Recast

Security Settings

Last Modified on 2026-09-28

Options for tuning the webserver security. These settings impact the usage of the portal.

HTTP Strict Transport Security (HSTS)

A webserver can send a so-called HSTS header to a browser to indicate that the browser should only contact the webserver over a secure channel. This will help prevent man-in-the-middle attacks. The options for preloading and subdomains exist in case the parent domain wants to apply to a HSTS preload list like hstspreload.org.

HSTS Options:

- **Number of days the webbrowser should remember the zone, recommended minimum value is 365. To let browsers forget any old HSTS policy, set the number of days** – The number of days the browser should remember this setting. If HSTS is no longer desired after it has been activated, a value of zero tells the browser to forget any HSTS policy that has been associated with this zone in the past.
- **Enable preloading (custom actions required)** – For more information, see scotthelme.co.uk/hsts-preloading and hstspreload.org
- **Indicates that the policy should apply to subdomains next to the zone**

> If a zone certificate expires and HSTS is enabled, you may encounter difficulties reaching a zone.
> Consult your browser documentation on how to remove the HSTS state in the browser for the zone domain.

Content Security Policy (CSP)

Browsers allow for a vast amount of different content to be displayed on a page, ranging from external JavaScript to web assembly. With a CSP policy, the browser is told what should be allowed and what should not. By restricting the kind of content a page can host, the number of attack vectors can be greatly reduced.

CSP Options:

- **Enforce the policy**
- **Report violations**
  - **The url where the CSP violation reports should be sent to** – Specify a report URL that can receive the browser's reports and display them in a useful way. An example of a free service that provides this is report-uri.com

  A CSP policy can operate in four modes:
  - Disabled: No CSP is sent to the browser and the browser will not restrict the content based on CSP.
  - Enforced, no reporting: The browser will restrict the content and will not report any content that has been blocked.
  - Enforced and reporting: The browser will restrict the content and will report any content that has been blocked.
  - Reporting, no enforcing: The browser will not restrict the content but will report any content that violates the policy
- **Upgrade insecure requests and enforce HTTPS schema** – If the policy should include directives to upgrade insecure requests (HTTP) and enforce only HTTPS access for all resources.
- **List of websites that are allowed to embed the zone** – Include directives in the policy to allow the specified websites to embed Application Workspace via an iFrame.

Cross-Origin Resource Sharing

Recast

Using Cross-Origin Resource Sharing (CORS), you can limit the number of sources that can access the Application Workspace REST API. Recast recommends limiting who can authenticate against Application Workspace. Only allow trusted sources, for example Microsoft Teams if you wish to use the integration with Application Workspace.

CORS Options:

- **Restrict cross origin authentication** – When enabled, checks for allowed authentication sources.
- **List of websites that are allowed to authenticate against the zone**