Genesys Knowledge Center Deployment Guide

Security

5/4/2025

Security

Genesys is committed to offering products and solutions with a high level of security. Opening Application Programming Interface (API) access on the web requires a secure transmission. Genesys Knowledge Center does not compromise the security level of the enterprise network.

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

The following topics discuss issues that you may wish to consider when deploying the Genesys Knowledge Center, depending on your enterprise network architecture.

> **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:

- 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.
- Cross Origin Resource Sharing (CORS) filter — Configure web resources that are allowed to access Knowledge Center APIs