Deployment Guide

Security

12/17/2025

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 Web Engagement server.
- 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.

> **Important**
> Genesys performs security testing with OWASP Zed Attack Proxy (ZAProxy) to protect the Genesys Web Engagement solution against known vulnerabilities. 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 Web Engagement Server, Interaction Workspace, and the Engagement Strategy.
- Cassandra Security — Establish a secure channel between your client and Cassandra coordinator notes.

Next Steps

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