Genesys Interaction Recording Solution Guide

Secure Transport Configuration

4/2/2025

Contents

Secure Transport Configuration

This section describes how to configure Transport Layer Security (TLS) for the Genesys Interaction Recording solution.

Server-Side Configuration

The following components must configure secure transports for HTTP.

Interaction Recording Web Services

Configuring TLS for Interaction Recording Web Services

See Configuring TLS on the Server Side for Interaction Recording Web Services.

Configuring TLS for the Recording Processor Script

1. Configure HTTPS on the primary recording server. For more information, see the "Configure SSL" section of Configuring Recording Processor Script.
   a. For Windows, make sure the pyOpenSSL is installed. pyOpenSSL is already be installed on RHEL6.
   b. Create a self-signed certificate and private key for the Recording Processor host. For example, on Ubuntu run:

      ```
      openssl req -new -x509 -days 1024 -nodes -out cert228.pem -keyout cert228key.pem
      ```

   c. In the `rp_server` section of the Recording Processor's configuration file, set the following parameters:
      - `ssl_certificate`—Point to the certificate PEM file. For example, `ssl_certificate=cert228.pem`.
      - `ssl_private_key`—To point to the private key file. For example, `cert228.pem`.
   d. Send the self-signed certificate PEM file to any MCP client that needs to validate the certificate during the SSL handshake. See the "Enable Secure Communication" section of the GVP 8.5 User's Guide.
   e. Restart Recording Processor.
2. Configure HTTPS on the backup recording server by following the same instructions as above using a new certificate and private key.

Configuring TLS for the Voice Processor

See Voice Processor Service Level Configuration.

Configuring TLS for the Recording Crypto Server

See Configure HTTP Port tab in the Configuring Recording Crypto Server section.

Configuring TLS for the WebDAV Server

See Configuring TLS for the WebDAV Server.

Configuring TLS for the Interaction Receiver and SpeechMiner UI Server

See Enabling HTTPS for SpeechMiner.

Configuring TLS for the HTTP Load Balancer

See Configuring TLS for the HTTP Load Balancer in a single-tenant environment.
See Configuring TLS for the HTTP Load Balancer in a multi-tenant environment.

Client-Side Configuration

Configuring TLS for the Media Control Platform (MCP)

To add a Certificate Authority (CA):

1. Place the CA file on the MCP.
2. Using Genesys Administrator or Genesys Administrator Extension, in the **[fm]** section set the **ssl_ca_info** option to the location of the CA file.
3. Restart MCP.

To add client-side authentication:

1. Place the certificate file (PEM format) on the MCP.
2. Using Genesys Administrator or Genesys Administrator Extension, in the **[fm]** section set the **ssl_cert** option to the location of the certification file.
3. Restart MCP.

For more information about the MCP options, see the Voice Platform Media Control Platform Configuration Options.

Configuring TLS for the IVR Profile

Using Genesys Administrator Extension, navigate to the `Recording` tab of the IVR Profile. Update the following addresses with the HTTPS locations:

- Storage Destination
- Recording Processor URI

- SpeechMiner Interaction Receiver
- SpeechMiner Destination for Analytics only

Configuring TLS for the Recording Processor Script

The Recording Processor Script creates three client connections, to:

- Interaction Recording Web Services (Web Services)
- SpeechMiner Interaction Receiver
- Backup Recording Processor Script

For details on configuring each connection, refer to the appropriate section at the Configure SSL link on the page Deploying Recording Processor Script.

Configuring TLS for the Voice Processor

The Voice Processor creates three client connections, to:

- Interaction Recording Web Services (Web Services)
- SpeechMiner Interaction Receiver
- Genesys Info Mart

For details on configuring these connections, see Configuring Voice Processor.

Configuring TLS for Interaction Recording Web Services

Interaction Recording Web Services (RWS) may be configured to use secure connections to the following components:

- Configuration Server
- SIP Server
- Interaction Server
- WebDAV
- Recording Crypto Server
- SpeechMiner Interaction Receiver
- Cassandra

For details on configuring each connection using TLS, refer to the appropriate section in Configuring Security.

Configuring TLS for the Recording Muxer Script

The Recording Muxer Script creates client connections to the following:

- Interaction Recording Web Services
- Recording Crypto Server (if the recordings are encrypted)
- WebDAV

For details on configuring each connection using TLS, refer to the appropriate section in Configuring Transport Layer Security (TLS) Connections.

Configuring TLS for the Recording Crypto Server

The Recording Crypto Server creates client connections to the following:

- Interaction Recording Web Services
- SpeechMiner Interaction Receiver
- Message Server
- Configuration Server

For details on configuring each connection using TLS, refer to the appropriate section in Configuring Transport Layer Security (TLS) Connections.

Configuring TLS for the Recording Plug-in for GAX

See Configuring Transport Layer Security.