Genesys Security Deployment Guide

Secure HTTP (HTTPS)

5/5/2025

Secure HTTP (HTTPS)

In addition to Transmission Control Protocol (TCP) support for TLS, most Genesys connections using Hypertext Transfer Protocol (HTTP) also support Communications Integrity through the use of HTTP Secure (HTTPS). HTTPS applies SSL or TLS to HTTP connections. In most cases, HTTP is used for communications between web servers and web browsers, and therefore applications are set up to be compatible with the HTTPS setup at the web server. In some cases, HTTP is also used for connections which do not include a web browser, such as web services like Representational State Transfer (REST). See product documentation for details.

Supporting Components

The following components, or elements thereof (as indicated), support the use of HTTPS:

- Universal Routing (connecting to external Web Services)
- Outbound Contact (HTTP Connections for Pre-Validation)
- eServices Web API Server
- Genesys Co-browse (if customer site does not already support)
- Genesys Knowledge Center
- Context Services (REST API)
- Workforce Management (Web and connections between internal components)
- SIP Feature Server
- Voice Platform
- Interaction SDK
- Mobile Services API
- Genesys Agent Desktop
- Genesys Pulse
- Workspace Desktop Edition (ClickOnce)
- Agent Scripting (Plug-in for Workspace Desktop Edition)
- Performance Management Advisors (to Web Server)
- Genesys Administrator
- Genesys Administrator Extension
- Pulse (Plug-in for Genesys Administrator Extension)
- License Reporting Manager (Plug-in for Genesys Administrator Extension)
- Composer (Web Request Block, Context Services)
- Gplus Adapter for Siebel CRM

- Gplus Adapter for SAP CRM

- Intelligent Workload Designer (Web User Interface)

- Genesys Rules System

- Web Engagement

- WebRTC

- Genesys Web Services

- Speech & Text Analytics

- Genesys Video Gateway 9.0

- Genesys Predictive Routing