SSL Self-Signed Cert Installation

Revision 20220201

Denodo Inc.: 525 University Avenue, Suite 31, Palo Alto, CA 94301. USA www.denodo.com

Goal

This document gives a simple step-by-step walkthrough of how to configure SSL on Denodo Platform installations using a self-signed certificate.

Content

This guide assumes that the DENODO_HOME environment variable is set. All parameters within "<>" characters must be replaced.

Windows

Generate and install a self-signed SSL certificate

Generate new key pair in a key store

```
"%DENODO_HOME%\jre\bin\keytool" -genkeypair -alias self-signed -keyalg RSA -keysize 2048 -sigalg SHA1withRSA -keypass <keystore password> -keystore <keystore path *.jks> -storepass <keystore password> -storetype jks -validity 365 -ext "SAN=IP:10.100.0.1,IP:192.168.0.1,DNS:myserver.mydomain.com,DNS:otherserver.otherdomain.com"
```

Note that Subject Alternative Names are not required for JDBC or ODBC connections, but they are required by the browser when accessing the web tools of the Denodo Platform. If the web tools will be used, ensure that all the hostnames and IP addresses used to access the Denodo Platform are added into the "`SAN`" entry following the format shown above. If this is not necessary, everything including and after "`-ext`" can be removed.

Samples of valid SAN attributes:

```
SAN=IP:123.456.789.101,DNS:hostname.example.com,DNS:hostname
SAN=IP:123.456.789.101
SAN=DNS:hostname.example.com
```

Additionally, note that it is required that the keystore is in the JKS format, and that the password of the private key matches the password of the generated Keystore in order for Denodo to be able to access the key.

Export self-signed certificate

```
"%DENODO_HOME%\jre\bin\keytool" -exportcert -alias self-signed -keystore <keystore path *.jks> -storepass <keystore password> -file <self-signed certificate path *.cer>
```

Import self-signed certificate into TrustStore

```
"%DENODO_HOME%\jre\bin\keytool" -importcert -alias self-signed -file <self-signed certificate path *.cer> -keystore "%DENODO_HOME%\jre\lib\security\cacerts" -storepass changeit
```

Uncomment and change properties in these files:

%DENODO_HOME%\conf\vdp\VDBConfiguration.properties

```
com.denodo.security.ssl.enabled=true
com.denodo.security.ssl.keyStore=<client keystore path *.jks>
com.denodo.security.ssl.keyStorePassword=<client keystore password>
com.denodo.security.ssl.trustStore=%DENODO_HOME%/jre/lib/security/cacerts
```

%DENODO_HOME%\conf\vdp-admin\VDBAdminConfiguration.properties

```
com.denodo.security.ssl.trustStore=%DENODO_HOME%/jre/lib/security/cacerts
```

%DENODO_HOME%\resources\apache-tomcat\conf\tomcat.properties

```
com.denodo.tomcat.https.port=9443
com.denodo.security.ssl.enabled=true
com.denodo.security.ssl.keyStore=<client keystore path *.jks>
com.denodo.security.ssl.keyStorePassword=<client keystore password>
com.denodo.security.ssl.trustStore=%DENODO_HOME%/jre/lib/security/cacerts
com.denodo.security.ssl.trustStorePassword=changeit
```

Comment the non-SSL Connector and uncomment the SSL Connector in the file %DENODO_HOME%\resources\apache-tomcat\conf\server.xml (server.xml.template for Denodo versions previous to 6.0)

```
<!-- Define a non-SSL HTTP/1.1 Connector -->
<!--<Connector port="${com.denodo.tomcat.http.port}" … />-->

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<Connector port="${com.denodo.tomcat.https.port}" … />
```

After enabling port 9443 and disabling port 9090 the port number of the Data Catalog registered in the Solution Manager needs to be changed too. See section Creating Servers of the Solution Manager Administration guide.

Linux

Generate and install a self-signed SSL certificate

Generate new key pair in a key store

```
"$DENODO_HOME/jre/bin/keytool" -genkeypair -alias self-signed -keyalg RSA
-keysize 2048 -sigalg SHA1withRSA -keypass <keystore password -keystore
<keystore path *.jks> -storepass <keystore password> -storetype jks
-validity 365 -dname
"CN=<CommonName>,OU=<OrganizationalUnit>,O=<Organization>,L=<Locality>,ST
=<StateOrProvinceName>,C=<CountryName>" -ext
"SAN=IP:<10.100.0.1>,IP:<192.168.0.1>,DNS:<myserver.mydomain.com>,DNS:<ot
herserver.otherdomain.com>"
```

Note that Subject Alternative Names are not required for JDBC or ODBC connections, but they are required by the browser when accessing the web tools of the Denodo Platform. If the web tools will be used, ensure that all the hostnames and IP addresses used to access the Denodo Platform are added into the "`SAN`" entry following the format shown above. If this is not necessary, everything including and after "`-ext`" can be removed.

Samples of valid SAN attributes:

```
SAN=IP:123.456.789.101,DNS:hostname.example.com,DNS:hostname
SAN=IP:123.456.789.101
SAN=DNS:hostname.example.com
```

Additionally, note that it is required that the keystore is in the JKS format, and that the password of the private key matches the password of the generated Keystore in order for Denodo to be able to access the key.

Export self-signed certificate

```
"$DENODO_HOME/jre/bin/keytool" -exportcert -alias self-signed -keystore
<keystore path *.jks> -storepass <keystore password> -file <self-signed
certificate path *.cer>
```

Import self-signed certificate into TrustStore

```
"$DENODO_HOME/jre/bin/keytool" -importcert -alias self-signed -file
<self-signed certificate path *.cer> -keystore
"$DENODO_HOME/jre/lib/security/cacerts" -storepass changeit
```

Uncomment and change properties in these files:

$DENODO_HOME/conf/vdp/VDBConfiguration.properties

```
com.denodo.security.ssl.enabled=true
com.denodo.security.ssl.keyStore=<client keystore path *.jks>
com.denodo.security.ssl.keyStorePassword=<client keystore password>
com.denodo.security.ssl.trustStore=$DENODO_HOME/jre/lib/security/cacerts
```

$DENODO_HOME/conf/vdp-admin/VDBAdminConfiguration.properties

```
com.denodo.security.ssl.trustStore=$DENODO_HOME/jre/lib/security/cacerts
```

$DENODO_HOME/resources/apache-tomcat/conf/tomcat.properties

```
com.denodo.tomcat.https.port=9443
com.denodo.security.ssl.enabled=true
com.denodo.security.ssl.keyStore=<client keystore path *.jks>
com.denodo.security.ssl.keyStorePassword=<client keystore password>
com.denodo.security.ssl.trustStore=$DENODO_HOME/jre/lib/security/cacerts
com.denodo.security.ssl.trustStorePassword=changeit
```

Comment the non-SSL Connector and uncomment the SSL Connector in the file $DENODO_HOME/resources/apache-tomcat/conf/server.xml (server.xml.template for Denodo versions previous to 6.0)

```
<!-- Define a non-SSL HTTP/1.1 Connector -->
<!--<Connector port="${com.denodo.tomcat.http.port}" … />-->

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<Connector port="${com.denodo.tomcat.https.port}" … />
```

After enabling port 9443 and disabling port 9090 the port number of the Data Catalog registered in the Solution Manager needs to be changed too. See section Creating Servers of the Solution Manager Administration guide.