Genesys Security Deployment Guide

Introduction to Genesys Transport Layer Security

4/30/2025

Introduction to Genesys Transport Layer Security

Contents

Genesys supports the optional use of the Transport Layer Security (TLS) protocol to secure data exchange between its components. TLS is an industry-standard protocol for secure communications on the Internet, and it is the successor of Secure Sockets Layer (SSL) 3.0.

Security Benefits

TLS provides strong authentication, message privacy, and integrity capabilities. TLS secures data transmission by using a variety of encryption options. TLS authenticates servers to prove the identities of the 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 considered to be compliant with Federal Information Processing Standards (FIPS).

Supporting Components

This section lists the Genesys components that currently support TLS and on what connections. For detailed information about TLS support by Genesys components, see the corresponding product documentation.

[+] Show supporting components

> **Important**
> This list indicates that secure data exchange using TLS is supported on the given connections; it does not specify the type of TLS supported. Refer to product- or component-specific documentation to determine if Mutual TLS and/or Simple TLS is supported.

CCPulse+

Secure data exchange is supported on the following CCPulse+ and Framework connections:

- Between CCPulse+ and Stat Server
- Between CCPulse+ and DB Server
- Between CCPulse+ and Configuration Server

Configuration Layer Components

Secure data exchange is supported on all Configuration Layer connections:

- Between Configuration Server and Configuration Manager

- Between Configuration Server and Configuration Server Proxy
- Between Configuration Server and DB Server
- Between primary and backup Configuration Servers
- Between Configuration Server and External Authentication LDAP Directory (LDAPS)

eServices Components

Secure data exchange is implemented on those connections involving eServices components, as indicated in the following table.

From	To	
Component	**Port (Secure Listening Port)**	
Chat Server 8.1.0 and later	Interaction Server 8.1.0 and later	`default` (or alternate name)
	Universal Contact Server 8.1.0 and later	`default` (or alternate name)
	Configuration Server or Configuration Server Proxy	`default` (or alternate name)
	Message Server	`default` (or alternate name)
Interaction Server 8.1.0 and later	Universal Contact Server	`default` (or alternate name)
	DB Server	`default` (or alternate name)
	Stat Server	`default` (or alternate name)
	Chat Server 8.1.0 and later	ESP (required name)
	Configuration Server or Configuration Server Proxy	`default` (or alternate name)
	Message Server	`default` (or alternate name)
	E-mail Server 8.1.0 and later	`default` (or alternate name)
	Interaction Server 8.1.0 and later	`default` (or alternate name)
E-mail Server 8.1.0 and later	Configuration Server or Configuration Server Proxy	`default` (or alternate name)
E-mail Server 8.1.2 and later	Universal Contact Server 8.1.1 and later	`default` (or alternate name)
	Interaction Server 8.1.0 and later	`default` (or alternate name)
	Configuration Server or Configuration Server Proxy (writable)	`default` (or alternate name)
	Message Server	`default` (or alternate name)
Universal Contact Server Proxy 8.1.0 and later	Configuration Server	`default` (or alternate name)

From	To	
	or Configuration Server Proxy	
	Universal Contact Server 8.1.0 and later	`default` (or alternate name)
SMS Server 8.1.0 and later	Configuration Server or Configuration Server Proxy	`default` (or alternate name)
	Solution Control Server	`default` (or alternate name)
	Message Server	`default` (or alternate name)
	Interaction Server 8.1.0 and later	`default` (or alternate name)
Social Messaging Server 8.1.0 and later	Configuration Server or Configuration Server Proxy	`default` (or alternate name)
	Message Server	`default` (or alternate name)
	Interaction Server 8.1.0 and later	`default` (or alternate name)
Classification Server 8.1.0 and later	Configuration Server or Configuration Server Proxy	`default` (or alternate name)
Web API Server Java 8.1.0 and later	Configuration Server or Configuration Server Proxy	`default` (or alternate name)
	Solution Control Server	`default` (or alternate name)
	Message Server	`default` (or alternate name)
	Interaction Server 8.1.0 and later	`default` (or alternate name)
	E-mail Server 8.1.0 and later	`default` (or alternate name)
	Chat Server 8.1.0 and later	`default` (or alternate name)
	Stat Server 8.1.0 and later	`default` (or alternate name)
	Universal Contact Server 8.1.0 and later	`default` (or alternate name)
Web API Server .NET	Configuration Server or Configuration Server Proxy	`default` (or alternate name)
	Solution Control Server	`default` (or alternate name)
	Message Server	`default` (or alternate name)
	Interaction Server 8.1.0 and later	`default` (or alternate name)
	E-mail Server 8.1.0 and later	`default` (or alternate name)
	Chat Server 8.1.0 and later	`default` (or alternate name)
	Stat Server 8.1.0 and later	`default` (or alternate name)

From	To	
	Universal Contact Server 8.1.0 and later	`default` (or alternate name)

In addition to the general procedures discussed in this Guide:

- Additional steps are required to configure TLS for Universal Contact Server and E-mail Server, both of which are Java-based servers. Refer to the *eServices 8.1 Deployment Guide* for additional information.
- If TLS is configured on Universal Contact Server (UCS), E-mail Server, or Social Messaging Server, either as a server on its ESP port or as a client of Configuration Server, Interaction Server, Chat Server, UCS, or Message Server, follow these steps to enable it as a Windows Service:
  1. Select the Windows service related to UCS, E-mail Server, or Social Messaging Server.
  2. Select the `Log On` tab.
  3. Select `Log on as this account` and provide the username and password of a local host user.

Genesys Composer

Secure data exchange is supported between Genesys Composer and Configuration Server/ Configuration Server Proxy, and on both TCP and SIP connections to GVP Debugger.

Genesys Info Mart

Secure data exchange is supported between Genesys Info Mart and:

- Configuration Server/Configuration Server Proxy
- Message Server
- Interaction Concentrator database and Info Mart databases (via SSL)

Genesys Knowledge Center

Secure data exchange is supported between Genesys Knowledge Center and:

- Configuration Server/Configuration Server Proxy
- Message Server
- Solution Control Server

Genesys Voice Platform

Secure data exchange is supported on the following connections within Genesys Voice Platform (GVP) and between GVP and Framework:

- Between GVP components and Configuration Server/Configuration Server Proxy
- Between GVP components and SIP Server
- Between GVP Reporting Server and GVP Media Control Platform/Call Control Platform/Resource Manager/ MRCP Proxy

- SIP interface on GVP Resource Manager/Media Control Platform/Call Control Platform/CTI Connector
- MRCP Platform on GVP Media Control Platform/MRCP Proxy
- HTTP interface on GVP Media Control Platform/Call Control Platform
- HTTP interface on GVP Supplementary Service Gateway

> **Important**
> GVP does not use standard TLS configuration in all cases. It uses a different format for its internal connections (for example, `sip.transport.0=transport0 tls:any”<SIP Port>`) that is described in the GVP Deployment Guide and GVP User’s Guide.

Gplus Adapter for Siebel CRM

Secure data exchange is supported on all internal connections of the Gplus Adapter for Siebel CRM, and between the adapter and:

- Configuration Server/Configuration Server Proxy
- Interaction Server
- Siebel

intelligent Workload Distribution

Secure data exchange is supported on Workload Distribution (iWD) connections to all other Genesys Servers. In addition, Business Context Management Service (BCMS) supports TLS on its connection with Interaction Server.

Interaction Concentrator (ICON)

Secure data exchange is supported between the ICON Server and all other Genesys Servers.

Interaction Layer Components

Secure data exchange is supported on the following Interaction Layer Components:

- From the web browser to the Genesys Administrator/Genesys Administrator Extension server (HTTPs/ SSL)
- From the Genesys Administrator Extension server to:
  - Configuration Layer components—Configuration Server, Solution Control Server, Genesys Deployment Agent
  - Interaction Layer components—Genesys Administrator Extension Database, Genesys Administrator API
  - Database Management Systems—Oracle, MS SQL
  - License Reporting Manager (LRM) Database

Interaction Workspace Components

See Workspace Desktop Edition.

IVR Server and IVR Drivers Components

Secure data exchange is supported on the following IVR Drivers, IVR Server, and Framework connections:

- Between IVR Driver for WVR for AIX, IVR Driver for MPS and Configuration Server/Configuration Server Proxy
- Between IVR Drivers WVR for AIX, IVR Driver for MPS and IVR Server(s)
- Between IVR Server and Configuration Server/Configuration Server Proxy and/or T-Servers
- Between IVR SDK (C-library version only)

License Resource Manager (LRM)

Secure data exchange is supported between License Resource Manager and:

- All other Genesys Servers
- All supported databases

Load Distribution Server

Load Distribution Server supports secure data exchange on all connections.

Management Layer

Secure data exchange is supported on the following Management Layer connections:

- Between Message Server and DB Server
- Between Message Server and its clients
- Between Message Server and Solution Control Servers
- Between Solution Control Server (SCS) and Solution Control Interface (SCI)
- Between SCS and Configuration Server/Configuration Server Proxy
- Between SCI and Configuration Server/Configuration Server Proxy
- Between SCI and DB Server
- Between Local Control Agent (LCA) and SCS
- Between Genesys Deployment Agent and its clients
- Between primary and backup Solution Control Servers

Media Layer Components

Secure data exchange is supported on the following Media Layer connections:

- Between T-Servers
- Between Network T-Servers
- Between T-Server and Network T-Server
- Between T-Server/Network T-Server and Configuration Server/Configuration Server Proxy
- Between primary and backup T-Servers in hot standby mode
- Between T-Server and custom client applications that have been created with the new T-Library

SIP Server supports secure data exchange on all connections listed above, plus on all SIP traffic.

Orchestration Server

Secure data exchange is supported on the following connections between Orchestration Server and:

- Configuration Server/Configuration Server Proxy
- DB Server
- Message Server
- T-Server
- SIP Server
- IVR Server
- Interaction Server
- Federation Server
- Intracluster connections

Outbound Contact Components

Secure data exchange is supported on the following Outbound Contact and Framework connections:

- Between Outbound Contact Server and CPD Server/CPD Proxy Server
- Between Outbound Contact Server and Configuration Server/Configuration Server Proxy
- Between Outbound Contact Server and T-Server
- Between Outbound Contact Server and DB Server
- Between Outbound Contact Server and Stat Server
- Between CPD Server and CPD Proxy Server
- Between CPD Server and T-Server
- Between CPD Server/CPD Proxy Server and Configuration Server/Configuration Server Proxy

Platform SDK

Platform SDK supports TLS for Genesys components that support this feature. For details about how TLS can be used in custom-built applications, refer to the appropriate API Reference for your development platform.

Pulse

Secure data exchange is supported between Pulse and all other Genesys Servers.

Services Layer Components

Secure data exchange is supported on the following Services Layer connections:

- Between Stat Server and Configuration Server/Configuration Server Proxy
- Between Stat Server and T-Server/SIP Server
- Between Stat Server and DB Server
- Between Stat Server and Interaction Server
- Between Stat Server and Message Server
- Between Stat Server II and Configuration Server/Configuration Server Proxy

In addition, secure data exchange is supported between Stat Server and all client connections that support this feature.

Universal Contact Components

Refer to eServices Components to determine on what connections involving Universal Contact Server/ Universal Contact Server Proxy support secure data exchange using TLS.

Universal Routing Components

Secure data exchange is supported between all Universal Routing components and those Framework components that support this feature.

Starting with Security Pack on Unix 8.1.2, a secure HTTP (HTTPS) connection for Universal Routing Server can be configured without a client certificate.

Workforce Management Components

Secure data exchange is supported on the following connections within Workforce Management (WFM) and between WFM and Framework:

- Between WFM Data Aggregator and Configuration Server/Configuration Server Proxy, Message Server, and Stat Server
- Between WFM Data Aggregator and WFM Server
- Between WFM Daemon and Configuration Server/Configuration Server Proxy and Message Server
- Between WFM Daemon and WFM Server
- Between WFM Server and Configuration Server/Configuration Server Proxy and Message Server
- Between WFM Server and WFM Builder and WFM Server (acting as a server application)
- Between WFM Builder and Configuration Server/Configuration Server Proxy and Message Server
- Between WFM Builder and WFM Server

- Between WFM Web and WFM Server, WFM Data Aggregator, and WFM Builder
- Between WFM Configuration Utility and WFM Server
- All internal connections, and all connections to Configuration Server/Configuration Server Proxy, and Message Server.

> **Important**
>
> Connections internal to WFM use OpenSSL, not the standard IIRC. Refer to WFM documentation for specific instructions about setting up secure connections using OpenSSL.

Workspace Desktop Edition (formerly known as Interaction Workspace) Components

Secure data exchange is supported on the following Workspace Desktop Edition connections:

- Between Workspace Desktop Edition and Stat Server
- Between Workspace Desktop Edition and T-Server
- Between Workspace Desktop Edition and Configuration Server
- Between Workspace Desktop Edition and Universal Contact Server
- Between Workspace Desktop Edition and Interaction Server
- Between Workspace Desktop Edition and Chat Server Server
- Between Workspace Desktop Edition SIP Endpoint and SIP Server

Workspace Desktop Edition can connect to any Genesys application configured for TLS, and whose Host is assigned a certificate as described in Assigning a Certificate to a Host.

Connection to Configuration Server in TLS relies on the auto-detect mode implemented by Configuration Server as described in Configuring Secure Connections to Configuration Server.

Feature Description

TLS secures connections through the exchange of authentication digital certificates during a handshake process which negotiates ciphers and key lengths used to encrypt exchanged data.

TLS can be configured in two ways, as described in the following sections:

- Simple TLS
- Mutual TLS

See Supporting Components for the list of components and connections that support TLS.

Simple TLS

In simple TLS, only the Server has a security certificate. It sends this certificate to the Client, which checks the certificate against its own Certificate Authority (CA). In effect, this authenticates the identity of only the Server.

Basic steps of this authentication are as follows:

1. TLS Client connects as anonymous.
2. TLS Server sends to TLS Client its certificate, containing a certificate chain that begins with the server's public key certificate and ends with the CA's root certificate. See Certificate Generation and Installation.
3. TLS Client checks the CA certificate in its trusted CA list.
4. TLS Client compares the TLS Server host name and the certificate's subject field, which must be identical (**tls-target-name-check=**`host`). See Check for Certificate-Host Matching.
5. TLS Client is satisfied that the server certificate is not expired and has not been revoked. See Certificate Revocation Lists.

Mutual TLS

In mutual TLS, both the Server and the Client have security certificates. They exchange their certificates, then each checks the other's certificate against its own CA. This authenticates the identities of both the Server and the Client.

Basic steps of this authentications are as follows:

1. TLS Server and TLS Client exchange their certificates and check the root CA in the list of trusted CAs. See Certificate Generation and Installation.
2. TLS Client compares the TLS Server host name and the certificate's subject field, which must be identical (**tls-target-name-check=**`host`). See Check for Certificate-Host Matching.
3. TLS Client is satisfied that the server certificate is not expired and has not been revoked. See Certificate Revocation Lists.
4. TLS Server is satisfied that the client certificate is not expired and has not been revoked. See Certificate Revocation Lists.

You can upgrade to mutual TLS by setting the **tls-mutual** option in the **[security]** section to 1, as follows:

tls-mutual
Default Value: `0`
Valid Values: `0`, `1`
Changes Take Effect: Immediately

Specifies if mutual TLS is used for secure data transfer. If set to `1`, TLS certificates must be configured on both the server and client applications. If set to `0` (the default), client certificates are not required, and either simple TLS or data encryption (if **client-auth=**`0`) is used.

Evolution of Genesys TLS

Prior to 8.1.3, secure data exchange was accomplished by encrypting the data, using the TLS server certificate.

Starting in 8.1.3, simple TLS is the default method of secure data exchange. On the Windows platform, Configuration Server enables automatic authentication of a server's security certificate by the Windows TLS client socket. However, this might cause the failure of existing TLS connections for which server certificates were not configured or CAs were not configured on the clients. Genesys recommends that to prevent authentication errors on those existing TLS connections, make sure that server certificates are used and/or CAs are configured on the client applications. Alternatively, you can set the **client-auth** option to zero (`0`) to disable the default behavior and restore pre-8.1.3 behavior. This option can be set at the connection, application, or host level, with the same order of precedence.

Environment Prerequisites

The instructions in this document assume that you are adding Genesys TLS to existing connections of your Genesys configuration—that is, that your applications have already been installed, properly configured, and associated with hosts and with each other. See product-specific deployment guides for instructions about, and deployment instructions for, these components.

Supported Platforms

> **Important**
>
> Genesys TLS is not supported on all operating systems that Genesys products support. For UNIX-based operating systems, see Setting the Environment Variables for more information.

Refer to the *Genesys Supported Operating Environment Reference Guide* for a list of operating systems and database systems supported in Genesys releases 7.6 and later.

Supported Versions of TLS

Genesys TLS supports the following versions of TLS:

- TLS 1.1
- TLS 1.0
- SSL v3
- SSL v2

However, the version of TLS that is actually supported depends on the involved components and the software they are running. Refer to product documentation for TLS version information.

Specifying the TLS Protocol

Starting with Security Pack 8.5, an application can specify the lowest compatible protocol used by Security Pack on UNIX to send and accept secure connection requests on one or more of its connections, thereby limiting the use of obsolete protocols. To enable this, use the following option:

sec-protocol
Default Value: SSLv23
Valid Values: SSLv23, SSLv3, TLSv1, TLSv11
Changes Take Effect: Immediately

Specifies the protocol used by the component to set up secure connections.

This option is configured on one of three levels:

- Host-level (the application host): In the **[security]** section of the annex of the Host object.
- Application-level: In the **[security]** section of the options of the Application object.
- Port-level (connection-level): As a transport parameter of the application's connection.

> **Important**
> If the component reads its configuration information solely from its configuration file, such as LCA or Genesys Deployment Agent, set this option in the **[security]** section of the appropriate configuration file (such as **lca.cfg** for LCA or **gda.cfg** for Genesys Deployment Agent).

On a single component, this option must be configured at the same level where the certificate is configured. Across a network, if this option is configured at multiple levels (connection, application, host), the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
- The value set at the application level takes precedence over the value set at the host level.

Feature Configuration

All Genesys components are configured in Genesys Administrator. To enable secure data exchange between the components, you must configure additional parameters in the Host objects, and in the Application objects that represent these components.

To use Genesys TLS functionality, you must complete the following steps:

1. For UNIX, install the Security Pack on each host computer where Genesys components run. See Security Pack on UNIX.
2. Set up a Certificate Authority (CA) on all server and client hosts that will be using TLS. See Certificate Generation and Installation.

3. Create and install security certificates on UNIX and/or Windows platforms, as follows:
   - For simple TLS, install the certificates on only those hosts where the Server applications are running.
   - For mutual TLS, install the certificates as follows:
     - On those hosts on which the Server applications are running.
     - On other hosts that are not running Server applications but are running Client applications.

   See Certificate Generation and Installation.
4. Complete application-specific and/or host-specific configuration procedures in Genesys Administrator. See Genesys TLS Configuration.

You can create and manage certificates and the corresponding private keys by using the OpenSSL toolkit and Windows Certification Services.