Genesys Security Deployment Guide

Securing Core Framework Connections

5/2/2025

Contents

Securing Core Framework Connections

This page contains information about securing connections between core Genesys servers, including Configuration Server, and Genesys clients. It also provides instructions for automatically securing a connection with Configuration Server when a client starts up.

Configuring TLS on Genesys Servers

For all server applications, configure a new or existing server port for secure connections. A port must be secure before you can configure a secure connection to that port.

Server-type applications that support Genesys TLS also support multiple server ports. This enables you to set up secure communications on only those connections for which security is considered necessary, rather than all server connections at the same time.

> **Tip**
>
> - If you intend to use the secure data exchange capabilities on connections to a specific server, Genesys recommends that you configure a new port for such secure connections, and that you leave the existing port intact for connections that do not require security .while protecting that port using network security.
> - If you want to use mutual TLS, set the **tls-mutual** configuration option to 1 .on the server side, at the same level (host, application, port) as your certificate.

Configuring TLS on Configuration Server

To configure TLS on Configuration Server, do the following:

1. In the Configuration Server Application object, configure an Auto-Detect port to enable clients to connect securely to Configuration Server.
2. If you want to use mutual TLS, set the **tls-mutual** option to 1 at the Auto-Detect port level.
3. Assign a certificate to be used by Configuration Server at the Auto-Detect port level.

Configuring TLS on Other Genesys Servers

To configure a secure port on a TLS server application, do the following:

1. In Genesys Administrator, click the **Provisioning** tab and navigate to the folder containing the server

application.

2. Select the server application and click the **Configuration** tab.
3. In the **Server Info** section, click **Add** in the **Listening Ports** table. The **Port Info** dialog box appears.
4. In the **Port Info** dialog box, on the **General** tab:
   - In the **ID** box, enter the port ID.
   - In the **Port** box, enter the number of the new port.
   - In the **Connection Protocol** box, select the connection protocol, if necessary.
   - In the **Select Listening Mode** box, select **Secured**.
   - Click **OK**.
5. Click **Save** to save the new configuration.
6. Assign a certificate to be used by this server. Genesys recommends that you assign the certificate on the host level, but you can assign it at the application level or port level if required.
7. If you want to use mutual TLS, set the **tls-mutual** option to 1 at the same level as the certificate you assigned to the server in the previous step.

Configuring TLS on Genesys Clients

After you configure your server applications so that they have secure ports, you must change the configuration of your client applications, so that they connect to these ports. Remember that you must do this only for the connections on which extra measures are necessary to protect the data that is transferred between the Genesys applications.

Configuring a Secure Bootstrap Connection to Configuration Server

Client applications must be provisioned with their secure connection parameters at application or host level when connecting to auto-upgrade port of configuration server. Configuration Server validate client configuration and send it to client application as a part of auto-upgrade procedure. Client apply receivied parameters. To configure a secure bootstrap connection to Configuration Server, follow the appropriate procedure based on the type of client application.

Server Applications

Prerequisite:

- A trusted CA certificate is configured and accessible by the client application.

Procedure:

1. Verify that the command-line parameters in the initial startup **.bat** or **.sh** file (if it exists) are set to connect to the Autodetect port.

2. In the configuration of the client server Application object, do the following:
    a. Configure a connection to the Autodetect port of Configuration Server.
    b. If mutual TLS (**tls-mutual=1**) is configured on the server side, obtain a client certificate and configure it accordingly.
3. If you need to install a new instance of the client application, use the appropriate Installation Package and provide the Application object you just configured.
4. Start the client server application using Solution Control Server and/or a startup batch file, if applicable.

User Interface Applications

For User Interface applications that utilize a login requiring host and port information, do the following:

Prerequisite:

- A trusted CA certificate is configured and accessible by the client application.

Procedure:

1. In the configuration of the client server Application object, do the following:
    a. Configure a connection to the Autodetect port of Configuration Server.
    b. If mutual TLS (**tls-mutual=1**) is configured on the server side, obtain a client certificate and configure it accordingly.
2. If you need to install a new instance of the client application, use the appropriate Installation Package and provide the Application object you just configured.
3. Start the client application by entering the Configuration Server Autodetect port in the login dialog box.

Configuring a Secure Client Connection to Other Genesys Servers

To configure a secure connection of a client application to other Genesys servers, do the following:

1. Click the **Configuration** tab of the client application.
2. Select a server to which you need to make a secure connection, and click **Edit**.
3. In the **Connection** table in the **General** section, click **Add**, and enter the properties of the secure port that you created for the server during the previous configuration steps. The read-only **Connection Type** property indicates that this connection is secure.
4. If you are configuring mutual TLS, assign the certificate, private key, and Trusted CA to this application.
5. Click **OK**.
6. Click **Save** to save the new connection configuration.

The next time this application starts, it will connect to the server over a secure connection.