GVP Documentation Supplement

Configuring SSG TLS Interface

4/4/2026

Contents

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