Recast

Security Settings

Last Modified on 04.16.26

The security settings allow you to tune 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 sub domains exist in case the parent domain wants to apply to a HSTS preload list like hstspreload.org.

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 not desired anymore after it has been activated, a value of zero should be provided to tell 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

You can have difficulties reaching a zone if a zone certificate expires andHTST is enabled. Consult your browser documentation on how to remove the HSTS state in the browser for the zone domain.

Content Security Policy (CSP)

Browsers nowadays 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 not. By restricting the kind of content a page can host, the amount of attack vectors can be greatly reduced.

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.

For the reporting to work, you should 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

With CSP, you can also prevent other websites to embed the Application Workspace. You can specify trusted websites who can embed Application Workspace.

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

With CORS you can limit the number of sources that can access the Application Workspace REST API. It's recommended to restrict who can authenticate against Application Workspace. Only allow trusted sources, for example Microsoft Teams if you wish to use the integration with Application Workspace.

Restrict cross origin authentication – If checked, this will enable the checks for allowed authentication sources.

Recast