Genesys Info Mart Deployment Guide

Enabling Secure Connections

4/24/2025

Enabling Secure Connections

The following steps summarize the task flow to enable Genesys Info Mart to implement the features that Genesys provides to secure connections in the deployment. All of the security features are optional.

1. **Enable the** Transport Layer Security (TLS) **protocol on the connections from Genesys Info Mart Server to Configuration Server and Message Server.**

   a. (For UNIX-based deployments only) Install the Genesys Security Pack on the Genesys Info Mart Server host, and set the applicable environment variable to specify the path to the Security Pack libraries. For more details, see the information about Installing Genesys Security Pack in the *Genesys Security Deployment Guide.*

   b. If certificates do not already exist, create and install certificates on the Genesys Info Mart Server host, as well as on the Configuration Server and Message Server hosts. Genesys Info Mart supports mutual TLS, which requires exchange of certificates from both the TLS Server and the TLS Client. For more details, see the information about installing and generating certificates and about Securing Connections Using TLS in the *Genesys Security Deployment Guide.*

      To enable TLS 1.2, ensure that you use versions of the applications that support the protocol (see TLS Protocol Support) and that you modify the transport protocol parameters to specify the **sec-protocol** option (`sec-protocol=TLSv12`).

   c. If necessary, modify the configurations of the Configuration Server and Message Server applications to:

      i. Add a new port for secure connections. On the Configuration Server and Message Server Application objects, select the **Secured** mode.

      ii. Use a host certificate.

      For full details, see Securing Core Framework Connections and other pages about TLS configuration in the *Genesys Security Deployment Guide*.

   d. On the Genesys Info Mart Application object, add connections to Configuration Server and Message Server (as described for the Connections tab in Creating the Genesys Info Mart application). When you add the connection(s), ensure that you specify the port that you created for secure connections.

2. **Enable compliance with** Federal Information Processing Standards (FIPS)**.**
   Genesys Info Mart support for TLS complies with FIPS, but there are additional steps to enable FIPS mode. For details about setting up your Java environment to be compliant with FIPS, see the information about enabling FIPS in a Genesys Java environment in the *Genesys Security Deployment Guide*.

3. **Enable client-side port definition for the connection from Genesys Info Mart Server to Configuration Server.**

   a. When you install Genesys Info Mart, specify the connection parameters that Genesys Info Mart will use for the initial connection to Configuration Server.

   b. In the Genesys Info Mart Application object, add or modify the connection to Configuration Server, to specify the connection parameters (port number and, optionally, IP address) that Genesys Info Mart will use to reconnect to Configuration Server after a switchover or disconnection. You configure the parameters in the **Transport Parameters** text box on the **Advanced** tab of the connection properties.

      For full details, see the information about client-side port definition in the *Genesys Security Deployment Guide*.

4. **Enable client-side port definition for the connection from Genesys Info Mart Server to Message Server.**

   In the Genesys Info Mart Application object, add or modify the connection to Message Server, to specify the connection parameters (port number and, optionally, IP address) that Genesys Info Mart will use. You configure the parameters in the **Transport Parameters** text box on the **Advanced** tab of the connection properties.

   For full details, see the information about client-side port definition in the *Genesys Security Deployment Guide*.

5. **Enable use of the Secure Socket Layer (SSL) protocol on the JDBC connections between Genesys Info Mart Server and its source and target databases.**

   Create the certificates and configure the RDBMS server and client as described in your RDBMS vendor documentation for Java clients, including JVM startup parameters. See also the Environment Settings information in the *Framework Database Connectivity Reference Guide.*

   When you configure the extraction DAP(s) and the Info Mart DAP, use the jdbc-url option to specify the URL information as required by your RDBMS to implement JDBC over SSL. See the extended description of the **jdbc-url** option for examples of the syntax to use.

   For more information about configuring the **jdbc-url** option, see Configuring a JDBC extraction DAP or Configuring a non-JDBC extraction DAP. For more information about the parameters that you must specify, see your RDBMS vendor documentation.

6. **In deployments that rely on obtaining reporting data from Kafka, enable a secure client connection from Genesys Info Mart to the Kafka instance.**
   Starting with release 8.5.014.19, you can set native Kafka configuration options in the **kafka-<cluster-name>** configuration section to enable secure client connections. In particular, see kafka-<cluster-name> Section in the *Genesys Info Mart Options Reference* for security options you should consider for a Kafka cluster that uses SASL_SSL authentication or if you are using SSL connections with a self-signed certificate.