# GVP Documentation Supplement

## Configuring TLS in all RS interfaces

4/2/2026

# Contents

# Configuring TLS in all RS interfaces

SUMMARY: Add instructions for configuring TLS in all RS interfaces.

DOCUMENT: The next publication of the GVP 8.5 User's Guide will include these revisions.

CHAPTER: Chapter 14: Configuring the Reporting Server

SECTION: Configuring TLS in all RS interfaces

Add a new section title "Configuring TLS in all RS interfaces", at the end of the chapter, and add the following information to the section:

## Configuring TLS in all RS interfaces

### TLS interface between Reporting Server and GAX Plugin

For the Reporting Server-side configuration, follow these steps:

1. Generate CA file and certificate file for the Reporting Server (RS) host.
2. Convert the certificate file into JKS format by using the following command:
   ```
   openssl pkcs12 -export -in GEN-C10-039.crt -inkey GEN-C10-039.key -out GEN-C10-039.p12

   keytool -importkeystore -srckeystore GEN-C10-039.p12 -srcstoretype PKCS12 -destkeystore GEN-C10-039.jks -deststoretype JKS
   ```
3. In addition, add the CA file to the RS JKS file.
   ```
   keytool -importcert -alias cert_authority -file cert_authority.crt -keystore GEN-C10-039.jks -storepass password
   ```
4. Configure certificate and password in the **https.keystore.path** and **password** parameters in the **https** section.
5. For a simple Transport Layer Security (TLS), configure **https.client.authentication** as `none`, and for Mutual TLS, configure **https.client.authentication** as `required`.
6. Make sure the RS host application is configured only with the hostname.

For the GAX-side configuration, follow these steps:

1. Generate CA file and certificate file for the RS host.
2. Convert the certificate file into JKS format by using the following command:
   ```
   openssl pkcs12 -export -in GEN-C10-042.crt -inkey GEN-C10-042.key -out GEN-C10-042.p12

   keytool -importkeystore -srckeystore GEN-C10-042.p12 -srcstoretype PKCS12
   ```

```
-destkeystore GEN-C10-042.jks -deststoretype JKS
```

3. In addition, add the CA file to the GAX JKS file.
```
keytool -importcert -alias cert_authority -file cert_authority.crt -keystore GEN-C10-042.jks -storepass password
```
4. Add the server certificate file to the GAX JKS file.
```
keytool -importcert -alias GEN-C10-039 -file GEN-C10-039.crt -keystore GEN-C10-042.jks -storepass password
```
5. Configure certificate and password for Windows/Linux.
   - For Windows, configure certificate and password in the **setenv.bat** file:
```
set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.trustStore="C:\GEN-C10-039\GEN-C10-039.jks

set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.trustStorePassword=password
```
   - For Linux, configure certificate and password file in the **setenv.sh file**:
```
export JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=/opt/certificate/GEN-C11-192.jks

export JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStorePassword=password
```

## TLS Interface between Reporting Server and Configuration Server (Auto Detect mode)

See Configuring TLS Parameters in Configuration Manager.

For the Configuration Server-side configuration, follow these steps:

1. Configure certificate, certificate key, and trusted-ca at the port level in the Configuration Server application.
2. Set the selected port to autodetect mode.
3. For certificate, certificate-key, and trusted-ca, the file should be in PEM format (for Windows, you can use either thumbprint or PEM files).

For the Reporting Server-side configuration, follow these steps:

1. Start Reporting Server with command line parameters(provide respective certificate, CA file, and key files).
2. Ensure certificate and CA files are in JKS format.
```
java -Djavax.net.ssl.trustStore="/certificates/cacerts"
 -Djavax.net.ssl.trustStorePassword=changeit
 -Djavax.net.ssl.keyStore="/certificates/GEN-C8-233.jks"
 -Djavax.net.ssl.keyStorePassword=password -jar reporting-servlet-851.81.77.jar
 -host 172.24.130.100 -port 2040 -app "VP_ReportingServer_8"
```

## TLS Interface between Reporting Server and Configuration Server (Secure mode)

See Configuring TLS Parameters in Configuration Manager.

For the Configuration Server-side configuration, follow these steps:

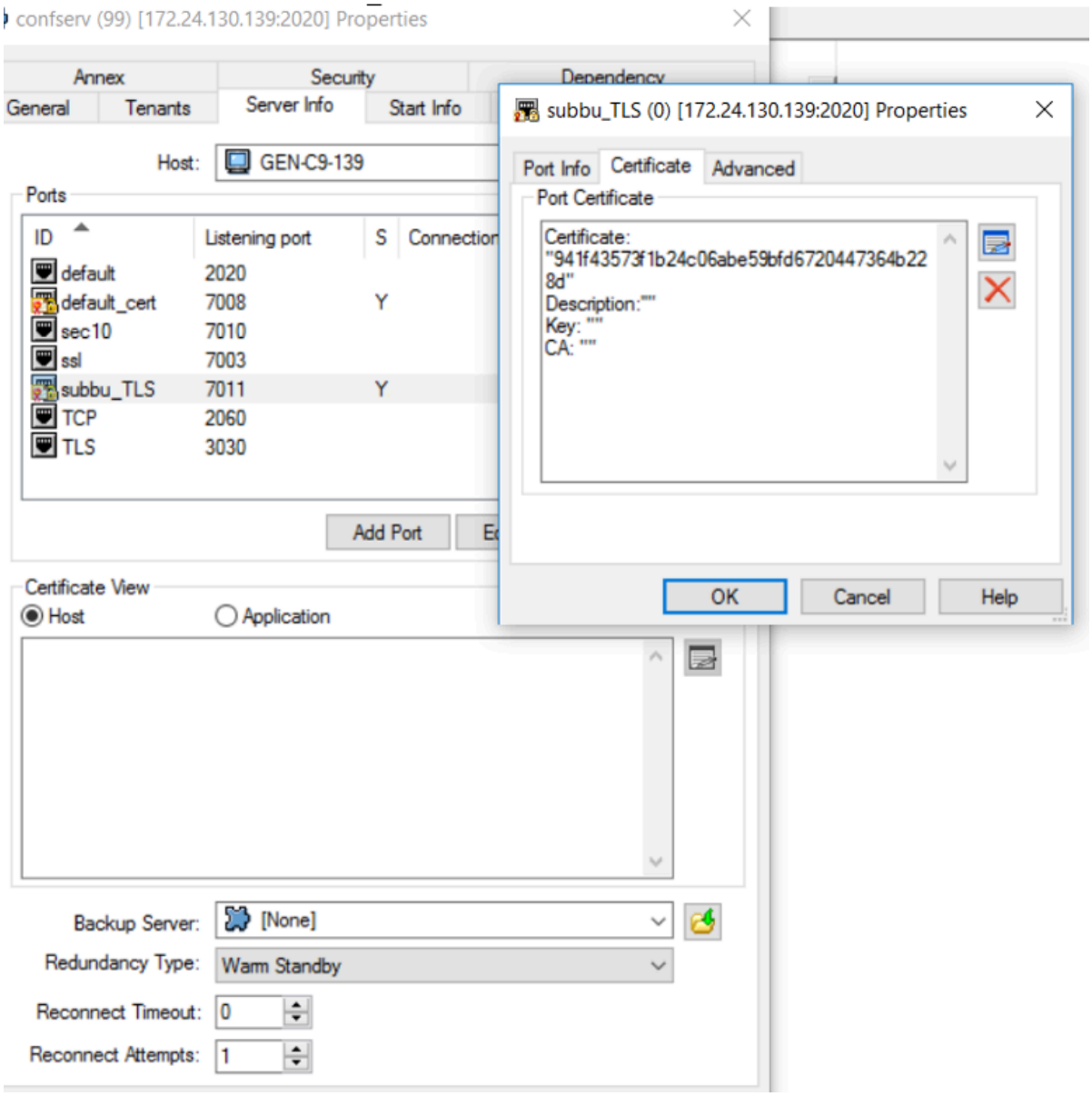
1. Configure certificate, certificate key, and trusted-ca at the port level in the Configuration Server application.
2. Set the selected port to secure mode.
3. For certificate, certificate-key, and trusted-ca, the file should be in PEM format (for Windows, you can use either thumbprint or PEM files). For example, PEM file should be configured as:

   ```
   Certificate =/opt/cert/GEN-C10-042.pem

   Certificate Key=/opt/cert/GEN-C10-042_key.pem

   Trusted CA =/opt/cert/cert_authority.pem at the port level
   ```

   For Windows, Thumbprint should be copied in certificate parameter at the port level.




For the Reporting Server-side configuration, follow these steps:

1. Start Reporting Server with command line parameters (provide respective certificate, CA file, and key files).
2. Ensure certificate and CA files are in JKS format. To connect with secured port, start RS with `-Dconfigserversecured=1`

```
java -Djavax.net.ssl.trustStore="/certificates/cacerts"
-Djavax.net.ssl.trustStorePassword=changeit
-Djavax.net.ssl.keyStore="/certificates/GEN-C8-233.jks"
-Djavax.net.ssl.keyStorePassword=password -Dconfigserversecured=1 -jar reporting-
servlet-851.81.77.jar -host 172.24.130.100 -port 2040 -app "VP_ReportingServer_8"
```

## Reporting Client to Reporting server TLS

For the Reporting Server-side configuration, follow these steps:

1. Configure **activemq.tlsKeyStore** and **password** in the **activemq.tlsKeyStore** section (ensure keystore files are in JKS format).
2. Configure the CA file and password in the **activemq.tlsTrustStore** section (ensure the file is in JKS format).
3. Configure **activemq.connectionMode=2** in the **Messaging** section to enable TLS port.

For the Reporting Client-Side Configuration (Resource Manager/Media Control Platform), follow these steps:

1. Configure certificate file in the **rc.keystore_certificate** parameter in the **ems** section (ensure the file is in pem format) and configure password in the **rc.keystore_password** parameter.
2. Configure CA file in the **rc.truststore_certificate** parameter.

## Reporting Server to Message TLS

To configuring Reporting Server to Message TLS, follow the steps in TLS Interface between Reporting Server and Configuration Server (Secure mode).

## Reporting Server with SQL Server in TLS

The following is the prerequisite information for RS – RS DB (SQL Server) TLS 1.2 Connection Support:

- Install and enable MS SQL Server to support TLS 1.2 version.
- Configure SQL Server's SSL certificate authority's certificate (CA certificate of SQLServer).
- Use JRE 1.8 to have TLS 1.2 enabled by default.

## Reporting Server connecting SQL Server with TLS Encryption

For information on Reporting Server connecting SQL Server with TLS encryption, see this vendor documentation. Follow the procedures detailed in this vendor document, replacing the code samples as follows:

For **trustServerCertificate** property in a connection string:

```
hibernate.remote.url =

jdbc:sqlserver://172.24.134.87:1433;sslProtocol=TLS;encrypt=true;trustServerCertificate=true;
```

For the **trustStore** and **trustStorePassword** properties in a connection string:

```
hibernate.remote.url =
jdbc:sqlserver://172.24.134.87:1433;sslProtocol=TLS;encrypt=true;trustServerCertificate=false;trustStore=/opt/
genesys/gvp/VP_Reporting_Server_8.5/Certificates/
cert_authority.jks;trustStorePassword=changeit
```

For the **hostNameInCertificate** property in a connection string:

```
hibernate.remote.url =
jdbc:sqlserver://172.24.134.87:1433;sslProtocol=TLS;encrypt=true;trustServerCertificate=false;trustStore=/opt/
genesys/gvp/VP_Reporting_Server_8.5/Certificates/
cert_authority.jks;trustStorePassword=changeit;hostNameInCertificate=GEN-C7-87
```

## Importing the Server Certificate to Client (Reporting Server) Trust Store

For information on importing the Server Certificate to Client (Reporting Server) Trust Store, see the section **Importing the Server Certificate to Trust Store** in this vendor documentation. After using the JAVA **keytool** utility that is installed with the JRE (as specified in the vendor documentation), create a Certificates directory on the RS installed location. For Reporting Server, the following command demonstrates how to use the **keytool** utility to import a certificate from a file:

```
keytool -importcert -alias <ca-alias-name> -keystore <keystore-filename-withpath >
-storepass <keystore-password> -file <ca-cert-filename> keytool -importcert -alias
startcassl -keystore C:\Program Files\GCTI\gvp\VP Reporting Server 8.5\
VP_ReportingServer_851\Certificates\cert_authority.jks -storepass changeit -file
cert_authority.crt
```

> **Important**
>
> GEN-C7-87 is a SQL Server Host Name.

For more details for Client connection to SQL Server, see this page.

## Reporting Server with Oracle server in TLS

To configure Reporting Server with Oracle server in TLS, follow these steps:

1. Enable TLS port in Oracle server.
2. In RS, configure hibernate.url with
   ```
   jdbc:oracle:oci:@(DESCRIPTION =(ADDRESS = (PROTOCOL = TCPS)(HOST = chi-
   uor01-s.us.int.genesyslab.com)(PORT = 1523))(CONNECT_DATA =(SERVER =
   DEDICATED)(SERVICE_NAME = db01)))
   ```
3. Start RS with the following command line parameters:
   ```
   java -Djavax.net.ssl.trustStore="C:\RS_CERTS\new\GEN-C11-190.genesys.lab.jks"
   -Djavax.net.ssl.trustStorePassword="Genesys#1"
   -Djavax.net.ssl.keyStore="C:\RS_CERTS\new\GEN-C11-190.genesys.lab.jks"
   -Djavax.net.ssl.keyStorePassword="Genesys#1" -jar reporting-servlet-900.19.56.jar
   -host 172.24.130.139 -port 2020 -app "RS_TLS_1" -Xmx1536m
   ```