This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Deployment Guide

Security

5/9/2025

Security

Genesys Web Engagement supports HTTPS/SSL/TLS to protect data over the web.

- All connections can be secured, including connections from the browser to the Frontend and Backend servers.
- Applications defined in Configuration Server can have both HTTP and HTTPS connections.

Transport Layer Security (TLS) is supported above Java containers, Jetty and Apache Tomcat. The user data submitted from the browser tier is always sent through secure connections. To support secure (TLS) connections to Configuration Server on Windows OS, if you use the JDK 6 64 bit, it is mandatory to do *one* of the following:

- Update Java Development Kit 6 64 bit with Java SE Development Kit 6, Update 38 (JDK 6u38) or older.
- Setup JDK 7.

> ## Important
> Genesys performs security testing with OWASP Zed Attack Proxy (ZAProxy) to make sure the Genesys Web Engagement solution is invincible to known attacks. For details, see Security Testing with ZAProxy.

Genesys Web Engagement includes additional security configurations that can be used with your GWE installation:

- Secure Sockets Layer (SSL) — Load SSL certificates and configure Jetty.
- Transport Layer Security (TLS) — Configure TLS for Genesys and Web Engagement servers.
- Authentication — Enable authentication for the Backend Server, Interaction Workspace, and the Engagement Strategy.

Next Steps

After you configure security for Genesys Web Engagement, you can configure features to enable additional functionality.