Genesys Security Deployment Guide

Secure Connections (TLS)

5/7/2025

Contents

Secure Connections (TLS)

Genesys products handle consumer data for customers in sensitive and regulated industries (banking, insurance, retail, government, and so on). In many cases, this data should be protected while being transmitted via network media. Such protection can be implemented for connections that are established across public networks, as well as corporate internal networks.

This section of the Genesys Security Deployment Guide is intended to present a user-level guide on how to utilize the Transport Layer Security (TLS) protocol to secure network connections in a Genesys deployment, both between Genesys components or between Genesys components and 3rd-party software. It is intended to be a complete source of information on how to configure secure connections.

Security Benefits

TLS provides strong authentication, message confidentiality, and integrity capabilities. TLS secures data transmission by using a variety of encryption options. TLS can authenticate one or both parties engaged in secure communication. It also provides data integrity through an integrity check value. In addition to protecting against data disclosure, the TLS protocol can be used to help protect against masquerade attacks, man-in-the-middle attacks, bucket brigade attacks, rollback attacks, and replay attacks. TLS, as implemented by Genesys, is in most cases considered to be consistent with Federal Information Processing Standards (FIPS).

Securing Connections – An Overview

Securing connections in an existing Genesys environment should be done iteratively. The following is a high-level summary of how to accomplish this.

1. Enumerate all connections that are to be secured. Then categorize those connections based on the following parameters:
   - Whether the connection is between Genesys components or a Genesys component and a 3rd-party component, and which Genesys components are linked by the connection.
   - The payload data protocol used, namely TLib, a Genesys internal protocol, or an application data protocol (such as SIP).
   - The types of operating systems used by the connection peers, namely Windows or *nix (Linux, AIX, Solaris).
   - Details of the connection peer implementation, such as a Java application, a Web application, a C++ application based on a common library, and so on.
2. Having identified and categorized the connection, do the following:
   a. Generate the entities required to secure the connection. Note that this is the minimum required, your implementation may require more.

- For the certificate presenter:
  - A certificate (or certificate chain), which represents the entity presenting it; typically digitally signed by a CA and set with an expiration date. This is not required on the client side of a simple TLS connection.
  - A private key, generated with the certificate as part of a public/private key pair. This is also not required on the client side of a simple TLS connection.
- For the receiver of the certificate:
  - A certificate list of the trusted CAs, including the CA that signed the certificate to be received.

b. Install the certificates on the host where the component is running.

c. Use Genesys Administrator to configure the certificates.

d. If running in the *nix environment, configure an environment variable to point to the security libraries.

e. For third-party components, determine the source of the certificates (such as a Java keystore, an Oracle `cacerts` file, web servers for https connections, and so on) and then configure them appropriately.

About this Section

This section of the Security Guide describes how to secure connections using TLS, and is intended to be a structured source of information. It describes how to secure certain types of connections that have been identified in the deployment and categorized as described above. Decisions on whether to protect or not to secure a connection are outside the scope of this guide.

A complex Genesys deployment can have many different network connections, utilizing many types of payload protocols. Most of these connections are configured in (almost) the same way. Some connections require specific details in their security configuration. Because it is impossible to describe every type of connection between every type of Genesys component, this guide is organized as follows. All information is divided into general sections, corresponding to general types of connections. Inside each general section, subsections describe specific connections of that category of connection type.

Before starting, note the following:

- The instructions in this document assume that you are adding Genesys Transport Layer Security (TLS) to existing connections of your Genesys 8.x environment—that is, that your applications have already been installed, properly configured, and associated with hosts and with each other. For information about configuring new hosts, applications, and associations between them, see the *Framework Deployment Guide*.
- If you are using pre-8.x Genesys components, you must upgrade them to release 8.x before you can configure secure connections between them.
- Some components require additional steps to complete the configuration of secure connections. These steps are provided in the Deployment Guide for the particular product or component.