SSL connection from VDP to data sources

Revision 20180322

Goal
This document describes how to configure VDP to connect to data sources that use an SSL connection.

Content
When Virtual DataPort establishes an SSL connection with a data source, the data source presents a certificate. Virtual DataPort relies on the Java Cryptography Architecture (JCA) to check if the certificate is valid. JCA accepts certificates signed by known Certificate Authorities (CA). To see the list of known CA execute the below command,

```
$cd <DENODO_HOME>/jre/bin
$keytool -list -keystore <JAVA_HOME>\lib\security\cacerts
```

However, if the certificate used by the server is signed by an authority not present in this list, you have to import this certificate into the list of trusted certificates (called TrustStore).

To import a certificate into the TrustStore of the Java Runtime Environment (JRE), execute the following commands:

```
$cd <DENODO_HOME>/jre/bin
$keytool -importcert -alias <name of the certificate> -file
<newcertificate>.crt –keystore ../lib/security/cacerts
```

This command will prompt for the password of the TrustStore, which by default is "changeit" (without the quotes).

Explanation of the parameters:

- **alias**: this parameter is mandatory. The certificate will be stored in the TrustStore identified by this alias. If the TrustStore already contains a certificate with this alias, use another alias.
- **keystore**: path to the TrustStore where the certificate will be stored. "../lib/security/cacerts" is the path of the TrustStore of the JRE included in the Denodo Platform. If you have uncommented the property com.denodo.security.ssl.trustStore of the file <DENODO HOME>/conf/vdp/VDBConfiguration.properties, the value of this parameter has to be the value of this property, instead of "../lib/security/cacerts". That is because, if this property is uncommented, Virtual DataPort will use the TrustStore set in this property of the VDBConfiguration.properties file, instead of the JRE one. If you are going to launch Virtual DataPort with a JRE not included in the Denodo Platform and the property com.denodo.security.ssl.trustStore is commented, the value of this parameter has to be the path to the cacerts file of this other JRE, which is located in the directory lib/security of the JRE.

To check that the certificate has been imported correctly, execute this command:

```
$keytool -list -v -alias <name of the certificate> -keystore
..\lib\security\cacerts
```

After adding a certificate, **the Virtual DataPort server needs to be restarted** to save the changes.