Deployment Guide

Security

5/11/2025

Security

Genesys Co-browse is part of a solution deployment, and security should be considered at the solution level. For example, Genesys Co-browse takes measures to make sure hidden attacks in DOM do not make it to agent desktops. Meanwhile, you must consider other areas, like only exposing Genesys Co-browse on HTTPs ports, hardening intermediate proxies so as to suppress or add certain HTTP headers, and so on. The Open Web Application Security Project provides excellent guidelines to help.

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:
    - **Configure Security Certificate**—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.
    - **Configuring Cipher Suites**—To configure specific cipher suites to include or exclude, see the Disabling/Enabling Specific Cipher Suites section of the Jetty TLS documentation.
    - **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 Object in Genesys Administrator
        - *Edit the connection and set the ID to the HTTPS listening port* in the Configuring Connection to Co-browse Server/Node Application for Workspace Desktop Edition
    - **HTTPS connection for Co-browse cluster**—A Co-browse Server application supports both HTTP and HTTPS connections for Co-browse cluster. Related documentation:
        - `url` option in the cluster section of the Co-browse Server application configuration.
        - `url` option 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.

- **Role-based control (RBAC) for Workspace Desktop Edition**—starting in version 8.5.001.09, the Co-browse WDE plug-in supports the `Agent—Can Monitor Co-browse` privilege. This privilege allows the agents to work with Co-browse sessions.
  Related documentation: Configuring Role-Based Access Control for Co-browse.
- **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
- **Security with External Cassandra**—Starting from 8.5.1, Genesys Co-browse supports secure access interfaces through authentication and authorization and secure network traffic through TLS.
  Related documentation: Cassandra Security
- **Static resources proxying**—Co-browse server proxies some static assets of your website like CSS, images, and fonts. While this is generally safe since your website is the only source of these assets in a Co-browse session, you may enforce the security using the following configuration options:
  - The `allowedExternalDomains` option in the http-proxy section allows you to list all the domains resources of which are allowed to be proxied through Co-browse server. Use this to prevent unauthorized parties from abusing the Co-browse server proxy.
  - The `disableCaching` option in the http-security section. Sometimes caching of resources loaded via HTTPS is considered not fully secure. While this is not so in 99% of cases because only static assets such as images or CSS are cached, you can force all caching to be disabled using this option.

> ### Important
> Genesys performs security testing with the OWASP Zed Attack Proxy (ZAProxy) to protect the Genesys Co-browse solution against known OWASP vulnerabilities. For details, see Security Testing with ZAProxy.