

## Security

Last Modified on 04.16.26

When you enable Content Security Policy (CSP) and/or Cross-Origin Resource Sharing within your Application Workspace zone, you need to add the URL of the portal to the security settings. If you do not add these, the Application Workspace widget will not be able to communicate with the Application Workspace Server.

CSP is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. Deprecated headers will also be used for maximum compatibility (X-XSS-Protection and X-Frame-Options).

Enforce the policy

Report violations

The url where the CSP violation reports should be send to \*

Upgrade insecure requests and enforce HTTPS schema

List of websites that are allowed to embed the zone (only used if enforce and/or reporting is enabled)

+ Add    Edit		Export	Search for...
Website ↑			
No records available.			

Save

With CORS, other websites can access resources on this zone. It is recommended to restrict cross origin authentication to only the websites that are trusted.

Restrict cross origin authentication

List of websites that are allowed to authenticate against the zone

+ Add    Edit		Export	Search for...
Website ↑			
No records available.			

Save