Deployment Guide

slave Section

5/2/2026

slave Section

Contents

localization

Default value:
Valid Values: String containing a valid URL
Changes Take Effect: Immediately

URL used to load external localization file. This file should be a JSON file hosted on a server with JSONP support (For example, the Co-browse server. See Serving JSONP). By default, the built-in English localization is used. For more information about localization, see Localization—Localizing the agent side UI.

> **Important**
>
> Starting in release 9.0.005.33, Genesys Co-browse Plug-in for Workspace Desktop Edition (WDE) now has a stricter policy for working with origins against the agent's localization. To allow working with the localization resource via HTTPS, you must place the resource in the same origin that the Co-browse Plug-in for WDE uses to work with Co-browse.
>
> If load balancing is used for the Co-browse Plug-in for WDE to access Co-browse, place the JSON localization file in the static folder of the Co-browse nodes, and add the following snippet in your NGINX configuration file.
>
> ```
> location /static {
>             proxy_pass https://<cobrowsecluster>$uri?$args;
> }
> ```

cssPatchUrl

Default value:
Valid Values: String containing a valid URL
Changes Take Effect: Immediately

URL used to load an external CSS file that is applied to the agent side representation of the page seen by the user. May be used to solve CSS synchronization issues.

theme

Default value: `wde`
Valid Values:

- `iws`—theme matching the look and feel of Interaction Workspace 8.1.
- `wde`—theme matching the look and feel of Workspace Desktop Edition.
- `wde-hc`—theme matching the **High Contrast** theme in Workspace Desktop Edition.

Changes Take Effect: Immediately

Name of theme applied to the agent side UI.

disableWebSockets

Default value: `false`
Valid Values:

- `true`—disable WebSockets
- `false`—do not disable WebSockets

Changes Take Effect: Immediately

This option will disable WebSocket communication.

> **Important**
> Use of this option in production is **not** recommended as it may have a significant impact on performance. See JavaScript API disable WebSockets for the analogous option for the customer side and more details.

externalJS

Default value:
Valid Values: String containing a valid URL

Changes Take Effect: Immediately (after agent side page reloads)

This option specifies the URL of an additional JavaScript file that will be loaded and executed on the agent side.

wweOrigins

Default value:
Valid Values: A comma-separated list of origins. For example, `http://my-web-server-1,http://my-web-server-2`.
Changes Take Effect: Immediately (after agent side page reloads)

Available since Co-browse Server **8.5.003.04**.

Configures the list of Workspace Web Edition origins used by agents. This option enables communication with Workspace Web Edition so an agent does not automatically become **inactive** when using the Co-browse iframe.

An origin consists of a protocol and domain. Optionally, you may include the port, username, and password in an origin. For example, if agents open Workspace Web Edition from `https://htcc.genhtcc.com/ui/ad/v1/index.html`, then you should set this option to `https://htcc.genhtcc.com`.

allowedThirdPartyDomains

Default Value: Empty

Valid Values: Empty, *, or a comma-separated list of origins. Example value: `https://site.com,http://test.site.org:8080`
Changes Take Effect: For new Co-browse sessions

Use this option to enable iframes from specific third-party domains for agents. By default, all third-party iframes in a website are disabled for agents. For example, if your website contains an iframe pointing to `https://third-party-site.com/a-page.html`, the iframe does not load for agents unless you list `https://third-party-site.com` in this option. You can also leave this option empty or set it to *:

- Empty—disables all third-party domains for agents.
- *—allows all third-party domains. Note that even if all third-party domains are allowed, JavaScript execution is always disabled in third-party iframes for the agent's browser.

When configuring third-party domains, you must list each subdomain seperately. For example, `https://third-party-site.com` does not include `https://subdomain.third-party-site.com`. You must list both to enable them.

password

Default Value: None
Valid Values: String with 16 characters
Changes Take Effect: Immediately for co-browse sessions started after change

Added in: Co-browse Server 8.5.102.02

Specifies the token used to authenticate communication between Co-browse Server and Workspace Desktop Edition.

CSP.enabled

Default value: true
Valid Values: true or false
Changes Take Effect: For new Co-browse sessions

Available from Co-browse Server 9.0.014.xxx.
If set to true, enables Content-Security-Policy header on agent side to prevent third-party JavaScript code.

CSP.reportOnly

Default value: false
Valid Values: true or false
Changes Take Effect: For new Co-browse sessions

Available from Co-browse Server 9.0.014.xxx.
If set to true, turns Content-Security-Policy into Content-Security-Policy-Report-Only header on the agent side.