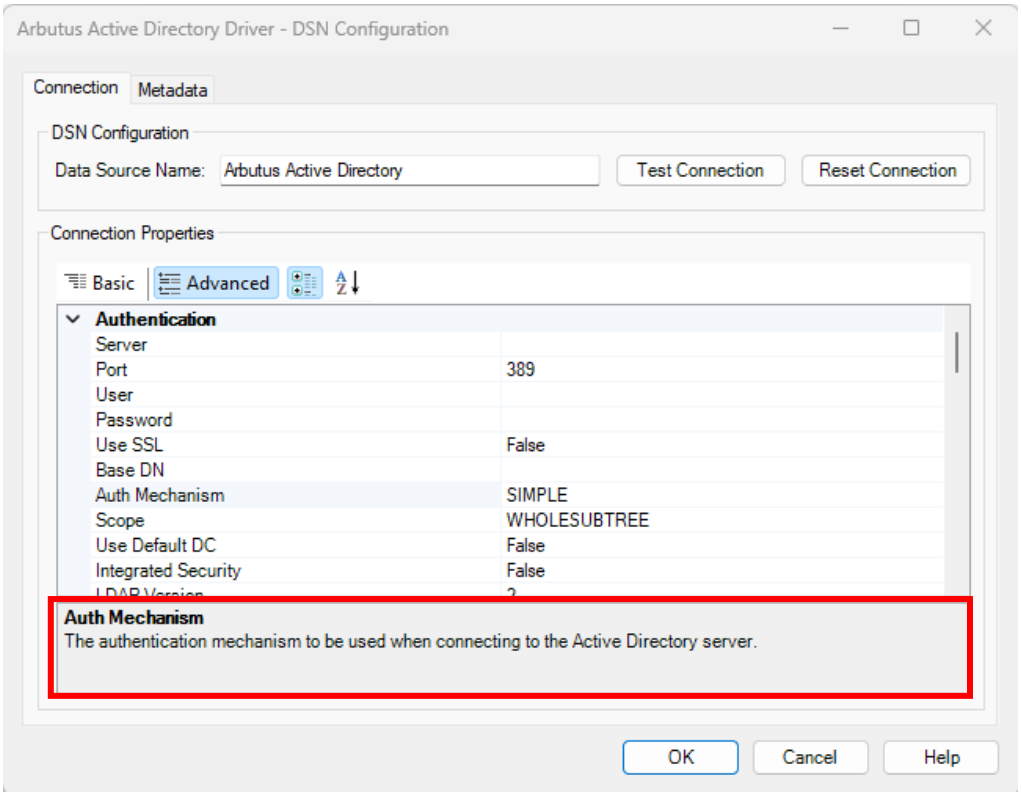
This tab includes more detailed and technical properties. It is intended for those users who need more control over the configuration and are comfortable with more complex options. The **Advanced** tab often includes properties that can fine-tune the behaviour of the system feature.

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 Active Directory 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, 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.