Genesys Security Deployment Guide

Supporting Components

12/15/2025

Contents

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.

> ### 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.

[+] Show 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)

From	To	
	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 or Configuration Server Proxy	default (or alternate name)
	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	default (or alternate name)

From	To	
	or Configuration Server Proxy	
	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)`
	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 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 Co-browse Server

Secure data exchange is supported on the following connections:

- Between Co-browse Server and Configuration Server/Configuration Server Proxy
- Between Co-browse Server and Message Server
- Between Co-browse Server and External Cassandra
- HTTPS to communicate with proxied resources target servers.

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 Softphone

Secure data exchange is supported between Genesys Softphone and the other components of the SIP Infrastructure.

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 Routing Designer (IRD)

Secure data exchange is supported between IRD and Message Server.

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
- Stat Server
- Universal Routing 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.

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.