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

12/14/2025

Security

Genesys Co-browse supports the following ways to protect data over the web:

- **Encryption of co-browsing data**—Co-browsing related data passed between the user, the Co-browse Server and the agent is encrypted through the HTTPS connection:
  - **HTTPS connection for Jetty**—A Co-browse Server application defined in Configuration Server can have both HTTP and HTTPS connections for Jetty supplied with Co-browse. Related documentation:
    - *Add the secure port* section in Creating the Co-browse Server Application
    - *Edit the connection and set the ID to the HTTPS listening port* in Configuring Connection to Co-browse Server for Interaction Workspace
  - **HTTPS connection for Co-browse cluster**—A Co-browse Server application supports both HTTP and HTTPS connections for Co-browse cluster. Related documentation:
    - `secureUrl` and `useSecureConnection` options in the cluster section of the Co-browse Server application configuration.
    - `secureUrl` and `useSecureConnection` options in the cobrowse section of the Workspace Desktop Edition application configuration.
  - **HTTPS website instrumentation**—to work with Co-browse, the web page must include the Co-browse JavaScript code that provides the access to Co-browse resources. Co-browse resources can be loaded through HTTPS.
    Related documentation: Website Instrumentation.

> **Warning**
>
> For Co-browse cluster to work correctly, specify HTTPS access to the Co-browse resources through the Load Balancer. In case there is a single Co-browse Server node, the instrumentation snippet should include HTTPS access to single node resources.

- **Access the internet through a forward proxy**—If HTTP connections must go through an internal proxy server (for example, DMZ or local intranet), you must configure forward proxy options to let the Co-browse server obtain public web resources.
  Related documentation: See the forward-proxy section in the Co-browse Server application configuration.
- **Secure Sockets Layer (SSL)**—the Jetty web server supplied with the Co-browse solution includes a pre-configured, self-signed certificate. This allows you to use HTTPS out of the box in a lab or demo environment. For a production environment, you should use a certificate issued by a third-party Certificate Authority.
  Related documentation: Load SSL certificates and configure Jetty.
- **DOM restrictions**—Genesys Co-browse allows you to hide sensitive data and restrict web elements control from agents in a Co-browse session.
  Related documentation: Configure DOM Restrictions
- **CORS control**—Co-browse Server supports CORS control for websites. You may specify the list of origins allowed to access the Co-browse Server.
  Related documentation: cross-origin section in the Co-browse Server application configuration.

- **Transport Layer Security (TLS)**—all connections to the Genesys servers can be secured. TLS is supported above Java containers and Jetty. The user data submitted from the browser tier is always sent through secure connections.
  Related documentation: Configuring TLS
- **Static resources proxying**—Co-browse server proxies some static assets of your website like CSS, images, and fonts. This is generally safe since your website is the only source of these assets in a Co-browse session.

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