eServices Deployment Guide

Configuring TLS for Oracle database connections (8.5.300.12+)

12/19/2025

Contents

Configuring TLS for Oracle database connections (8.5.300.12+)

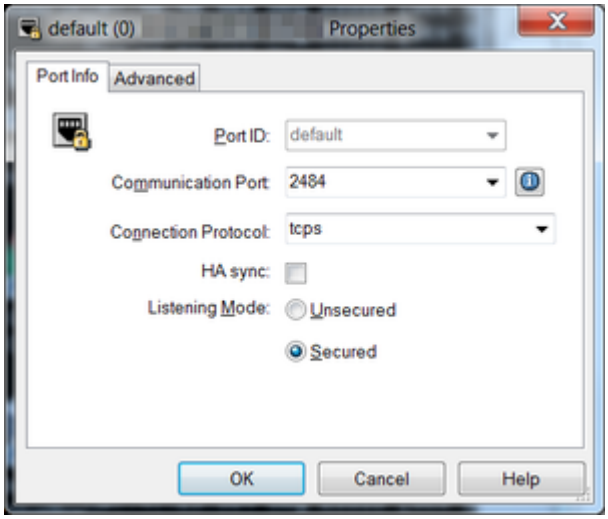
TLS configuration for UCS connecting to an Oracle database

Note that mutual TLS is not supported, only simple TLS.

Configuring UCS DAP in Configuration Server

The below procedure applies to both main and archive DAPs.

1. Stop the UCS server.
2. Open the Oracle DAP used by UCS.
3. Select the **Server Info** tab.
4. Open the port to be secured.
5. Type `tcps` in the **Connection Protocol** textbox.
6. Select Listening Mode **Secured**.
7. Click **OK.**



UCS Configuration

1. Retrieve the required certificates.
   Ask the Oracle administrator to provide the Oracle certificate chain. This may include the root CA if your certificates are self-signed.

2. Register the Oracle certificate(s) in the **truststore** file.
   Register on the UCS 8.5 server hosts (**primary** and **backup**) the chain of certificates that will be used to validate the Oracle server certificate with the Java **truststore** file. The following example uses keytool and a self-signed CA:

   ```
   keytool -import -trustcacerts -keystore /usr/lib/jvm/java-8-oracle/jre/lib/
   security/cacerts -storepass changeit -noprompt -alias "Genesys Internal CA" -file
   ~/ca-intermediate.crt
   ```

3. Configure UCS to use your **truststore** file.
   Truststore can be configured by specifying Java environment variables in **contactServer.sh** or **ContactServerDriver.ini**.

   ```
   -Djavax.net.ssl.trustStore=/usr/lib/jvm/java-8-oracle/jre/lib/security/cacerts

   -Djavax.net.ssl.trustStoreType=jks

   -Djavax.net.ssl.trustStorePassword=changeit
   ```

   You may also need to specify common cipher suites to use. Please refer to Java SSL vendor documentation for a more details.

4. Start UCS 8.5 server.