




# CAST Database Extractor - Source panel

 This section provides a detailed description of the contents of the **Source panel** in the [CAST Database Extractor](#).

Source	Options	Target
Vendor	Oracle	
JDBC Driver	oracle.jdbc.OracleDriver	
Database URL	jdbc:oracle:thin:@<server name>:1521:<instance name>	
User		
Password		
Database Parameters	schema	<schemas or blank>
	minimal_access_mode	dba
	skip_comments	no
	skip_modification_check_schema	
	connection:oracle.net.encryption_client	REQUESTED
	connection:oracle.net.encryption_types_client	( AES 128 )
	connection:oracle.net.crypto_checksum_client	REQUESTED
	connection:oracle.net.crypto_checksum_types_client	( MD5 )

This panel enables you to define the parameters for the extraction process, i.e. your source database server, how to connect to it, what to extract etc. Each item is explained in more detail below:

<b>Vendor</b>	<p>Use this option to choose the target RDBMS vendor for the extraction process:</p> <ul style="list-style-type: none"><li>• <b>Oracle</b> (default)</li><li>• <b>SQLServer</b> (Microsoft SQL Server)</li><li>• <b>ASESybaseServer</b> (Sybase ASE)</li><li>• <b>AzureSQL</b> (Azure SQL - handled as Microsoft SQL Server)</li></ul> <p> Choosing an option will display configuration options specific to that Vendor.</p>
<b>JDBC Driver</b>	<p>Choose the JDBC Driver from the drop down list that is appropriate for the platform chosen above:</p> <ul style="list-style-type: none"><li>• <b>oracle.jdbc.OracleDriver</b> (Oracle - default)</li><li>• <b>net.sourceforge.jtds.jdbc.Driver</b> (Microsoft SQL Server, Sybase ASE or AzureSQL)</li></ul> <p> Note that in early beta releases of this component, the driver <b>com.microsoft.jdbc.sqlserver.SQLServerDriver</b> is available for use. <b>PLEASE DO NOT USE THIS DRIVER - INSTEAD ALWAYS USE THE net.sourceforge.jtds.jdbc.Driver DRIVER FOR BOTH MICROSOFT SQL SERVER AND SYBASE ASE</b></p>

**Database URL**

This command is used to specify the source server for connection purposes. Manually enter the JDBC Connection parameters for the platform /JDBC driver chosen above.



Note that by default the field will be populated with the **Oracle** database URL, therefore you may need to change it as described below.

**oracle.jdbc.OracleDriver** (default)

```
SID/INSTANCE NAME: jdbc:oracle:thin:@<SERVER_NAME>:<PORT>:<INSTANCE NAME>  
SERVICE NAME: jdbc:oracle:thin://<SERVER_NAME>:<PORT>/<SERVICE>
```

- **<SERVER NAME>**: replace with the name or IP address of the server hosting your Oracle database
- **<PORT>**: specify the port number on which your Oracle instance/service is running. By default this is 1521 but this may have been changed in your environment
- **<INSTANCE NAME>**: replace with the name of your Oracle instance
- **<SERVICE>**: replace with the service name of your Oracle database

## net.sourceforge.jtds.jdbc.Driver

```
jdbc:jtds:<SERVER_TYPE>://<SERVER>[:<PORT>][/<DATABASE>][;<PROPERTY>=<VALUE>[;...]]
```

- **<SERVER\_TYPE>**: (required) replace this with either "sqlserver" or "sybase" depending on the RDBMS you are accessing. For **Azure SQL**, use "sqlserver".
- **<SERVER>**: (required) replace with the name or IP address of the server hosting your RDBMS. For **Azure SQL** this is the **Azure SQL server name**.
- **<PORT>**: (optional) specify the port number on which your RDBMS is running. By default this is **1433** for **Azure SQL/Microsoft SQL Server** and **5000** for **Sybase ASE**, but this may have been changed in your environment
- **<DATABASE>**: (optional and only used when working with **Microsoft SQL Server/Azure SQL**):
  - For **Microsoft SQL Server**, specifies the instance name where the RDBMS is running in a named instance configuration. If you omit this, then the default instance will be accessed.
  - For **Azure SQL**, this is the Azure SQL database name (only one database can be associated to an Azure SQL server)
- **<PROPERTY>/<VALUE>**: (optional) only required in specific situations (see below).



See <http://jtds.sourceforge.net/faq.html#urlFormat> for more information about the jTDS URL format.

### Specific situation: Azure SQL

Example Azure SQL database URL:

```
jdbc:jtds:sqlserver://my_server.database.windows.net:1433/my_database;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30
```

### Specific situations: Windows authentication

If your target server requires that you use **Windows authentication**, you can use the following URL format when running the extractor on a Windows machine:

```
jdbc:jtds:<SERVER_TYPE>://<SERVER>[:<PORT>];useNTLMv2=true;domain=xxx
```

Note that:

- You still need to insert a **User** and **Password** in the relevant fields (see <http://jtds.sourceforge.net/faq.html#windowsAuth> for more information)
- You need to ensure that you download and install the **ntlmauth.dll** file as follows:
  - Download the latest jTDS driver in ZIP format from <https://sourceforge.net/projects/jtds/files/>
  - Extract the ZIP and then find the following file in the resulting folder hierarchy: **x64\SSO\ntlmauth.dll** (or **x86\SSO\ntlmauth.dll** if you are running the extractors on a 32bit Windows Operating System)
  - Copy the **ntlmauth.dll** file to **%SYSTEMROOT%\system32**
  - Now restart the extractor before you attempt to use it.

### Specific situations: SSL encryption

If your target server requires that you use **SSL encryption**, you can use the following URL format when running the extractor on a Windows machine:

```
jdbc:jtds:<SERVER_TYPE>://<SERVER>[:<PORT>];ssl=require
```

**Us  
er**

This command tells the extraction tool what login to use to access the source server. Enter a login with sufficient rights as explained in [SQL - Required RDBMS rights for packaging a database using the legacy CAST Delivery Manager Tool](#). When attempting to connect to an **Azure SQL database**, the user name should be entered as follows:



```
[User]@[Server]
```

**Pa  
ss  
wo  
rd**

This command tells the extraction tool what password to use to access the source server (corresponds to the login specified above). Enter the correct password for the login specified above.

**Da  
tab  
as**

These commands specify the schema/database you would like to extract:

Option	Description
<b>schema</b>	Only visible when an <b>Oracle driver has been selected</b> and is therefore only of use for <b>Oracle</b> extractions. Please see the notes below about how to use this field.
<b>minimal_access_mode</b>	<p>Only visible when an <b>Oracle driver has been selected</b> and is therefore only of use for <b>Oracle</b> extractions. This option accepts either of the following values:</p> <ul style="list-style-type: none"> <li>• <b>dba</b> (default setting) &gt; this value will prevent an extraction from starting if the user login entered in the <b>User</b> field (above) only has rights to query the <b>ALL_* views</b>. This is a fail-safe mechanism because these views only give access to objects that the user is entitled to access: this means that CAST cannot guarantee that the extraction will contain all the required data. This value can also improve performance.</li> <li>• <b>all</b> &gt; if the user login entered in the <b>User</b> field (above) only has rights to query the <b>ALL_* views</b> and you understand that these views only give access to objects that the user is entitled to access (meaning that CAST cannot guarantee that the extraction will contain all the required data) and that extraction performance may be reduced, then you <b>MUST</b> enter the <b>all</b> value in this field to enable the extraction to start. <b>ALL_* views</b> will then be queried.</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Note that this option is identical to the <b>ALL access mode</b> check box provided in the <b>CAST Delivery Manager Tool</b> for Oracle extractions. In the CAST Delivery Manager Tool, <b>selecting the ALL access mode check box</b> is equivalent to inserting "all" in the <b>minimal_access_mode</b> field.</p> </div>
<b>skip_comments</b>	<p>Only visible when an <b>Oracle driver has been selected</b> and is therefore only of use for <b>Oracle</b> extractions. This option determines whether comments on tables, columns, views and materialized views will be extracted or not. Extracting comments (or not) has no impact on analysis results or Automated Function Point values - they will either be visible or not in CAST Enlighten. Accepts either of the following lowercase values:</p> <ul style="list-style-type: none"> <li>• <b>no</b> (default setting)</li> <li>• <b>yes</b> &gt; this can improve performance.</li> </ul>
<b>skip_modification_check_schema</b>	<p>Only visible when an <b>Oracle driver has been selected</b> and is therefore only of use for <b>Oracle</b> extractions. If an object is compiled or modified when the extraction is run, the database extractor will detect this by default and messages to that effect will be displayed in the log file (see <a href="#">What happens if an object is compiled or modified when the extraction is run on an Oracle Server?</a>). If you would prefer that this check is <b>not performed</b> during an extraction, then you can list the <b>schemas (separated by commas)</b> which should be excluded from the check.</p>
<b>database</b>	<p>Only visible when a <b>Microsoft SQL Server</b> or <b>Sybase ASE</b> driver has been selected and is there only of use for <b>Microsoft SQL Server</b> and <b>Sybase ASE</b> extractions. Please see the notes below about how to use this field.</p>
<b>connection:oracle.net.encryption_client</b>	<p>Only visible when an <b>Oracle driver has been selected</b>. These options are aimed at extraction of schemas hosted on <b>Oracle Server 11 / 12</b> that require <b>encrypted connections</b>.</p> <p>These four options allow you to configure the database extractor to connect to an <b>Oracle Server which accepts only encrypted connections</b>. The default values provided in the CAST Database Extractor are the default settings used on the Oracle Server side, therefore if your target Oracle Server uses a custom/specific encryption policy, you should change the options in the CAST Database Extractor to match those defined in the <b>SQLNET.ORA</b> file.</p>
<b>connection:oracle.net.encryption_types_client</b>	<p>If your target Oracle Server is configured to accept unencrypted connections, please manually remove all options from all four fields.</p> <p>Permitted values:</p>
<b>connection:oracle.net.crypto_checksum_client</b>	<ul style="list-style-type: none"> <li>• <b>connection:oracle.net.encryption_client</b>: REJECTED, ACCEPTED, REQUESTED, REQUIRED</li> <li>• <b>connection:oracle.net.encryption_types_client</b>: AES256, AES192, AES128</li> <li>• <b>connection:oracle.net.crypto_checksum_client</b>: REJECTED, ACCEPTED, REQUESTED, REQUIRED</li> <li>• <b>connection:oracle.net.crypto_checksum_types_client</b>: SHA512, SHA384, SHA256, SHA1, MD5</li> </ul>
<b>connection:oracle.net.crypto_checksum_types_client</b>	<div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Note that while the possibility to accept encrypted was introduced in <b>Oracle Server 10g</b>, the default settings available in the CAST Database Extractor may not be fully compatible and CAST does not recommend using them unless you are forced to.</p> </div>

**Notes**

- To extract an **individual schema/database**, enter the **NAME** of the schema/database in the **schema** or **database** field.
- If you intend to extract an **entire instance** and all schemas/databases, leave the **schema** or **database** field blank.
- If you intend to extract **multiple schemas/databases** you can list them separated with a comma (",").
- Please ensure that you input the name of the schema/database in the schema/database field in the **correct case** (i.e. upper or lower) as these fields are case sensitive - remember that the vast majority of Oracle schemas are in upper case.
- If you have objects from different schemas/databases on the same instance that are linked (i.e. inter-schema links such as "Database-Links" or between objects in different schemas) and you expect the analysis to detect and store these links, then you must ensure that you carry out ONE extraction on all the schemas/databases involved (i.e. specify the schemas/database involved separated with a comma). If you are unsure which schemas/databases are involved, you can extract the entire instance by leaving the field blank, but this can affect performance.
- The CAST Database Extractor will carry out an automatic validation of the information entered into this field to counter the incorrect use of case or the input of a non-existent schema/database. The extraction process will be stopped and an error will be displayed if the validation fails.