



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

[http-proxy Section](#)

http-proxy Section

Contents

- [1 http-proxy Section](#)
 - [1.1 allowedExternalDomains](#)
 - [1.2 clientTlsProtocols](#)

Configures Co-browse Server's HTTP proxy functionality.

allowedExternalDomains

Default value: *

Valid Values: List of any valid domains or wild cards. For example, ***.mydomain.com**, ***.net**, **mydomain-*.com**.

Changes take effect: Immediately

List of domains from which resources are allowed to be proxied through Co-browse server. This option enforces an additional level of control of what can be included on the web page during a Co-browse session.

clientTlsProtocols

Default value: No value

Valid Values: A comma separated list of values from the following: TLSv1, TLSv1.1, TLSv1.2

Changes take effect: After Co-browse server restart

Explicitly lists TLS protocol versions Co-browse server should use when using HTTPS to communicate with proxied resource target servers. Co-browse server does not work with SSL protocol due to its security vulnerabilities. If a target server supports only a specific protocol (for example, TLSv1), specify only this protocol.