Copyright © 2021 Magnitude Software, Inc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from Magnitude.

The information in this document is subject to change without notice. Magnitude strives to keep this information accurate but does not warrant that this document is error-free.

Any Magnitude product described herein is licensed exclusively subject to the conditions set forth in your Magnitude license agreement.

Simba, the Simba logo, SimbaEngine, and Simba Technologies are registered trademarks of Simba Technologies Inc. in Canada, the United States and/or other countries. All other trademarks and/or servicemarks are the property of their respective owners.

All other company and product names mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective owners.

Information about the third-party products is contained in a third-party-licenses.txt file that is packaged with the software.

Contact Us

Magnitude Software, Inc.

www.magnitude.com
About This Guide

Purpose
The *Magnitude Simba SQL Server ODBC Data Connector Installation and Configuration Guide* explains how to install and configure the Magnitude Simba SQL Server ODBC Data Connector. The guide also provides details related to features of the connector.

Audience
The guide is intended for end users of the Simba SQL Server ODBC Connector, as well as administrators and developers integrating the connector.

Knowledge Prerequisites
To use the Simba SQL Server ODBC Connector, the following knowledge is helpful:

- Familiarity with the platform on which you are using the Simba SQL Server ODBC Connector
- Ability to use the data source to which the Simba SQL Server ODBC Connector is connecting
- An understanding of the role of ODBC technologies and driver managers in connecting to a data source
- Experience creating and configuring ODBC connections
- Exposure to SQL

Document Conventions
*Italics* are used when referring to book and document titles.

*Bold* is used in procedures for graphical user interface elements that a user clicks and text that a user types.

*Monospace font* indicates commands, source code, or contents of text files.

*Note:*
A text box with a pencil icon indicates a short note appended to a paragraph.
Important:
A text box with an exclamation mark indicates an important comment related to the preceding paragraph.
# Table of Contents

About the Simba SQL Server ODBC Connector .......................................................... 7

Windows Connector .................................................................................................... 8
  Windows System Requirements ................................................................................. 8
  Installing the Connector on Windows ..................................................................... 8
  Verifying the Connector Version Number on Windows ........................................... 9
  Creating a Data Source Name on Windows ............................................................. 9
  Configuring Authentication on Windows ............................................................... 12
  Configuring Connector-wide Logging Options on Windows ................................. 13

macOS Connector ..................................................................................................... 19
  macOS System Requirements ............................................................................... 19
  Installing the Connector on macOS ................................................................... 19
  Verifying the Connector Version Number on macOS ......................................... 20

Linux Connector ....................................................................................................... 21
  Linux System Requirements .................................................................................. 21
  Installing the Connector Using the Tarball Package .......................................... 21
  Verifying the Connector Version Number on Linux ........................................... 22

Configuring the ODBC Driver Manager on Non-Windows Machines ..................... 23
  Specifying ODBC Driver Managers on Non-Windows Machines ....................... 23
  Specifying the Locations of the Connector Configuration Files ........................... 24

Configuring ODBC Connections on a Non-Windows Machine ............................... 26
  Creating a Data Source Name on a Non-Windows Machine .............................. 26
  Configuring a DSN-less Connection on a Non-Windows Machine ................... 29
  Configuring Authentication on a Non-Windows Machine .................................... 31
  Configuring TLS Verification on a Non-Windows Machine ............................... 32
  Configuring Logging Options on a Non-Windows Machine ............................... 33
  Testing the Connection on a Non-Windows Machine ......................................... 36

Using a Connection String ....................................................................................... 39
  DSN Connection String Example ....................................................................... 39
  DSN-less Connection String Examples ............................................................... 39

Features .................................................................................................................... 42
  Data Types .......................................................................................................... 42
  Security and Authentication ................................................................................ 44

www.magnitude.com
Connector Configuration Options ................................................................. 45
  Configuration Options Appearing in the User Interface ................................ 45
  Configuration Options Having Only Key Names ........................................... 55

Third-Party Trademarks .................................................................................. 60
About the Simba SQL Server ODBC Connector

The Simba SQL Server ODBC Connector enables Business Intelligence (BI), analytics, and reporting on data that is stored in Microsoft SQL Server databases. The connector complies with the ODBC 3.80 data standard and adds important functionality such as Unicode, as well as 32- and 64-bit support for high-performance computing environments on all platforms.

ODBC is one of the most established and widely supported APIs for connecting to and working with databases. At the heart of the technology is the ODBC connector, which connects an application to the database. For more information about ODBC, see Data Access Standards on the Simba Technologies website: https://www.simba.com/resources/data-access-standards-glossary. For complete information about the ODBC specification, see the ODBC API Reference from the Microsoft documentation: https://docs.microsoft.com/en-us/sql/odbc/reference/syntax/odbc-api-reference.

The Simba SQL Server ODBC Connector is available for Microsoft® Windows®, Linux, and macOS platforms.

The Installation and Configuration Guide is suitable for users who are looking to access SQL Server data from their desktop environment. Application developers might also find the information helpful. Refer to your application for details on connecting via ODBC.

Note:

For information about how to use the connector in various BI tools, see the Simba ODBC Connectors Quick Start Guide for Windows: http://cdn.simba.com/docs/ODBC_QuickstartGuide/content/quick_start/intro.htm.
Windows System Requirements

The Simba SQL Server ODBC Connector supports SQL Server versions 2012 to 2019.

Install the connector on client machines where the application is installed. Before installing the connector, make sure that you have the following:

- Administrator rights on your machine.
- A machine that meets the following system requirements:
  - One of the following operating systems:
    - Windows 10 or 8.1
    - Windows Server 2019, 2016, or 2012
  - 100 MB of available disk space

Before the connector can be used, the Visual C++ Redistributable for Visual Studio 2013 with the same bitness as the connector must also be installed. If you obtained the connector from the Simba website, then your installation of the connector automatically includes this dependency. Otherwise, you must install the redistributable manually.


Installing the Connector on Windows

If you did not obtain this connector from the Simba website, you might need to follow a different installation procedure. For more information, see the Simba OEM ODBC Connectors Installation Guide.

On 64-bit Windows operating systems, you can execute both 32- and 64-bit applications. However, 64-bit applications must use 64-bit connectors, and 32-bit applications must use 32-bit connectors. Make sure that you use a connector whose bitness matches the bitness of the client application:

- SimbaSQLServerODBC32.msi for 32-bit applications
- SimbaSQLServerODBC64.msi for 64-bit applications

You can install both versions of the connector on the same machine.
To install the Simba SQL Server ODBC Connector on Windows:

1. Depending on the bitness of your client application, double-click to run `SimbaSQLServerODBC32.msi` or `SimbaSQLServerODBC64.msi`.
2. Click Next.
3. Select the check box to accept the terms of the License Agreement if you agree, and then click Next.
4. To change the installation location, click Change, then browse to the desired folder, and then click OK. To accept the installation location, click Next.
5. Click Install.
6. When the installation completes, click Finish.
7. If you received a license file through email, then copy the license file into the `\lib` subfolder of the installation folder you selected above. You must have Administrator privileges when changing the contents of this folder.

Verifying the Connector Version Number on Windows

If you need to verify the version of the Simba SQL Server ODBC Connector that is installed on your Windows machine, you can find the version number in the ODBC Data Source Administrator.

To verify the connector version number on Windows:

1. From the Start menu, go to ODBC Data Sources.

   ![Note:](Note.png)

   Make sure to select the ODBC Data Source Administrator that has the same bitness as the client application that you are using to connect to SQL Server.

2. Click the Drivers tab and then find the Simba SQL Server ODBC Connector in the list of ODBC connectors that are installed on your system. The version number is displayed in the Version column.

Creating a Data Source Name on Windows

Typically, after installing the Simba SQL Server ODBC Connector, you need to create a Data Source Name (DSN).

Alternatively, for information about DSN-less connections, see Using a Connection String on page 39.
To create a Data Source Name on Windows:

1. From the Start menu, go to ODBC Data Sources.

**Note:**

Make sure to select the ODBC Data Source Administrator that has the same bitness as the client application that you are using to connect to SQL Server.

2. In the ODBC Data Source Administrator, click the Drivers tab, and then scroll down as needed to confirm that the Simba SQL Server ODBC Connector appears in the alphabetical list of ODBC connectors that are installed on your system.

3. Choose one:
   - To create a DSN that only the user currently logged into Windows can use, click the User DSN tab.
   - Or, to create a DSN that all users who log into Windows can use, click the System DSN tab.

**Note:**

It is recommended that you create a System DSN instead of a User DSN. Some applications load the data using a different user account, and might not be able to detect User DSNs that are created under another user account.

4. Click Add.

5. In the Create New Data Source dialog box, select Simba SQL Server ODBC Connector and then click Finish. The Simba SQL Server ODBC Connector DSN Setup dialog box opens.

6. In the Data Source Name field, type a name for your DSN.

7. Optionally, in the Description field, type relevant details about the DSN.

8. In the Server field, type the name or IP address of the host where your SQL Server instance is running.

**Note:**

You can specify the name of the SQL Server instance by using the syntax `[ServerInfo]\[Instance]`, where `[ServerInfo]` is the IP address or host name of the server and `[Instance]` is the name of the instance. Make sure that the Port field is left empty in this scenario.

9. In the Port field, type the number of the TCP port that the server uses to listen for client connections.
10. In the **Database** field, type the name of the database that you want to access.

11. Optionally, in the **Application Name** field, type the name of the application that calls SQLDriverConnect.

12. To use TLS to encrypt all communication with the SQL Server instance before sending it over the network, select the **Encrypt** check box and then do one of the following:
   - To enable one-way authentication so that the connector verifies the server certificate using a CA certificate, in the **CA Certificate** field, type the full path and file name of the CA certificate that you want to use.
   - Or, to trust the server certificate instead of verifying it, select the **Trust Server Certificate** check box.

13. To specify the minimum version of TLS that the connector must use to connect to the server, from the **Minimum TLS/SSL** drop-down list, select the required TLS version.

14. To configure the connector to enable read-only mode, from the **Application Intent** drop-down list, select the **ReadOnly** option. For more information, see [Application Intent on page 46](#).

15. Configure authentication by specifying the authentication mechanism. For more information, see [Configuring Authentication on Windows](#) on page 12.

16. To return certain SQL Server-specific data types as ODBC data types instead of SQL Server data types, select the **Return SQL Server-Specific Types as ODBC Types** check box. For a complete list of the data types that this setting applies to, see [Return SQL Server-Specific Types as ODBC Types on page 52](#).

17. To include temporary tables in the results when calling SQLTables, select the **Enable Table Types** check box.

18. To configure logging behavior for the connector, click **Logging Options**. For more information, see [Configuring Connector-wide Logging Options on Windows](#) on page 13.

19. To test the connection, click **Test**. Review the results as needed, and then click **OK**.

**Note:**

If the connection fails, then confirm that the settings in the Simba SQL Server ODBC Driver DSN Setup dialog box are correct. Contact your SQL Server administrator as needed.
20. To save your settings and close the Simba SQL Server ODBC Driver DSN Setup dialog box, click OK.

21. To close the ODBC Data Source Administrator, click OK.

**Configuring Authentication on Windows**

Connections to SQL Server require authentication. You can authenticate the connection using your SQL Server user account, the Kerberos protocol, or the NTLM protocol.

**Using a User Account**

You can authenticate the connection by providing your user name and password for accessing the SQL Server instance.

**To configure authentication using a user account:**

1. To access authentication options, open the ODBC Data Source Administrator where you created the DSN, then select the DSN, and then click **Configure**.
2. In the **User** and **Password** fields, type your credentials for accessing the server.

**Using Kerberos**

You can authenticate the connection by using the Kerberos protocol.

**To configure authentication using Kerberos:**

1. To access authentication options, open the ODBC Data Source Administrator where you created the DSN, then select the DSN, and then click **Configure**.
2. Select the **Use Trusted Connection** check box.
3. Optionally, in the **Server SPN** field, type the service principal name of your SQL Server instance.

**Note:**

If you leave the field empty, then the connector uses **MSSQLSvc/[HostName]:[Port]** as the service principal name, where `[HostName]` is the IP address or host name of the server and `[Port]` is the number of the port that you are connecting to.

**Using NTLM**

You can authenticate the connection by using the NTLM protocol.
To configure authentication using NTLM:

1. To access authentication options, open the ODBC Data Source Administrator where you created the DSN, then select the DSN, and then click Configure.
2. Select the Use NTLM check box.

Important:
Make sure that you clear the Use Trusted Connection check box. If Use Trusted Connection is selected, then the Use NTLM option is not available and the connector uses Kerberos authentication instead.

3. In the User and Password fields, type your credentials for accessing the server.

Configuring Connector-wide Logging Options on Windows

To help troubleshoot issues, you can enable logging in the connector or in the wire protocol component. In addition to these forms of logging supported by the Simba SQL Server ODBC Connector, the ODBC Data Source Administrator provides tracing functionality.

Important:
Only enable logging or tracing long enough to capture an issue. Logging or tracing decreases performance and can consume a large quantity of disk space.

The settings for logging apply to every connection that uses the Simba SQL Server ODBC Connector, so make sure to disable the feature after you are done using it. To configure logging for the current connection, see Configuring Logging for the Current Connection on page 17.

Connector Logging

Use connector logging to track the activity in the Simba SQL Server ODBC Connector. You can specify the amount of detail included in the log files. The table below lists the logging levels that are available, in order from least verbose to most verbose.

<table>
<thead>
<tr>
<th>Logging Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF</td>
<td>Disables all logging.</td>
</tr>
<tr>
<td>FATAL</td>
<td>Logs severe error events that lead the connector to abort.</td>
</tr>
<tr>
<td>Logging Level</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ERROR</td>
<td>Logs error events that might allow the connector to continue running.</td>
</tr>
<tr>
<td>WARNING</td>
<td>Logs events that might result in an error if action is not taken.</td>
</tr>
<tr>
<td>INFO</td>
<td>Logs general information that describes the progress of the connector.</td>
</tr>
<tr>
<td>DEBUG</td>
<td>Logs detailed information that is useful for debugging the connector.</td>
</tr>
<tr>
<td>TRACE</td>
<td>Logs all connector activity.</td>
</tr>
</tbody>
</table>

**To enable connector logging on Windows:**

1. To access logging options, open the ODBC Data Source Administrator where you created the DSN, then select the DSN, then click **Configure**, and then click **Logging Options**.
2. In the **Log Level** drop-down list, select the desired level of information to include in log files.
3. In the **Log Path** field, type the full path to the folder where you want to save log files.
4. In the **Max Number Files** field, type the maximum number of log files to keep.
   
   **Note:**
   After the maximum number of log files is reached, each time an additional file is created, the connector deletes the oldest log file.

5. In the **Max File Size** field, type the maximum size of each log file in megabytes (MB).
   
   **Note:**
   After the maximum file size is reached, the connector creates a new file and continues logging.

6. Click **OK**.
7. Restart your ODBC application to make sure that the new settings take effect.

The Simba SQL Server ODBC Connector produces the following log files at the location you specify using the **LogPath** key:
- A `simba\sqlserverodbcdriver.log` file that logs connector activity that is not specific to a connection.
- A `simba\sqlserverodbcdriver_connection_[Number].log` file for each connection made to the database, where `[Number]` is a number that identifies each log file. This file logs connector activity that is specific to the connection.

If you enable the `UseLogPrefix` connection property, the connector prefixes the log file name with the user name associated with the connection and the process ID of the application through which the connection is made. For more information, see `UseLogPrefix` on page 59.

**To disable connector logging on Windows:**

1. To access logging options, open the ODBC Data Source Administrator where you created the DSN, then select the DSN, then click **Configure**, and then click **Logging Options**.
2. In the **Log Level** drop-down list, select **LOG_OFF**.
3. Click **OK**.

**Wire Protocol Component Logging**

Use wire protocol component logging to track the data activity between the connector and the SQL Server instance. You can specify the amount of detail to include in the log files. The table below lists the logging levels that are available, in order from least verbose to most verbose.

<table>
<thead>
<tr>
<th>Logging Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disables all logging.</td>
</tr>
<tr>
<td>1</td>
<td>Logs error events that might allow the wire protocol component to continue running. 1 is the default logging level.</td>
</tr>
<tr>
<td>2</td>
<td>Logs general information that describes the progress of the wire protocol component.</td>
</tr>
<tr>
<td>3</td>
<td>Logs detailed information that is useful for debugging the wire protocol component.</td>
</tr>
<tr>
<td>4</td>
<td>Logs all activity in the wire protocol component.</td>
</tr>
</tbody>
</table>

Wire protocol component logging is configured through the `TDSTRACE` environment variable.

www.magnitude.com
To enable wire protocol component logging on Windows:

1. Open the System Information dialog box:
   - If you are using Windows 7 or earlier, click Start , then right-click Computer, and then click Properties.
   - Or, if you are using Windows 8 or later, on the Start screen, right-click This PC and then click Properties.
2. Click Advanced System Settings.
3. In the System Properties dialog box, click the Advanced tab and then click Environment Variables.
4. Choose one:
   - If the TDSTRACE variable already exists in the System Variables list, select it and then click Edit.
   - Or, if the TDSTRACE variable does not appear in the System Variables list, click New and then in the Variable Name field type TDSTRACE.
5. In the Variable Value field, type \[LoggingLevel]:[LogFilePath], where \[LoggingLevel] is the logging level indicating the amount of detail to include in the log file and \[LogFilePath] is the full path of the log file.

   For example, the value 3:C:\Logs\MyWireLog.log configures the wire protocol component to log debugging information in a file named MyWireLog.log located in the C:\Logs folder.
6. To save your changes and close the Edit System Variable dialog box, click OK.
7. Click OK to close the Environment Variables dialog box, and then click OK to close the System Properties dialog box.

To disable wire protocol component logging on Windows:

1. Open the System Information dialog box:
   - If you are using Windows 7 or earlier, click Start , then right-click Computer, and then click Properties.
   - Or, if you are using Windows 8 or later, on the Start screen, right-click This PC and then click Properties.
2. Click Advanced System Settings.
3. In the System Properties dialog box, click the Advanced tab and then click Environment Variables.
4. Select TDSTRACE from the System Variables list and then click Edit.
5. In the Variable Value field, replace the existing value with 0.
6. To save your changes and close the Edit System Variable dialog box, click OK.
7. Click OK to close the Environment Variables dialog box, and then click OK to close the System Properties dialog box.
ODBC Tracing

You can use the ODBC Data Source Administrator to trace connection activity in the ODBC layer.

To start tracing using the ODBC Data Source Administrator:

1. In the ODBC Data Source Administrator, click the Tracing tab.
2. In the Log File Path area, click Browse. In the Select ODBC Log File dialog box, browse to the location where you want to save the log file, then type a descriptive file name in the File name field, and then click Save.
3. On the Tracing tab, click Start Tracing Now.

To stop ODBC Data Source Administrator tracing:

- In the ODBC Data Source Administrator, on the Tracing tab, click Stop Tracing Now.

For more information about tracing using the ODBC Data Source Administrator, see "How to Generate an ODBC Trace with ODBC Data Source Administrator" on the Microsoft Support website: http://support.microsoft.com/kb/274551.

Configuring Logging for the Current Connection

You can configure logging for the current connection by setting the logging configuration properties in the DSN or in a connection string. For information about the logging configuration properties, see Configuring Connector-wide Logging Options on Windows on page 13. Settings in the connection string take precedence over settings in the DSN, and settings in the DSN take precedence over connector-wide settings.

Note:

If the LogLevel configuration property is passed in via the connection string or DSN, the rest of the logging configurations are read from the connection string or DSN and not from the existing connector-wide logging configuration.

To configure logging properties in the DSN, you must modify the Windows registry. For information about the Windows registry, see the Microsoft Windows documentation.

Important:

Editing the Windows Registry incorrectly can potentially cause serious, system-wide problems that may require re-installing Windows to correct.

To add logging configurations to a DSN on Windows:
1. On the Start screen, type `regedit`, and then click the `regedit` search result.

2. Navigate to the appropriate registry key for the bitness of your connector and your machine:
   - 32-bit System DSNs: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ODBC\ODBC.INI\[DSN Name]`
   - 64-bit System DSNs: `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\[DSN Name]`
   - 32-bit and 64-bit User DSNs: `HKEY_CURRENT_USER\SOFTWARE\ODBC\ODBC.INI\[DSN Name]`

3. Navigate to the appropriate registry key for the bitness of your connector and your machine:

4. For each configuration option that you want to configure for the current connection, create a value by doing the following:
   a. If the key name value does not already exist, create it. Right-click the `[DSN Name]` and then select `New > String Value`, type the key name of the configuration option, and then press `Enter`.
   b. Right-click the key name and then click `Modify`.
      - To confirm the key names for each configuration option, see `Connector Configuration Options` on page 45.
   c. In the Edit String dialog box, in the `Value Data` field, type the value for the configuration option.

5. Close the Registry Editor.

6. Restart your ODBC application to make sure that the new settings take effect.
macOS Connector

macOS System Requirements

The Simba SQL Server ODBC Connector supports SQL Server versions 2012 to 2019.

Install the connector on client machines where the application is installed. Each client machine that you install the connector on must meet the following minimum system requirements:

- macOS version 10.13 or 10.14 or 10.15
- 150MB of available disk space
- One of the following ODBC driver managers installed:
  - iODBC 3.52.9 or later
  - unixODBC 2.2.14 or later

Installing the Connector on macOS

If you did not obtain this connector from the Simba website, you might need to follow a different installation procedure. For more information, see the Simba OEM ODBC Connectors Installation Guide.

The Simba SQL Server ODBC Connector is available for macOS as a .dmg file named SimbaSQLServerODBC.dmg. The connector supports both 32- and 64-bit client applications.

To install the Simba SQL Server ODBC Connector on macOS:

1. Double-click SimbaSQLServerODBC.dmg to mount the disk image.
2. Double-click SimbaSQLServerODBC.dmg to mount the disk image.
3. In the installer, click Continue.
4. On the Software License Agreement screen, click Continue, and when the prompt appears, click Agree if you agree to the terms of the License Agreement.
5. Optionally, to change the installation location, click Change Install Location, then select the desired location, and then click Continue.

Note:

By default, the connector files are installed in the
/Library/simba/sqlserverodbc directory.

6. To accept the installation location and begin the installation, click Install.
7. When the installation completes, click **Close**.

8. If you received a license file through email, then copy the license file into the 
   `/lib` subfolder in the connector installation directory. You must have root 
   privileges when changing the contents of this folder.

   For example, if you installed the connector to the default location, you would 
   copy the license file into the `/Library/simba/sqlserverodbc/lib` folder.

Next, configure the environment variables on your machine to make sure that the 
ODBC driver manager can work with the connector. For more information, see 
[Configuring the ODBC Driver Manager on Non-Windows Machines](#) on page 23.

### Verifying the Connector Version Number on macOS

If you need to verify the version of the Simba SQL Server ODBC Connector that is 
installed on your macOS machine, you can query the version number through the 
Terminal.

**To verify the connector version number on macOS:**

> At the Terminal, run the following command:

```
pkgutil --info com.simba.sqlserverodbc
```

The command returns information about the Simba SQL Server ODBC Connector that 
is installed on your machine, including the version number.
Linux Connector

**Linux System Requirements**

The Simba SQL Server ODBC Connector supports SQL Server versions 2012 to 2019.

Install the connector on client machines where the application is installed. Each client machine that you install the connector on must meet the following minimum system requirements:

- One of the following distributions:
  - Red Hat® Enterprise Linux® (RHEL) 7 or 8
  - CentOS 7 or 8
  - SUSE Linux Enterprise Server (SLES) 12 or 15
  - Debian 9
  - Ubuntu 16.04 or 18.04
- 150 MB of available disk space
- One of the following ODBC driver managers installed:
  - iODBC 3.52.9 or later
  - unixODBC 2.2.14 or later

To install the connector, you must have root access on the machine.

**Installing the Connector Using the Tarball Package**

If you did not obtain this connector from the Simba website, you might need to follow a different installation procedure. For more information, see the Simba OEM ODBC Connectors Installation Guide.

The Simba SQL Server ODBC Connector is available as a tarball package named, where [Version] is the version number of the connector and [Release] is the release number for this version of the connector. The package contains both the 32-bit and 64-bit versions of the connector.

On 64-bit editions of Linux, you can execute both 32- and 64-bit applications. However, 64-bit applications must use 64-bit connectors, and 32-bit applications must use 32-bit connectors. Make sure that you use a connector whose bitness matches the bitness of the client application. You can install both versions of the connector on the same machine.
To install the connector using the tarball package:

1. Log in as the root user, and then navigate to the folder containing the tarball package.
2. Run the following command to extract the package and install the connector:

```bash
    tar --directory=/opt -zxvf [TarballName]
```

Where `[TarballName]` is the name of the tarball package containing the connector.

The Simba SQL Server ODBC Connector files are installed in the `opt/simba/sqlserverodbc` directory.

3. If you received a license file through email, then copy the license file into the `opt/simba/sqlserverodbc/lib/32` or `opt/simba/sqlserverodbc/lib/64` folder, depending on the version of the connector that you installed.

Next, configure the environment variables on your machine to make sure that the ODBC driver manager can work with the connector. For more information, see Configuring the ODBC Driver Manager on Non-Windows Machines on page 23.

Verifying the Connector Version Number on Linux

If you need to verify the version of the Simba SQL Server ODBC Connector that is installed on your Linux machine, you can search the connector's binary file for version number information. Alternatively, you can search the connector's binary file for version number information.

To verify the connector version number on Linux using the binary file:

1. Navigate to the `/lib` subfolder in your connector installation directory. By default, the path to this directory is: `/opt/simba/sqlserverodbc`.
2. Open the connector's `.so` binary file in a text editor, and search for the text `$driver_version_sb$`. The connector's version number is listed after this text.
Configuring the ODBC Driver Manager on Non-Windows Machines

To make sure that the ODBC driver manager on your machine is configured to work with the Simba SQL Server ODBC Connector, do the following:

- Set the library path environment variable to make sure that your machine uses the correct ODBC driver manager. For more information, see Specifying ODBC Driver Managers on Non-Windows Machines on page 23.

- If the connector configuration files are not stored in the default locations expected by the ODBC driver manager, then set environment variables to make sure that the driver manager locates and uses those files. For more information, see Specifying the Locations of the Connector Configuration Files on page 24.

After configuring the ODBC driver manager, you can configure a connection and access your data store through the connector.

Specifying ODBC Driver Managers on Non-Windows Machines

You need to make sure that your machine uses the correct ODBC driver manager to load the connector. To do this, set the library path environment variable.

**macOS**

If you are using a macOS machine, then set the DYLD_LIBRARY_PATH environment variable to include the paths to the ODBC driver manager libraries. For example, if the libraries are installed in `/usr/local/lib`, then run the following command to set DYLD_LIBRARY_PATH for the current user session:

```
export DYLD_LIBRARY_PATH=$DYLD_LIBRARY_PATH:/usr/local/lib
```

For information about setting an environment variable permanently, refer to the macOS shell documentation.

**Linux**

If you are using a Linux machine, then set the LD_LIBRARY_PATH environment variable to include the paths to the ODBC driver manager libraries. For example, if the libraries are installed in `/usr/local/lib`, then run the following command to set LD_LIBRARY_PATH for the current user session:
For information about setting an environment variable permanently, refer to the Linux shell documentation.

### Specifying the Locations of the Connector Configuration Files

By default, ODBC driver managers are configured to use hidden versions of the odbc.ini and odbcinst.ini configuration files (named .odbc.ini and .odbcinst.ini) located in the home directory, as well as the simba.sqlserverodbc.ini file in the lib subfolder of the connector installation directory. If you store these configuration files elsewhere, then you must set the environment variables described below so that the driver manager can locate the files.

If you are using iODBC, do the following:

- Set ODBCINI to the full path and file name of the odbc.ini file.
- Set ODBCINSTINI to the full path and file name of the odbcinst.ini file.
- Set SIMBASQLSERVERINI to the full path and file name of the simba.sqlserverodbc.ini file.

If you are using unixODBC, do the following:

- Set ODBCINI to the full path and file name of the odbc.ini file.
- Set ODBCINSTINI to the full path of the directory that contains the odbcinst.ini file.
- Set SIMBASQLSERVERINI to the full path and file name of the simba.sqlserverodbc.ini file.

For example, if your odbc.ini and odbcinst.ini files are located in /usr/local/odbc and your simba.sqlserverodbc.ini file is located in /etc, then set the environment variables as follows:

For iODBC:

```bash
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCINSTINI=/usr/local/odbc/odbcinst.ini
export SIMBASQLSERVERINI=/etc/simba.sqlserverodbc.ini
```

For unixODBC:

```bash
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCINSTINI=/usr/local/odbc
```
To locate the `simba.sqlserverodbc.ini` file, the connector uses the following search order:

1. If the `SIMBASQLSERVERINI` environment variable is defined, then the connector searches for the file specified by the environment variable.
2. The connector searches the directory that contains the connector library files for a file named `simba.sqlserverodbc.ini`.
3. The connector searches the current working directory of the application for a file named `simba.sqlserverodbc.ini`.
4. The connector searches the home directory for a hidden file named `.simba.sqlserverodbc.ini` (prefixed with a period).
5. The connector searches the `/etc` directory for a file named `simba.sqlserverodbc.ini`.
Creating a Data Source Name on a Non-Windows Machine

When connecting to your data store using a DSN, you only need to configure the odbc.ini file. Set the properties in the odbc.ini file to create a DSN that specifies the connection information for your data store. For information about configuring a DSN-less connection instead, see Configuring a DSN-less Connection on a Non-Windows Machine on page 29.

If your machine is already configured to use an existing odbc.ini file, then update that file by adding the settings described below. Otherwise, copy the odbc.ini file from the Setup subfolder in the connector installation directory to the home directory, and then update the file as described below.

To create a Data Source Name on a non-Windows machine:

1. In a text editor, open the odbc.ini configuration file.

   Note:
   
   If you are using a hidden copy of the odbc.ini file, you can remove the period (.) from the start of the file name to make the file visible while you are editing it.

2. In the [ODBC Data Sources] section, add a new entry by typing a name for the DSN, an equal sign (=), and then the name of the connector.

   For example, on a macOS machine:
As another example, for a 32-bit connector on a Linux machine:

3. Create a section that has the same name as your DSN, and then specify configuration options as key-value pairs in the section:
   a. Set the **Driver** property to the full path of the connector library file that matches the bitness of the application.
      
      For example, on a macOS machine:
      
      ```
      Driver=/Library/
      simba/sqlserverodbc/lib/libsqlserverodbc_sbu.dylib
      ```
      
      As another example, for a 32-bit connector on a Linux machine:
      
      ```
      Driver=/opt/
      simba/sqlserverodbc/lib/32/libsqlserverodbc_sb32.so
      ```

   b. Set the **Server** property to the IP address or host name of the server, and then set the **Port** property to the number of the TCP port that the server uses to listen for client connections.
      
      For example:
      
      ```
      Server=192.168.222.160
      Port=1500
      ```

   c. Configure authentication by specifying the authentication mechanism and your credentials. For more information, see Configuring Authentication on a Non-Windows Machine on page 31

   d. Optionally, to specify the minimum version of TLS that the connector must use to connect to the server, set the **Min_TLS** property to the required version of TLS. The supported options include 1.0 for TLS 1.0, 1.1 for TLS 1.1, and 1.2 for TLS 1.2.

   e. Optionally, encrypt your connection with TLS and configure whether the connector verifies the identity of the server. For more information, see Configuring TLS Verification on a Non-Windows Machine on page 32.

   f. Optionally, set additional key-value pairs as needed to specify other optional connection settings. For detailed information about all the
configuration options supported by the Simba SQL Server ODBC Connector, see Connector Configuration Options on page 45.

4. Save the odbc.ini configuration file.

Note:
If you are storing this file in its default location in the home directory, then prefix the file name with a period (.) so that the file becomes hidden. If you are storing this file in another location, then save it as a non-hidden file (without the prefix), and make sure that the ODBCINI environment variable specifies the location. For more information, see Specifying the Locations of the Connector Configuration Files on page 24.

For example, the following is an odbc.ini configuration file for macOS containing a DSN that connects to SQL Server using a user account:

```
[ODBC Data Sources]
Sample DSN=Simba SQL Server ODBC Connector
[Sample DSN]
Driver=/Library/simba/sqlserverodbc/lib/libsqlserverodbc_sbu.dylib
Server=192.168.222.160
Port=1500
Trusted_Connection=no
UID=simba
PWD=simba123
```

As another example, the following is an odbc.ini configuration file for a 32-bit connector on a Linux machine, containing a DSN that connects to SQL Server using a user account:

```
[ODBC Data Sources]
Sample DSN=Simba SQL Server ODBC Connector 32-bit
[Sample DSN]
Driver=/opt/simba/sqlserverodbc/lib/32/libsqlserverodbc_sb32.so
Server=192.168.222.160
Port=1500
Trusted_Connection=no
UID=simba
PWD=simba123
```

You can now use the DSN in an application to connect to the data store.
Configuring a DSN-less Connection on a Non-Windows Machine

To connect to your data store through a DSN-less connection, you need to define the connector in the `odbcinst.ini` file and then provide a DSN-less connection string in your application.

If your machine is already configured to use an existing `odbcinst.ini` file, then update that file by adding the settings described below. Otherwise, copy the `odbcinst.ini` file from the Setup subfolder in the connector installation directory to the home directory, and then update the file as described below.

To define a connector on a non-Windows machine:

1. In a text editor, open the `odbcinst.ini` configuration file.

   ✍️ Note:
   
   If you are using a hidden copy of the `odbcinst.ini` file, you can remove the period (.) from the start of the file name to make the file visible while you are editing it.

2. In the `[ODBC Drivers]` section, add a new entry by typing a name for the connector, an equal sign (=), and then `Installed`.

   For example:

   ```
   [ODBC Drivers]
   Simba SQL Server ODBC Connector=Installed
   ```

3. Create a section that has the same name as the connector (as specified in the previous step), and then specify the following configuration options as key-value pairs in the section:

   a. Set the `Driver` property to the full path of the connector library file that matches the bitness of the application.

   For example, on a macOS machine:

   ```
   Driver=/Library/
   simba/sqlserverodbc/lib/libsqlserverodbc_sbu.dylib
   ```

   As another example, for a 32-bit connector on a Linux machine:

   ```
   Driver=/opt/
   simba/sqlserverodbc/lib/32/libsqlserverodbc_sb32.so
   ```
b. Optionally, set the **Description** property to a description of the connector.

For example:

```
Description=Simba SQL Server ODBC Connector
```

4. Save the **odbcinst.ini** configuration file.

**Note:**

If you are storing this file in its default location in the home directory, then prefix the file name with a period (.) so that the file becomes hidden. If you are storing this file in another location, then save it as a non-hidden file (without the prefix), and make sure that the ODBCINSTINI or ODBCSYSINI environment variable specifies the location. For more information, see [Specifying the Locations of the Connector Configuration Files](#) on page 24.

For example, the following is an **odbcinst.ini** configuration file for macOS:

```
[ODBC Drivers]
Simba SQL Server ODBC Connector=Installed
[Simba SQL Server ODBC Connector]
Description=Simba SQL Server ODBC Connector
Driver=/Library/simba/sqlserverodbc/lib/libsqlserverodbc_sbu.dylib
```

As another example, the following is an **odbcinst.ini** configuration file for both the 32- and 64-bit connectors on Linux:

```
[ODBC Drivers]
Simba SQL Server ODBC Connector 32-bit=Installed
Simba SQL Server ODBC Connector 64-bit=Installed
[Simba SQL Server ODBC Connector 32-bit]
Description=Simba SQL Server ODBC Connector (32-bit)
Driver=/opt/simba/sqlserverodbc/lib/32/libsqlserverodbc_sbsb32.so
[Simba SQL Server ODBC Connector 64-bit]
Description=Simba SQL Server ODBC Connector (64-bit)
Driver=/opt/simba/sqlserverodbc/lib/64/libsqlserverodbc_sbsb64.so
```

You can now connect to your data store by providing your application with a connection string where the `Driver` property is set to the connector name specified in the **odbcinst.ini** file, and all the other necessary connection properties are also...
set. For more information, see "DSN-less Connection String Examples" in Using a Connection String on page 39.

For instructions about configuring specific connection features, see the following:

- Configuring Authentication on a Non-Windows Machine on page 31
- Configuring TLS Verification on a Non-Windows Machine on page 32

For detailed information about all the connection properties that the connector supports, see Connector Configuration Options on page 45.

## Configuring Authentication on a Non-Windows Machine

Connections to SQL Server require authentication. You can authenticate the connection using your SQL Server user account, the Kerberos protocol, or the NTLM protocol.

You can set the connection properties described below in a connection string or in a DSN (in the odbc.ini file). Settings in the connection string take precedence over settings in the DSN.

### Note:

For some of the connection properties mentioned in the instructions below, the connector accepts variant spellings of the property name. Specifically:

- The connector accepts both `Integrated_Security` and `Integrated Security`.
- The connector accepts both `Server_SPN` and `ServerSPN`.

### Using a User Account

You can authenticate the connection by providing your user name and password for accessing the SQL Server instance.

**To configure authentication using a user account:**

1. Set the `Trusted_Connection` property to `false`.
2. Set the `Integrated_Security` property to `false`.
3. Set the `UID` property to an appropriate user name for accessing the server.
4. Set the `PWD` property to the password corresponding to the user name that you provided above.
Using Kerberos

You can authenticate the connection by using the Kerberos protocol.

To configure authentication using Kerberos:

1. Set the `Trusted_Connection` property to `true`.
2. Set the `Integrated_Security` property to `true`.
3. Set the `Server_SPN` property to the service principal name of the SQL Server instance.

Note:

If you do not set the `Server_SPN` property, the connector uses `MSSQLSvc/[HostName]:[Port]` as the service principal name, where `[HostName]` is the IP address or host name of the server and `[Port]` is the number of the port that you are connecting to.

Using NTLM

You can authenticate the connection by using the NTLM protocol.

To configure authentication using NTLM:

1. Set the `Trusted_Connection` property to NTLM or to NTLMv2 for NTLMv2.
2. Set the `Integrated_Security` property to `true`.
3. Set the `UID` property to an appropriate user name for accessing the server.
4. Set the `PWD` property to the password corresponding to the user name that you provided above.

Configuring TLS Verification on a Non-Windows Machine

If you are connecting to a SQL Server instance that has Transport Layer Security (TLS) enabled, then you can use TLS to encrypt your connection. When connecting to a server using TLS, the connector can be configured to verify the identity of the server. See Security and Authentication on page 44 for more details on TLS.

You can set the connection properties described below in a connection string or in a DSN (in the `odbc.ini` file). Settings in the connection string take precedence over settings in the DSN.

Configuring One-way TLS Verification

You can configure the connector to verify the identity of the server.
To configure one-way TLS verification on a non-Windows machine:

1. To encrypt your connection using TLS, set the Encrypt property to yes.
2. To specify the minimum version of TLS that the connector must use to connect to the server, set the Min_TLS property to the required TLS version. The supported options include 1.0 for TLS 1.0, 1.1 for TLS 1.1, and 1.2 for TLS 1.2.
3. To enable one-way authentication so that the connector verifies the identity of the server, set the TrustServerCertificate property to no.
4. To specify the CA certificate that you want to use to verify the server certificate, set the CACertificate property to the full path and file name of the CA certificate.

Configuring a TLS Connection without Identity Verification

You can configure the connector to use TLS encryption without verifying the identity of the server.

To configure a TLS connection without verification on a non-Windows machine:

1. To encrypt your connection using TLS, set the Encrypt property to yes.
2. To specify the minimum version of TLS that the connector must use to connect to the server, set the Min_TLS property to the required TLS version. The supported options include 1.0 for TLS 1.0, 1.1 for TLS 1.1, and 1.2 for TLS 1.2.
3. To trust the server certificate instead of verifying it, set the TrustServerCertificate property to yes.

Configuring Logging Options on a Non-Windows Machine

To help troubleshoot issues, you can enable logging in the connector or in the wire protocol component.

**Important:**

Only enable logging long enough to capture an issue. Logging decreases performance and can consume a large quantity of disk space.

You can set the connection properties described below in a connection string, in a DSN (in the odbc.ini file), or as a connector-wide setting (in the simba.sqlserverodbc.ini file). Settings in the connection string take precedence over settings in the DSN, and settings in the DSN take precedence over connector-wide settings.
**Connector Logging**

Use connector logging to track the activity in the Simba SQL Server ODBC Connector.

**To enable logging on a non-Windows machine:**

1. To specify the level of information to include in log files, set the `LogLevel` property to one of the following numbers:

<table>
<thead>
<tr>
<th>LogLevel Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disables all logging.</td>
</tr>
<tr>
<td>1</td>
<td>Logs severe error events that lead the connector to abort.</td>
</tr>
<tr>
<td>2</td>
<td>Logs error events that might allow the connector to continue running.</td>
</tr>
<tr>
<td>3</td>
<td>Logs events that might result in an error if action is not taken.</td>
</tr>
<tr>
<td>4</td>
<td>Logs general information that describes the progress of the connector.</td>
</tr>
<tr>
<td>5</td>
<td>Logs detailed information that is useful for debugging the connector.</td>
</tr>
<tr>
<td>6</td>
<td>Logs all connector activity.</td>
</tr>
</tbody>
</table>

2. Set the `LogPath` key to the full path to the folder where you want to save log files. For example:

3. Set the `LogFileCount` key to the maximum number of log files to keep.

**Note:**

After the maximum number of log files is reached, each time an additional file is created, the connector deletes the oldest log file.

4. Set the `LogFileSize` key to the maximum size of each log file in bytes.

**Note:**

After the maximum file size is reached, the connector creates a new file and continues logging.
5. Optionally, to prefix the log file name with the user name and process ID associated with the connection, set the UseLogPrefix property to 1.
6. Save the simba.sqlserverodbc.ini configuration file.
7. Restart your ODBC application to make sure that the new settings take effect.

The Simba SQL Server ODBC Connector produces the following log files at the location you specify in the Log Path field:

- A simbasqlserverodbcdriver.log file that logs connector activity that is not specific to a connection.
- A simbasqlserverodbcdriver_connection_[Number].log file for each connection made to the database, where [Number] is a number that identifies each log file. This file logs connector activity that is specific to the connection.

If you set the UseLogPrefix property to 1, then each file name is prefixed with [UserName]_[ProcessID]_, where [UserName] is the user name associated with the connection and [ProcessID] is the process ID of the application through which the connection is made.

To disable logging on a non-Windows machine:
1. Open the simba.sqlserverodbc.ini configuration file in a text editor.
2. Set the LogLevel key to 0.
3. Save the simba.sqlserverodbc.ini configuration file.
4. Restart your ODBC application to make sure that the new settings take effect.

**Wire Protocol Component Logging**

Use wire protocol component logging to track the data activity between the connector and the SQL Server instance.

To enable wire protocol component logging on a non-Windows machine:
1. Open the simba.sqlserverodbc.ini configuration file in a text editor.
2. Set the TDSTRACE key to [LoggingLevel]:[LogFilePath], where [LoggingLevel] is the logging level indicating the amount of detail to include in the log file and [LogFilePath] is the full path of the log file.

   The following logging levels are supported:
<table>
<thead>
<tr>
<th>Logging Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disables all logging.</td>
</tr>
<tr>
<td>1</td>
<td>Logs error events that might allow the wire protocol component to continue running. 1 is the default logging level.</td>
</tr>
<tr>
<td>2</td>
<td>Logs general information that describes the progress of the wire protocol component.</td>
</tr>
<tr>
<td>3</td>
<td>Logs detailed information that is useful for debugging the wire protocol component.</td>
</tr>
<tr>
<td>4</td>
<td>Logs all activity in the wire protocol component.</td>
</tr>
</tbody>
</table>

For example, the following setting configures the wire protocol component to log debugging information in a file named MyWireLog.log located in the C:\Logs folder:

```
TDSTRACE=3:/localhome/employee/Documents/MyWireLog.log
```

3. Save the simba.sqlserverodbc.ini configuration file.
4. Restart your ODBC application to make sure that the new settings take effect.

**To disable wire protocol component logging on a non-Windows machine:**

1. Set the TDSTRACE key to 0.
2. Save the simba.sqlserverodbc.ini configuration file.
3. Restart your ODBC application to make sure that the new settings take effect.

**Testing the Connection on a Non-Windows Machine**

To test the connection, you can use an ODBC-enabled client application. For a basic connection test, you can also use the test utilities that are packaged with your driver manager installation. For example, the iODBC driver manager includes simple utilities called iodbctest and iodbctestw. Similarly, the unixODBC driver manager includes simple utilities called isql and iusql.

**Using the iODBC Driver Manager**

You can use the iodbctest and iodbctestw utilities to establish a test connection with your connector. Use iodbctest to test how your connector works with an ANSI
application, or use iodbctestw to test how your connector works with a Unicode application.

**Note:**
There are 32-bit and 64-bit installations of the iODBC driver manager available. If you have only one or the other installed, then the appropriate version of iodbctest (or iodbctestw) is available. However, if you have both 32- and 64-bit versions installed, then you need to make sure that you are running the version from the correct installation directory.

For more information about using the iODBC driver manager, see [http://www.iodbc.org](http://www.iodbc.org).

**To test your connection using the iODBC driver manager:**

1. Run iodbctest or iodbctestw.
2. Optionally, if you do not remember the DSN, then type a question mark (?) to see a list of available DSNs.
3. Type the connection string for connecting to your data store, and then press ENTER. For more information, see Using a Connection String on page 39.

If the connection is successful, then the SQL> prompt appears.

**Using the unixODBC Driver Manager**

You can use the isql and iusql utilities to establish a test connection with your connector and your DSN. isql and iusql can only be used to test connections that use a DSN. Use isql to test how your connector works with an ANSI application, or use iusql to test how your connector works with a Unicode application.

**Note:**
There are 32-bit and 64-bit installations of the unixODBC driver manager available. If you have only one or the other installed, then the appropriate version of isql (or iusql) is available. However, if you have both 32- and 64-bit versions installed, then you need to make sure that you are running the version from the correct installation directory.

For more information about using the unixODBC driver manager, see [http://www.unixodbc.org](http://www.unixodbc.org).

**To test your connection using the unixODBC driver manager:**

- Run isql or iusql by using the corresponding syntax:
isql [DataSourceName]
 iusql [DataSourceName]

[DataSourceName] is the DSN that you are using for the connection.

If the connection is successful, then the SQL> prompt appears.

Note:
For information about the available options, run isql or iusql without providing a DSN.
Using a Connection String

For some applications, you might need to use a connection string to connect to your data source. For detailed information about how to use a connection string in an ODBC application, refer to the documentation for the application that you are using.

The connection strings in the following sections are examples showing the minimum set of connection attributes that you must specify to successfully connect to the data source. Depending on the configuration of the data source and the type of connection you are working with, you might need to specify additional connection attributes. For detailed information about all the attributes that you can use in the connection string, see Connector Configuration Options on page 45.

DSN Connection String Example

The following is an example of a connection string for a connection that uses a DSN:

```sql
DSN=[DataSourceName]
```

[DataSourceName] is the DSN that you are using for the connection.

You can set additional configuration options by appending key-value pairs to the connection string. Configuration options that are passed in using a connection string take precedence over configuration options that are set in the DSN.

DSN-less Connection String Examples

Some applications provide support for connecting to a data source using a connector without a DSN. To connect to a data source without using a DSN, use a connection string instead.

The placeholders in the example are defined as follows, in alphabetical order:

- \[PortNumber\] is the number of the TCP port that the SQL Server instance uses to listen for client connections.
- \[ServerInfo\] is the IP address or host name of the SQL Server instance to which you are connecting.
- \[ServiceName\] is the Kerberos service principal name of the SQL Server instance.
- \[SQLServerDatabase\] is the name of the database that you want to access.
- \[YourPassword\] is the password corresponding to your user name.
- \([\text{YourUserName}]\) is the user name that you use to access the SQL Server instance.

**Connecting to a SQL Server Instance Using User Login**

The following is an example of a DSN-less connection string for a connection to a SQL Server instance that requires user login:

```
Driver=Simba SQL Server ODBC Driver;Server=[ServerInfo];
Port=[PortNumber];Database=[SQLServerDatabase];
UID=[YourUserName];PWD=[YourPassword];
```

For example:

```
Driver=Simba SQL Server ODBC Driver;
Server=192.168.222.160;Port=1500;Database=TestDB;
UID=simba;PWD=simba;
```

**Connecting to a SQL Server Instance Using Kerberos Authentication**

**Note:**

For some of the connection properties included in the examples below, the connector accepts variant spellings of the property name. Specifically:

- The connector accepts both `Integrated_Security` and `Integrated Security`.
- The connector accepts both `Server_SPN` and `ServerSPN`.

The following is an example of a DSN-less connection string for a connection to a SQL Server instance that requires authentication through Kerberos:

```
Driver=Simba SQL Server ODBC Driver;Server=[ServerInfo];
Port=[PortNumber];Database=[SQLServerDatabase];
Trusted_Connection=true;Integrated_Security=true;
Server_SPN=[ServiceName];
```

For example:

```
Driver=Simba SQL Server ODBC Driver;
Server=192.168.222.160;Port=1500;Database=TestDB;
Trusted_Connection=true;Integrated_Security=true;
Server_SPN=sqls;
```
Connecting to a SQL Server Instance Using NTLM Authentication

Note:
For the Integrated Security property, which is included in the examples below, the connector also accepts Integrated Security as a valid spelling of the property name.

The following is an example of a DSN-less connection string for a connection to a SQL Server instance that requires authentication through the NTLM protocol:

```plaintext
Driver=Simba SQL Server ODBC Driver;Server=[ServerInfo];Port=[PortNumber];Database=[SQLServerDatabase];Integrated_Security=true;Trusted_Connection=NTLM;UID=[YourUserName];PWD=[YourPassword];
```

For example:

```plaintext
Driver=Simba SQL Server ODBC Driver;
Server=192.168.222.160;Port=1500;Database=TestDB;
Integrated_Security=true;Trusted_Connection=NTLM;
UID=domain\simba;PWD=simba;
```
For more information on the features of the Simba SQL Server ODBC Connector, see the following:

- Data Types on page 42
- Security and Authentication on page 44

Data Types

The Simba SQL Server ODBC Connector supports many common data formats, converting between SQL Server data types and SQL data types.

The table below lists the supported data type mappings.

<table>
<thead>
<tr>
<th>SQL Server Type</th>
<th>SQL Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>BigInt</td>
<td>SQL_BIGINT</td>
</tr>
<tr>
<td>BigInt Identity</td>
<td>SQL_BIGINT</td>
</tr>
<tr>
<td>Binary</td>
<td>SQL_BINARY</td>
</tr>
<tr>
<td>Bit</td>
<td>SQL_BIT</td>
</tr>
<tr>
<td>Char</td>
<td>SQL_CHAR</td>
</tr>
<tr>
<td>Date</td>
<td>SQL_TYPE_DATE</td>
</tr>
<tr>
<td>DateTime</td>
<td>SQL_TYPE_TIMESTAMP</td>
</tr>
<tr>
<td>DateTime2</td>
<td>SQL_TYPE_TIMESTAMP</td>
</tr>
<tr>
<td>DateTimeOffset</td>
<td>SQL_SS_TIMESTAMPOFFSET</td>
</tr>
<tr>
<td>Decimal</td>
<td>SQL_DECIMAL</td>
</tr>
<tr>
<td>Decimal() Identity</td>
<td>SQL_DECIMAL</td>
</tr>
<tr>
<td>Float</td>
<td>SQL_FLOAT</td>
</tr>
<tr>
<td>SQL Server Type</td>
<td>SQL Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>GUID</td>
<td>SQL_GUID</td>
</tr>
<tr>
<td>Image</td>
<td>SQL_LONGVARBINARY</td>
</tr>
<tr>
<td>Int</td>
<td>SQL_INTEGER</td>
</tr>
<tr>
<td>Int Identity</td>
<td>SQL_INTEGER</td>
</tr>
<tr>
<td>Money</td>
<td>SQL_DECIMAL</td>
</tr>
<tr>
<td>NChar</td>
<td>SQL_WCHAR</td>
</tr>
<tr>
<td>NText</td>
<td>SQL_WLONGVARCHAR</td>
</tr>
<tr>
<td>Numeric</td>
<td>SQL_NUMERIC</td>
</tr>
<tr>
<td>Numeric() Identity</td>
<td>SQL_NUMERIC</td>
</tr>
<tr>
<td>NVarChar</td>
<td>SQL_WVARCHAR</td>
</tr>
<tr>
<td>NVarChar(Max)</td>
<td>SQL_WVARCHAR</td>
</tr>
<tr>
<td>Real</td>
<td>SQL_REAL</td>
</tr>
<tr>
<td>RowVersion</td>
<td>SQL_BINARY</td>
</tr>
<tr>
<td>SmallDateTime</td>
<td>SQL_TYPE_TIMESTAMP</td>
</tr>
<tr>
<td>SmallInt</td>
<td>SQL_SMALLINT</td>
</tr>
<tr>
<td>SmallInt Identity</td>
<td>SQL_INTEGER</td>
</tr>
<tr>
<td>SmallMoney</td>
<td>SQL_DECIMAL</td>
</tr>
<tr>
<td>SysName</td>
<td>SQL_WVARCHAR</td>
</tr>
<tr>
<td>Text</td>
<td>SQL_LONGVARCHAR</td>
</tr>
<tr>
<td>Time</td>
<td>SQL_SS_TIME2</td>
</tr>
<tr>
<td>SQL Server Type</td>
<td>SQL Type</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>TinyInt</td>
<td>SQL_TINYINT</td>
</tr>
<tr>
<td>TinyInt Identity</td>
<td>SQL_TINYINT</td>
</tr>
<tr>
<td>VarBinary</td>
<td>SQL_VARBINARY</td>
</tr>
<tr>
<td>VarBinary(Max)</td>
<td>SQL_VARBINARY</td>
</tr>
<tr>
<td>VarChar</td>
<td>SQL_VARCHAR</td>
</tr>
<tr>
<td>VarChar(Max)</td>
<td>SQL_VARCHAR</td>
</tr>
</tbody>
</table>

In addition, certain SQL Server data types are exposed via custom type identifiers, as in the native SQL Server connector:

- Geometry, Geography, and HierarchyID use custom type -151.
- XML uses custom type -152.

## Security and Authentication

To protect data from unauthorized access, SQL Server data stores require connections to be authenticated with user credentials and sometimes the TLS protocol. The Simba SQL Server ODBC Connector provides full support for these authentication protocols.

The connector provides mechanisms that enable you to authenticate your connection using the Kerberos protocol, the NTLM protocol, or your SQL Server user name and password. For detailed configuration instructions, see Configuring Authentication on Windows on page 12 or Configuring Authentication on a Non-Windows Machine on page 31.

Additionally, the connector supports TLS connections with or without one-way authentication. If the server has a TLS-enabled socket, then you can configure the connector to connect to it. The connector supports TLS 1.0 to 1.2. The TLS version used for the connection is the highest version that is supported by both the connector and the server.

It is recommended that you enable TLS whenever you connect to a server that is configured to support it. TLS encryption protects data and credentials when they are transferred over the network, and provides stronger security than authentication alone. For detailed configuration instructions, see Creating a Data Source Name on Windows on page 9 or Configuring TLS Verification on a Non-Windows Machine on page 32.
Connector Configuration Options

Connector Configuration Options lists the configuration options available in the Simba SQL Server ODBC Connector alphabetically by field or button label. Options having only key names, that is, not appearing in the user interface of the connector, are listed alphabetically by key name.

When creating or configuring a connection from a Windows machine, the fields and buttons described below are available in the Simba SQL Server ODBC Driver DSN Setup dialog box.

When using a connection string or configuring a connection from a Linux or macOS machine, use the key names provided below.

Configuration Options Appearing in the User Interface

The following configuration options are accessible via the Windows user interface for the Simba SQL Server ODBC Connector, or via the key name when using a connection string or configuring a connection from a Linux or macOS machine:

- Application Intent on page 46
- Application Name on page 46
- CA Certificate on page 46
- Database on page 47
- Description on page 47
- Enable Table Types on page 47
- Encrypt on page 48
- Log Level on page 48
- Log Path on page 49
- Max File Size on page 50
- Max Number Files on page 51
- Minimum TLS/SSL on page 50
- Password on page 51
- Port on page 51
- Return SQL Server-Specific Types as ODBC Types on page 52
- Server on page 52
- Server SPN on page 53
- Trust Server Certificate on page 53
- Use NTLM on page 54
- Use Trusted Connection on page 54
- User on page 55
## Application Intent

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application(Intent)</td>
<td>ReadWrite</td>
<td>No</td>
</tr>
</tbody>
</table>

### Description

This option controls whether or not the connector is in read-only mode.

- **ReadWrite**: The connection is not in read-only mode.
- **ReadOnly**: The connection is in read-only mode.

## Application Name

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application_Name</td>
<td>None</td>
<td>No</td>
</tr>
</tbody>
</table>

### Description

This option specifies the name of the application that calls SQLDriverConnect.

## CA Certificate

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>CACertificate</td>
<td>cacerts.pem</td>
<td>Yes, if the Encrypt option is enabled and the Trust Server Certificate option is disabled.</td>
</tr>
</tbody>
</table>

### Description

The full path and file name of the CA certificate that you want to use to verify the server certificate when TLS encryption is enabled.

For information about how to trust the server certificate instead of verifying it, see [Trust Server Certificate](#) on page 53.
Database

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>None</td>
<td>No</td>
</tr>
</tbody>
</table>

Description
The name of the SQL Server database that you want to access.

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Simba AmazonSQL Server ODBC DSN</td>
<td>No</td>
</tr>
</tbody>
</table>

Description
This description can be used to provide information about the DSN. For example, a descriptive comment about what the DSN is used for.

Enable Table Types

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnableTableTypes</td>
<td>Clear (no)</td>
<td>No</td>
</tr>
</tbody>
</table>

Description
This option specifies whether the connector includes temporary tables in the results when calling SQLTables.

- **Enabled** (*yes, true, or 1*): The connector includes temporary tables.
- **Disabled** (*no, false, or 0*): The connector does not include temporary tables.
Encrypt

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt</td>
<td>Clear (no)</td>
<td>No</td>
</tr>
</tbody>
</table>

Description

This option specifies whether the connector uses TLS to encrypt communication with the SQL Server instance before sending it over the network. The connector supports TLS 1.0 to 1.2. The TLS version used for the connection is the highest version that is supported by both the connector and the server.

- **Enabled (yes, true, or 1):** The connector encrypts all communication with the SQL Server instance.
- **Disabled (no, false, or 0):** The connector does not encrypt communication with the SQL Server instance.

For information about configuring identity verification between the connector and the server, see **CA Certificate** on page 46 and **Trust Server Certificate** on page 53.

Log Level

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogLevel</td>
<td>OFF (0)</td>
<td>No</td>
</tr>
</tbody>
</table>

Description

Use this property to enable or disable logging in the connector and to specify the amount of detail included in log files.

⚠️ **Important:**

- Only enable logging long enough to capture an issue. Logging decreases performance and can consume a large quantity of disk space.
- When logging with connection strings and DSNs, this option only applies to per-connection logs.

Set the property to one of the following values:
- OFF (0): Disable all logging.
- FATAL (1): Logs severe error events that lead the connector to abort.
- ERROR (2): Logs error events that might allow the connector to continue running.
- WARNING (3): Logs events that might result in an error if action is not taken.
- INFO (4): Logs general information that describes the progress of the connector.
- DEBUG (5): Logs detailed information that is useful for debugging the connector.
- TRACE (6): Logs all connector activity.

When logging is enabled, the connector produces the following log files at the location you specify in the Log Path (LogPath) property:

- A simbasqlserverodbcdriver.log file that logs connector activity that is not specific to a connection.
- A simbasqlserverodbcdriver_connection_[Number].log file for each connection made to the database, where [Number] is a number that identifies each log file. This file logs connector activity that is specific to the connection.

If you enable the UseLogPrefix connection property, the connector prefixes the log file name with the user name associated with the connection and the process ID of the application through which the connection is made. For more information, see UseLogPrefix on page 59.

### Log Path

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogPath</td>
<td>None</td>
<td>Yes, if logging is enabled.</td>
</tr>
</tbody>
</table>

**Description**

The full path to the folder where the connector saves log files when logging is enabled.

**Important:**

When logging with connection strings and DSNs, this option only applies to per-connection logs.
Max File Size

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogFileSize</td>
<td>20971520</td>
<td>No</td>
</tr>
</tbody>
</table>

Description

The maximum size of each log file in bytes. After the maximum file size is reached, the connector creates a new file and continues logging.

If this property is set using the Windows UI, the entered value is converted from megabytes (MB) to bytes before being set.

⚠️ Important:
When logging with connection strings and DSNs, this option only applies to per-connection logs.

Minimum TLS/SSL

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min_TLS</td>
<td>When encryption is requested: 1.2 (1.2) When encryption is not requested: 1.0 (1.0)</td>
<td>No</td>
</tr>
</tbody>
</table>

Description

The minimum version of TLS/SSL that the connector allows the data store to use for encrypting connections. For example, if TLS 1.1 is specified, TLS 1.0 cannot be used to encrypt connections.

- 1.0 (1.0): The connection must use at least TLS 1.0.
- 1.1 (1.1): The connection must use at least TLS 1.1.
- 1.2 (1.2): The connection must use at least TLS 1.2.
Max Number Files

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogFileCount</td>
<td>50</td>
<td>No</td>
</tr>
</tbody>
</table>

Description

The maximum number of log files to keep. After the maximum number of log files is reached, each time an additional file is created, the connector deletes the oldest log file.

⚠️ Important:

When logging with connection strings and DSNs, this option only applies to per-connection logs.

Password

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWD</td>
<td>None</td>
<td>Yes, if authenticating through user login or the NTLM protocol.</td>
</tr>
</tbody>
</table>

Description

The password corresponding to the user name that you provided in the User field (the UID key).

Port

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>1433</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Description

The number of the TCP port that the SQL Server instance uses to listen for client connections.
Return SQL Server-Specific Types as ODBC Types

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReturnSpecificType AsOdbcType</td>
<td>Clear (no)</td>
<td>No</td>
</tr>
</tbody>
</table>

**Description**

This option specifies whether the connector returns the SQL Server-specific data types that are listed in the table below as ODBC data types, or as SQL Server data types.

- **Enabled (yes, true, or 1):** The connector returns the data types listed below as ODBC data types.
- **Disabled (no, false, or 0):** The connector returns the data types listed below as SQL Server data types.

<table>
<thead>
<tr>
<th>SQL Server Type</th>
<th>Returned ODBC Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDS_SQL_SS_TIME</td>
<td>SQL_TYPE_TIME</td>
</tr>
<tr>
<td>TDS_SQL_SS_DATETIMEOFFSET</td>
<td>SQL_WVARCHAR</td>
</tr>
</tbody>
</table>

**Server**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>None</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Description**

The host name or IP address of the SQL Server instance.
Server SPN

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server_SPN or ServerSPN</td>
<td>MSSQLSvc/ [HostName]:[Port], where [HostName] is the server name or IP address specified in the Server option and [Port] is the port number specified in the Port option.</td>
<td>No</td>
</tr>
</tbody>
</table>

Description
The service principal name of the SQL Server instance.

Trust Server Certificate

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrustServerCertificate</td>
<td>Clear (no)</td>
<td>No</td>
</tr>
</tbody>
</table>

Description
This option specifies whether the connector trusts the server certificate when connecting to the server using TLS.

- **Enabled (yes, true, or 1):** The connector trusts the server certificate.
- **Disabled (no, false, or 0):** The connector does not trust the server certificate, and instead uses a CA certificate to verify the server certificate.

For information about how to specify a CA certificate, see [CA Certificate](#) on page 46.
Use NTLM

<table>
<thead>
<tr>
<th>Names of Keys</th>
<th>Default Value for Each Key</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated_Security or Integrated Security and</td>
<td>Clear (false)</td>
<td>No</td>
</tr>
<tr>
<td>Trusted_Connection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description

This option specifies whether the connector uses the NTLM protocol to authenticate connections to SQL Server.

- **Enabled** (Integrated_Security or Integrated Security is set to true, and Trusted_Connection is set to NTLM or to NTLMv2): The connector uses the NTLM protocol to authenticate connections.
- **Disabled** (Integrated_Security, Integrated Security, or Trusted_Connection is set to false): The connector does not use the NTLM protocol.

Use Trusted Connection

<table>
<thead>
<tr>
<th>Names of Keys</th>
<th>Default Value for Each Key</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated_Security or Integrated Security and</td>
<td>Clear (false)</td>
<td>No</td>
</tr>
<tr>
<td>Trusted_Connection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description

This option specifies whether the connector uses the Kerberos protocol to authenticate connections to SQL Server.

- **Enabled** (Integrated_Security or Integrated Security is set to true, and Trusted_Connection is also set to true): The connector uses the Kerberos protocol to authenticate connections.
- **Disabled** (*Integrated Security*, *Integrated Security*, or *Trusted Connection* is set to false): The connector does not use the Kerberos protocol.

**User**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
<td>None</td>
<td>Yes, if authenticating through user login or the NTLM protocol.</td>
</tr>
</tbody>
</table>

**Description**

The user name that you use to access the SQL Server instance.

**Configuration Options Having Only Key Names**

The following configuration options do not appear in the Windows user interface for the Simba SQL Server ODBC Connector. They are accessible only when you use a connection string or configure a connection on macOS or Linux.

- **Driver** on page 56
- **LongColumnLength** on page 56
- **MaxCatalogNameLen** on page 56
- **MaxColumnNameLen** on page 57
- **MaxSchemaNameLen** on page 57
- **MaxTableNameLen** on page 57

The **TDSTRACE** option is available only as an environment variable.

- **TDSTRACE** on page 58

The **UseLogPrefix** property must be configured as a Windows Registry key value, or as a connector-wide property in the `simba.sqlserverodbc.ini` file for macOS or Linux.

- **UseLogPrefix** on page 59
## Driver

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver</td>
<td>Simba SQL Server ODBC Connector when installed on Windows, or the absolute path of the connector shared object file when installed on a non-Windows machine.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Description

On Windows, the name of the installed connector (Simba SQL Server ODBC Connector).

On other platforms, the name of the installed connector as specified in `odbcinst.ini`, or the absolute path of the connector shared object file.

## LongColumnLength

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>LongColumnLength</td>
<td>8000</td>
<td>No</td>
</tr>
</tbody>
</table>

### Description

The maximum size of BLOB and CLOB columns.

## MaxCatalogNameLen

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxCatalogNameLen</td>
<td>128</td>
<td>No</td>
</tr>
</tbody>
</table>

### Description

The maximum number of characters that can be returned for catalog names.
This option can be set to any integer from 0 to 65535, inclusive. To indicate that there is no maximum length or that the length is unknown, set this option to 0.

**MaxColumnNameLen**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxColumnNameLen</td>
<td>128</td>
<td>No</td>
</tr>
</tbody>
</table>

**Description**

The maximum number of characters that can be returned for column names.

This option can be set to any integer from 0 to 65535, inclusive. To indicate that there is no maximum length or that the length is unknown, set this option to 0.

**MaxSchemaNameLen**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxSchemaNameLen</td>
<td>128</td>
<td>No</td>
</tr>
</tbody>
</table>

**Description**

The maximum number of characters that can be returned for schema names.

This option can be set to any integer from 0 to 65535, inclusive. To indicate that there is no maximum length or that the length is unknown, set this option to 0.

**MaxTableNameLen**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxTableNameLen</td>
<td>128</td>
<td>No</td>
</tr>
</tbody>
</table>

**Description**

The maximum number of characters that can be returned for table names.

This option can be set to any integer from 0 to 65535, inclusive. To indicate that there is no maximum length or that the length is unknown, set this option to 0.
TDSTRACE

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDSTRACE</td>
<td>None</td>
<td>No</td>
</tr>
</tbody>
</table>

**Description**

Use this property to enable or disable logging in the wire protocol component and to specify the amount of detail included in log files.

⚠️ Important:

- Only enable logging long enough to capture an issue. Logging decreases performance and can consume a large quantity of disk space.
- This option is not supported in DSNs or connection strings. To configure wire protocol logging for the Windows connector, you must set TDSTRACE as an environment variable. To configure wire protocol logging for a non-Windows connector, you must set TDSTRACE in the simba.sqlserverodbc.ini file.

Set the property to `[LoggingLevel]:[LogFilePath]`, where `[LoggingLevel]` is the logging level indicating the amount of detail to include in the log file and `[LogFilePath]` is the fill path of the log file.

The logging levels are supported:

- 0: Disable all logging.
- 1: Logs error events that might allow the wire protocol component to continue running.
- 2: Logs general information that describes the progress of the wire protocol component.
- 3: Logs detailed information that is useful for debugging the wire protocol component.
- 4: Logs all activity in the wire protocol component.

For example, setting TDSTRACE to `3:C:\Logs\MyWireLog.log` configures the wire protocol component to log debugging information in a file named `MyWireLog.log` located in the `C:\Logs` folder.
UseLogPrefix

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseLogPrefix</td>
<td>0</td>
<td>No</td>
</tr>
</tbody>
</table>

**Description**

This option specifies whether the connector includes a prefix in the names of log files so that the files can be distinguished by user and application.

Set the property to one of the following values:

- 1: The connector prefixes log file names with the user name and process ID associated with the connection that is being logged.
- 0: The connector does not include the prefix in log file names.

To configure this option for the Windows connector, you create a value for it in one of the following registry keys:

- For a 32-bit connector installed on a 64-bit machine: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Simba\Simba SQL Server ODBC Connector\Driver`
- Otherwise: `HKEY_LOCAL_MACHINE\SOFTWARE\Simba\Simba SQL Server ODBC Connector\Driver`

Use `UseLogPrefix` as the value name, and either 0 or 1 as the value data.

To configure this option for a non-Windows connector, you must use the `simba.sqlserverodbc.ini` file.
Debian is a trademark or registered trademark of Software in the Public Interest, Inc. or its subsidiaries in Canada, United States and/or other countries.

Linux is the registered trademark of Linus Torvalds in Canada, United States and/or other countries.

Mac, macOS, Mac OS, and OS X are trademarks or registered trademarks of Apple, Inc. or its subsidiaries in Canada, United States and/or other countries.

Microsoft SQL Server, SQL Server, Microsoft, MSDN, Windows, Windows Server, Windows Vista, and the Windows start button are trademarks or registered trademarks of Microsoft Corporation or its subsidiaries in Canada, United States and/or other countries.

Red Hat, Red Hat Enterprise Linux, and CentOS are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in Canada, United States and/or other countries.

SUSE is a trademark or registered trademark of SUSE LLC or its subsidiaries in Canada, United States and/or other countries.

Ubuntu is a trademark or registered trademark of Canonical Ltd. or its subsidiaries in Canada, United States and/or other countries.

All other trademarks are trademarks of their respective owners.