Genesys Knowledge Center Deployment Guide

Security

4/24/2025

Security

Genesys Knowledge Center adheres to the standards described in the Open Web Application Security Project (OWASP) Top 10 — see the OWASP website for details about the Top 10 — and has adopted several methods of ensuring security, for example:

- Errors are logged locally to prevent information leakage through API requests.
- User sessions have a timeout option.
- Cross Site Request Forgery Protection

> **Important**
>
> Genesys performs security testing with OWASP Zed Attack Proxy (ZAProxy) to make sure the Genesys Knowledge Center solution is invincible to known attacks.

Genesys Knowledge Center includes additional security configurations that can be used with your Knowledge Center installation:

- Secure HTTP Communication — Load SSL certificates and configure Jetty to expose Knowledge Center API securely.
- Transport Layer Security (TLS) with Genesys Server — Configure TLS for connection between Knowledge Center servers and other Genesys server.
- Authentication — Enable authentication for the Knowledge Center Server and the CMS.
- Cassandra Security — Enable secure communication between Cassandra nodes and Knowledge Center CMS