GVP Documentation Supplement

Genesys Voice Platform 9.0.x

12/30/2021

Table of Contents

Supplement to Documentation for: GVP 9.0 and Media Server 9.0

This document lists additions and changes to the docs for Genesys Voice Platform 9.0.x and Media Server 9.0.x, as part of Continuous Delivery.

Latest Available IPs

The following tables document the latest IPs available for the Genesys Media Server and Genesys Voice Platform products.

Genesys Media Server

Component	9.0 available	Latest IP Version	Windows	Linux
Media Control Platform (MCP)	Y	9.0.041.92	Y	Y
Management Information Base (MIB)	Y	9.0.041.80	Y	Y
Resource Manager (RM)	Y	9.0.041.58	Y	Y
T-Server-CUCM to Media Server Connector	Y	9.0.041.02	Y	Y
GVP Reporting Plugin for GAX	Y	9.0.041.01	Y	Y
Reporting Server (RS)	Y	9.0.031.62	Y	Y

Important

See the *Genesys Supported Operating Environment Reference Guide* page for more detailed information and a list of all supported operating systems.

Genesys Voice Platform

Component	9.0 available	Latest IP Version	Windows	Linux
MRCP Proxy	Y	9.0.019.27	Y	Y
Supplementary Services Gateway (SSG)	Y	9.0.013.16	Y	Y
CTI Connector (CTIC)	Y	9.0.013.14	Y	Y
Call Control Platform (CCP)	Y	9.0.013.03	Y	Y

Component	9.0 available	Latest IP Version	Windows	Linux
Squid Caching Proxy	N	8.5.100.06	Y	N/A
Policy Server (PS)	N	8.5.010.10	Y	Y

> **Important**
>
> See the *Genesys Supported Operating Environment Reference Guide* page for more detailed information and a list of all supported operating systems.

Documentation Corrections

Document	Corrections
GVP 8.5 User's Guide	• CTIC TLS 1.2 Support • Reporting Server TLS 1.2 Support

CTIC TLS 1.2 Support

SUMMARY: Add TLS 1.2 Support information to the user guide.

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

CHAPTER: Chapter 10: Configuring the CTI Connector

SECTION: CTI Connector TLS 1.2 Support

Add a new section title "CTI Connector TLS 1.2 Support", and add the following information to the section:

CTI Connector (CTIC) supports TLS 1.2 for connection with:

- IVRServer
- Resource Manager (RM)
- Configuration Server and Message Server

TLS 1.2 is not supported for connections with Cisco ICM and LCA.

CTIC TLS 1.2 for IVRServer

CTIC supports TLS 1.2 for IVRServer. To enable TLS, set the secured parameter to true in the “IServer_Sample” section. The following TLS parameters are configured in the “IServer_Sample” section:

- **certificate**=[cert path and filename]—This parameter is mandatory for using TLS, and it denotes the path and the filename of the TLS certificate to be used.
- **key**=[key path and filename]—This denotes the path and the filename of the TLS key to be used.
- **type**=[Type of secure transport]—This denotes the type of secure transport to be used. The value can be TLSv1_2, TLSv1_1, or TLSv1. The default is TLSv1_2.
- **password**=[password]—This denotes the password associated with the certificate and key pair, and is required only if the key file is password protected.
- **cafile**=[CA cert path and filename]—This denotes the path and the filename of the certificate to be used for verifying the peer (IVRServer).
- **verifypeer**=true—This parameter turns on peer certificate verification. When enabled, CTIC verifies the IVRServer certificate with the ca certificate configured in the cafile parameter. If peer certificate verification fails, connection is not made with the IVRServer.
- **verifydepth**=[max depth for the certificate chain verification]—This parameter is applicable only to peer certificate authentication, and sets the maximum depth for the certificate chain verification.
- **Secured** = [Boolean true/false] When this parameter is set to `true`, TLS is enabled for CTIC-IVR connection. Setting this parameter to `false` disables TLS.

CTIC TLS 1.2 for RM

CTIC supports SIP over a secured transport layer from RM. CTIC supports TLSv1.2.

Example:

sip.transport2 tls:any:5081 cert=$InstallationRoot$/config/GEN-C8-232.pem key=$InstallationRoot$/config/GEN-C8-232_key.pem type=TLSv1_2 cafile=$InstallationRoot$/config/cert_authority.pem

`sip.transport.<n>`—This parameter defines how TLS is enabled in the SIP stack.

`type:ip:port`

where:

- **type** must be set to tls.
- **ip** is the IP address of the network interface that accepts incoming SIP messages. If ip is an IPv6 address, [] must be used. For example:
- To define a transport to listen to all IPv4 interfaces, set the value of ip to any or any4.
- To define a transport to listen to all IPv6 interfaces, set the value of ip to [any6].
- port is the port number where the SIP stack accepts incoming SIP messages.

`[parameters]` defines SIPS-TLS transport parameters. For example:

- **cert**=[cert path and filename]—This parameter is applicable to SIPS only and mandatory if using SIPS, and denotes the path and the filename of the TLS certificate to be used.
- **key**=[key path and filename]—This parameter is applicable to SIPS only and mandatory if using SIPS, and denotes the path and the filename of the TLS key to be used.
- **type**=[Type of secure transport]—This parameter is applicable to SIPS only and is optional. This denotes the type of secure transport to be used and the value can be TLSv1_2, TLSv1_1, TLSv1, SSLv3, or SSLv23. Default is TLSv1_2.
- **password**=[password]—This is applicable to SIPS only and is optional, and denotes the password associated with the certificate and key pair. This is required only if key file is password protected.
- **cafile**=[CA cert path and filename]—Mandatory for TLS mutual authentication. This denotes the path and the filename of the certificate to be used for verifying the peer.
- **verifypeer**=true—This parameter is mandatory for TLS mutual authentication, and turns on the TLS mutual authentication.
- **verifydepth**=[max depth for the certificate chain verification]—This parameter is applicable only to TLS mutual authentication, and sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

CTIC TLS 1.2 for Configuration Server and Message Server

CTIC supports TLS connection to Configuration Server and Message Server through secure ports exposed by Configuration Server.

Reporting Server TLS 1.2 Support

SUMMARY: Add TLS 1.2 Support information to the user guide.

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

CHAPTER: Chapter 14: Configuring the Reporting Server

SECTION: Reporting Server TLS 1.2 Support

Add a new section title "Reporting Server TLS 1.2 Support", and add the following information to the section:

TLS 1.2 MS SQL Server

Support of TLS 1.2 Connection between RS and RS Database (**MS SQL Server**) is validated for VP Reporting Server. The purpose of this section is to describe a simple configuration and environment setup.

The overall objective for supporting TLS 1.2 Connection for Reporting Server and Reporting Server database (MS SQL Server).

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.
- 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 RS installed location and then execute the following queries:

Windows:

```
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.

More details on Client connection to SQL Server are available at Microsoft JDBC Driver for SQL Server.

TLS 1.2 Support (Oracle)

Support of TLS 1.2 Connection between RS and RS Database (**Oracle**) is validated for VP Reporting Server. The purpose of this section is to describe a simple configuration and environment setup.

The overall objective is to support TLS 1.2 Connection for Reporting Server and Reporting Server database (Oracle).

Prerequisite information for RS – RS DB (Oracle) TLS 1.2 Connection Support

- Install and enable Oracle to support TLS 1.2 version.
- Oracle SSL certificate authority's certificate (CA certificate of Oracle).
- Use JRE 1.8 to have TLS 1.2 enabled.

Reporting Server Connecting Oracle with TLS Encryption

Set the following system properties and use the below connection string in "hibernate.remote.url" for connecting with Oracle in TLS 1.2:

- javax.net.ssl.trustStore
- javax.net.ssl.trustStoreType
- javax.net.ssl.trustStorePassword

```
hibernate.remote.url =
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=servername)(PORT=2484))(CONNECT_DAT
```

Reporting Server TLS 1.2 Support for HTTPS

Refer to the "Enabling HTTPS for Reporting" section of the GVP 8.5 User's Guide.

Reporting Server TLS 1.2 Support for Configuration Server and Message Server

RS supports TLS connection to Configuration Server and Message Server through secure ports exposed by the Configuration Server.

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:

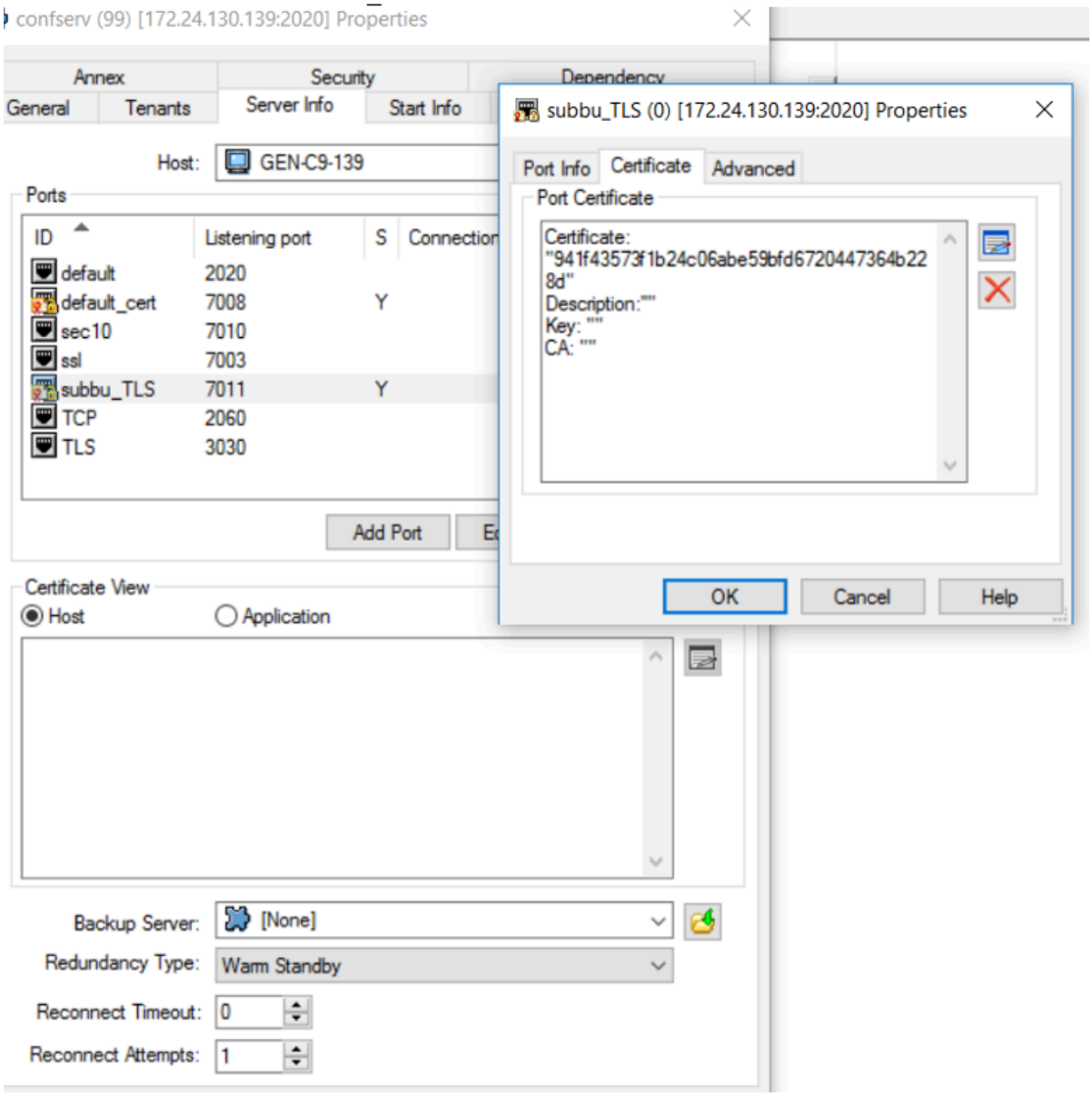
1. Configure certificate, certificate key, and trusted-ca at the port level in the Configuration Server application.
2. Set the selected port to secure mode.
3. For certificate, certificate-key, and trusted-ca, the file should be in PEM format (for Windows, you can use either thumbprint or PEM files).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

Configuring SSG TLS Interface

SUMMARY: Add steps for configuring the Supplementary Services Gateway (SSG) TLS interface.

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

CHAPTER: Chapter 11: Configuring the Supplementary Services Gateway

SECTION: Configuring SSG TLS Interface

Add a new section title "Configuring SSG TLS Interface", at the end of the chapter, and add the following information to the section:

Configuring SSG TLS Interface

> **Important**
> The information in this section pertains only to the configuration that is done via Configuration Management Environment. Genesys Administrator (GA) users must configure the corresponding parameters via GA.

SSG to Configuration Server in TLS

For information on how to enable TLS in Configuration Server, see Genesys Security Deployment Guide.

In SSG, perform these steps:

1. You can configure certificates at any level (Host level, Application level, or Connection level).
   Linux
   - Host level: In the Host object on which client is running, in the **Network Security** section of the **Configuration** tab, do the following:

   1. Enter the absolute path to the Trusted CA in the corresponding field.
   2. If you are configuring Mutual TLS, enter the absolute path to the certificate in the corresponding field.
   3. In the Client Application object, in the **Network Security** section of the **Configuration** tab, select Host in the **Certificate Source** field.

   - Application level: In the Server Application object, in the **Network Security** section of the **Configuration** tab, do the following:

1. Select Application in the **Certificate Source** field.
2. Enter the absolute path to the Trusted CA in the corresponding field.
3. If you are configuring Mutual TLS, enter the absolute path to the certificate in the corresponding field.

- Connection level: In the **Network Security** tab of the **Connection Info** window, do the following:

1. Enter the absolute path to the Trusted CA in the corresponding field.
2. If you are configuring Mutual TLS, enter the absolute path to the certificate in the corresponding field.

WINDOWS:

- Host level: In the Host object on which the client Application is running, in the **Network Security** section of the **Configuration** tab, do the following:

1. Enter the thumbprint of the certificate, in the **Certificate** field.
2. In the client Application object, in the **Network Security** section of the **Configuration** tab, select **Host** in the **Certificate Source** field.

- Application level: In the client Application object, in the **Network Security** section of the **Configuration** tab, do the following:

1. Select Application in the **Certificate Source** field.
2. Enter the thumbprint of the certificate, in the **Certificate** field.

- Connection level: In the **Network Security** tab of the **Connection Info** window, enter the thumbprint of the certificate, in the **Certificate** field

SSG to Message Server in TLS

In SSG, perform these steps:

1. Add the Message server in the Connection tab of SSG.
2. Configure client certificate as follows:

   Linux (Connection level): In the **Network Security** tab of the **Connection Info** window, do the following:

   1. Enter the absolute path to the Trusted CA in the corresponding field.
   2. If you are configuring Mutual TLS, enter the absolute path to the certificate in the corresponding field.
   3. Add TLS=1 in the **Transport Parameters** field of the **Advanced** tab.

   Windows (Connection level): In the **Network Security** tab of the **Connection Info** window, do the following:

   1. Enter the thumbprint of the certificate, in the **Certificate** field.
   2. Add TLS=1 in the **Transport Parameters** field of the **Advanced** tab.

SSG to SIP Server in TLS

In SIP Server, perform these steps:

1. Open **Server Info Configuration** tab of the SIP Server Application object, and select the **Add Port** field. The **Port Info** window opens.
2. In the **General** tab, select **Secured** in the **Select Listening Mode** field. This automatically enters TLS=1 in the **Transport Parameters** field of the **Advanced** tab.
3. If you are setting up Mutual TLS, also add tls-mutual=1 to the **Transport Parameters** field. All parameters in this field must be separated by semi-colons (;).
4. In the **Certificate** tab, configure certificate and CA files in the appropriate fields. For Windows, configure thumbprints.

In SSG, perform these steps:

1. Add the Sip Server with secured port in the **Connection** tab of SSG.
2. At the connection level in the **Certificate** tab, configure certificate and CA files in the appropriate fields. For Windows, configure thumbprints.
3. You can configure certificate at the application/host level similar to SSG to Configuration Server in TLS.

SSG to HTTPS notification URL (FM module)/HTTPS Client

In Webserver, perform these steps:

1. Install Certificate and CA file in the MMC console.
2. In the Server home page, double-click Server certificates, and check whether your imported certificates are listed here. Otherwise, create the certificate.
3. Add https as the binding type, and assign the IP address and port to use.
4. And in the Site page, in SSL setting, select the **Require SSL** check box and also accept the client certificate.

In SSG, configure the following certificate parameters in the FM module:

- ssl_ca_info
- ssl_cert and ssl_cert_type
- ssl_key and ssl _key_type
- ssl_version
- ssl_verify_host

Enabling HTTPS for SSG landing page/HTTPS Server

In SSG, configure the following certificate parameters in the HTTP section:

- CertFile

- CertKeyFile
- HTTPSPort
- TLStype

GVP GAX Plugin DID bulk creation feature

SUMMARY: Add GVP GAX Plugin DID bulk creation feature information to the user guide.

DOCUMENT: The next publication of the GVP 9.0 User's Guide will include these revisions.

CHAPTER: Chapter 16: Reporting Overview

SECTION: DID Bulk Operations Dialog

Add a new section title "DID Bulk Operations Dialog" after the "GAX Report Generation Table" section, and add the following information to the section:

DID Bulk Operations Dialog

Now Tenant Administrators can provision DIDs to DID Groups using DID Bulk Operations dialog. The implementation provides a GUI interface so a GAX user can create, edit, or delete Bulk DIDs in DID Groups. This functionality uses validation and overlap checking across multiple tenants to ensure that there are no duplicate DIDs.

To use the DID Bulk Operations feature, Tenant Administrators need the privilege PRIVILEGE_DID_GROUP_SERVICE. They can use if they have also have these privileges:

- To access Configuration Manager: ACCESS_CONFIGMANAGER
- The GAX user should be a Tenant administrator and have "GVP DID Groups Access" Privilege (Configuration -> Roles: Home -> Roles -> <Role> -> Assigned Privileges -> gvp-rpt -> GVP DID Groups Access.)
- **DID Bulk Operations dialog** should only be performed by users with read access into all tenants. Otherwise, DID uniqueness cannot be ensured and this may lead to problems during call processing.
- Users who do not have this Privilege "GVP DID Groups Access" (Configuration -> Roles: Home -> Roles -> <Role> -> Assigned Privileges -> gvp-rpt -> GVP DID Groups Access) and no read access into all tenants those will not be updated the DIDs.

The DID Bulk Operations dialog allows you to add, delete, and move multiple DIDs among DID groups. You can also create new DID groups with the dialog. The following procedure describes how to use the DID Bulk Operations dialog.

Using the DID Bulk Operations dialog

Purpose: To add, delete, and move DIDs using the DID Bulk Operations dialog.

Prerequisites

- The IVR Profiles have been created.

For more information about creating an IVR Profile, see the chapter about post-installation activities in the Genesys Voice Platform 8.5 Deployment Guide. For more information about configuring the IVR Profile, see “IVR Profile Configuration Options” in the Genesys Voice Platform 8.5 User’s Guide.

- You are logged in to Genesys Administrator Extension. To access Genesys Administrator Extension, go to the following URL:
  http://<Genesys Administrator Extension host>/<port>/gax/

Start of procedure

1. Go to the Configuration > DID Groups.
2. Optionally, select the DID Group you want to change.
3. In the Tasks panel, click DID Bulk Operations to invoke the dialog.
4. Select the appropriate operation.
5. After selecting the appropriate Operation Selection, CSV File and Uploaded CSV file has column header Options. Click Upload to start the Uploading the file to the server for Validating each DID at server for errors and overlap.
6. After reviewing the results click Apply for saving the DIDs.
    1. Select Add to add multiple DIDs to the selected group, or to create new DID groups, then select Next option.
        1. Click Browse to select the CSV file containing the list of new DIDs.
           The uploaded file must be a CSV file with the following columns (in the given order):
           - DID
           - DID Group
           - Tenant

           A DID is either a single DID (in the form <did>), a range of DIDs (in the form <start>-<end>) or a DID prefix (in the form <prefix>*). Lines of text that don’t match these patterns are considered invalid.

           A DID Group is the name of either an existing group or a new group that is to be created. This column is optional and defaults to the selected DID Group (if one was selected during the launching of the wizard).

           A Tenant is the name of the tenant that owns (or will own) the specified DID Group. This column is optional and defaults to the current tenant.

           Because DID Group and Tenant columns are optional, a flat list of DIDs can be uploaded (instead of a CSV) for addition/moving into of DIDs into the selected (in the DID group list) DID group.
        2. Click Upload.
        3. Review the Results section in screen for a summarization of the operation.
           The summary includes the counts for invalid DIDs, valid DIDs, and DIDs that currently belong to other DID Groups.
        4. Click Apply.
    2. Select Move to move the specified DIDs to a selected group, then select Next option.

1. Click Browse to select the CSV file containing the list of new DIDs.
   The uploaded file must be a CSV file with the following columns (in the given order):

   - DID
   - DID Group
   - Tenant

   A DID is either a single DID (in the form <did>), a range of DIDs (in the form <start>-<end>) or a DID prefix (in the form <prefix>*). Lines of text that don't match these patterns are considered invalid.

   A DID Group is the name of either an existing group or a new group that is to be created. This column is optional and defaults to the selected DID Group (if one was selected during the launching of the wizard).

   A Tenant is the name of the tenant that owns (or will own) the specified DID Group. This column is optional and defaults to the current tenant.
2. Click Upload.
3. Review the Results section in screen for a summarization of the operation.
   The summary includes the counts for invalid DIDs, valid DIDs, and DIDs that currently belong to other DID Groups.
4. Click Apply.

3. Select Delete to remove the specified DIDs from the selected group, then select Next option.

1. Click Browse to select the CSV file containing the list of new DIDs.
   The file must be a CSV file containing a list of DID numbers. Each line is either a single DID (for example, 100), a range of DIDs (for example, 100-199), or a DID prefix (for example,100*). Lines of text that do not match these patterns are ignored.
2. Click Upload.
3. Review the Results section in screen for a summarization of the operation.
   The summary includes the counts for invalid DIDs, valid DIDs, and DIDs that currently belong to other DID Groups.
4. Click Apply.
   You can download these generated CSV files for diagnostic or auditing purposes.

Service Quality (SQ) Reporting - Default Thresholds

SUMMARY: Default values listed in the GVP User's Guide are incorrect and they should match those contained in the XML data included in the VP Reporting Server IP (installation package).

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

CHAPTER: Chapter 3: Configuring Common Features

SECTION: Table 7: Service Quality Advisor Parameters

Update the default values of the following configuration options in Table 7:

Option Name - First Prompt Inbound Latency Threshold
Description - Specifies the maximum threshold, in milliseconds, before playing a prompt on an inbound call.
Valid Values and Syntax - Default value: `2000|95`

Option Name - Cumulative Response Latency Threshold
Description - Specifies the maximum threshold, in milliseconds, before playing a prompt after customer iteraction.
Valid Values and Syntax - Default value: `2000|95`

Option Name - Call Reject Latency Threshold
Description - Specifies the maximum time, in milliseconds, to determine whether the call reject latency is considered a failure because it falls below the threshold.
Valid Values and Syntax - Default value: `2000|95`

Option Name - Call Answer Latency Threshold
Description - Specifies the maximum time, in milliseconds, to determine whether the call answer latency is considered a failure because it falls below the threshold.
Valid Values and Syntax - Default value: `2000|95`