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.

# Web Services and Applications Deployment Guide

## Configuring security

5/8/2025

# Configuring security

Web Services 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

Web Services includes additional security configurations that you can use with your installation:

- Transport Layer Security (TLS)
- Security Assertion Markup Language (SAML) authentication
- Cross-Site Request Forgery (CSRF) protection
- Cross-Origin Resource Sharing (CORS) filter

For details about how Web Services handles authentication, see Web Services authentication flow.

## Next step

- Starting and testing Web Services and Applications