CSP Extension for Magento 2

Sprinix CSP (Content Security Policy) Extension helps to manage and whitelist to any host or external sources through configurations.
By Default, in Magento CSP module helps to detect and mitigate Cross-Site Scripting (XSS) and related data injection attacks, It can restrict browser content to allow only whitelisted resources to appear, whenever we had to add any external source, we had to manually upgrade and deploy it after adding it to the whitelist. Now with the help of Sprinix CSP extension , we just have to add our host or any external source in the config settings and it will already be whitelisted.

You can also add or manage the policies in csp_whitelist.xml which already exist in Sprinix CSP on path: app/code/Sprinix/CSP/etc/csp_whitelist.xml.

Installation Instructions

- Download 'Sprinix CSP Extension.zip' file .

- Extract 'Sprinix_CSP.zip' file to 'app/code/Sprinix/CSP'. You should create a folder path 'app/code/Sprinix/CSP' if not exist.

- Download '.overrides.zip' file .

- Extract '.overrides.zip' file to 'src'.

- Go to Magento root folder and run : bin/composer require kub-at/php-simple-html-dom-parser.

- bin/magento setup:upgrade;

- bin/magento setup:di:compile;

- bin/magento setup:static-content:deploy -f

- Add the below code in your src/composer.json file.

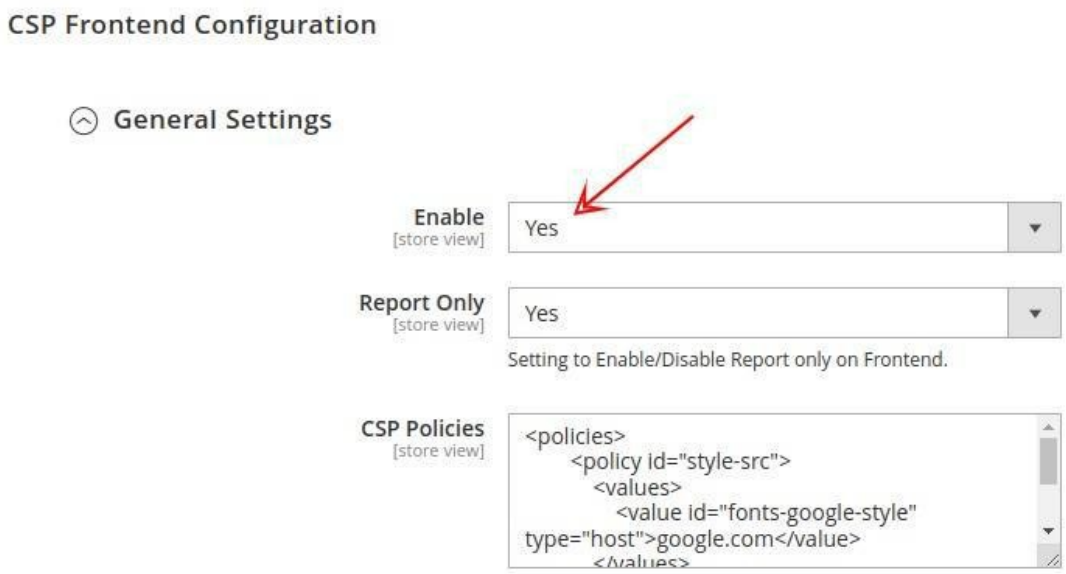
```
        "extra": {
            "magento-force": "override",
            "no-git-submodules": true,
            "composer-exit-on-patch-failure": true
        },
      "scripts": {
          "composer-overrides": "cp -rf .overrides/*/ ./",
          "post-install-cmd": [
          "@composer-overrides"
          ]
       },
      "scripts-descriptions": {
            "composer-overrides": "Override folders in project root with those i
n .overrides/ directory"
      }
```

- Then go to the root folder and run command : bin/composer install .
- Go to Magento root folder and run upgrade command line to install 'Sprinix_CSP'.
- bin/magento setup:upgrade
- bin/magento setup:di:compile
- bin/magento setup:static-content:deploy -f

Admin Store Configuration

To Configure the Sprinix CSP Extension for your stores follow the path given below:

STORES -> Configuration -> SPRINIX -> CSP

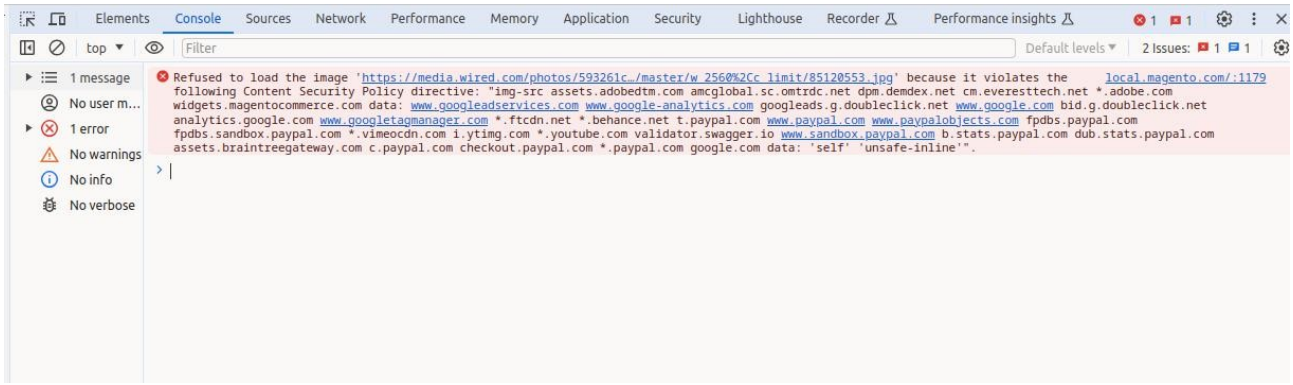


For the field, ‘Enable’ , select Yes to enable the extension.

There are two modes in CSP; “Reports_Only” and “Restrict Mode”. Ideally, Magento is always running with “Restrict Mode”.

Restrict Mode:

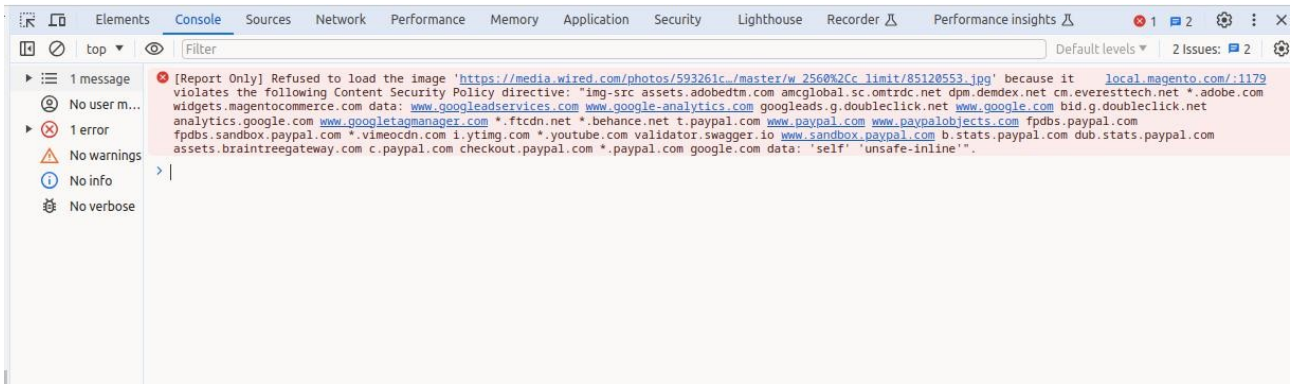
In this mode, Magento acts on any policy violations. The browser will refuse to load non-whitelisted content and report a CSP Error in the browser console.



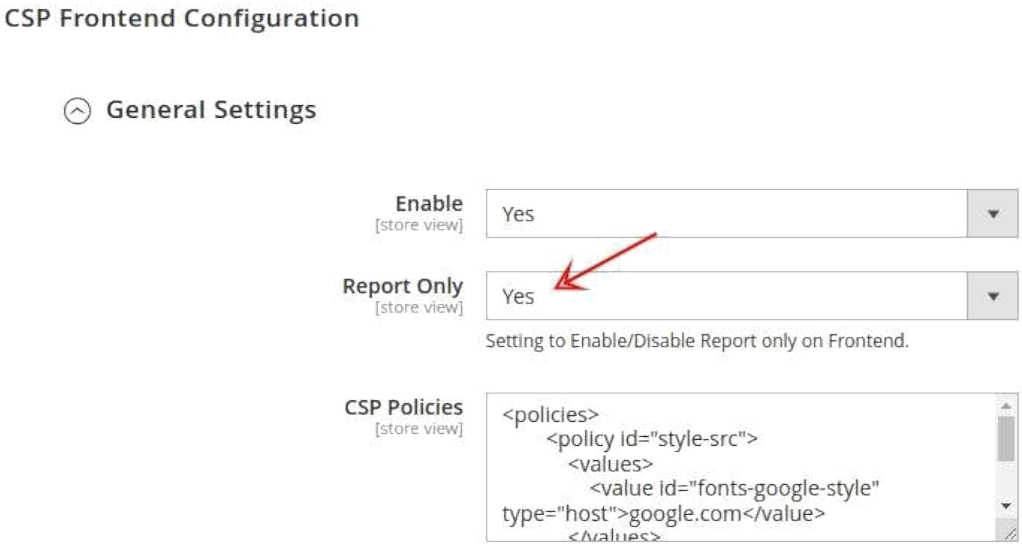
For Example, In the image attached above, CSP Refuses to load a image from “wired.com” as it is not on the CSP list.

Report Only:

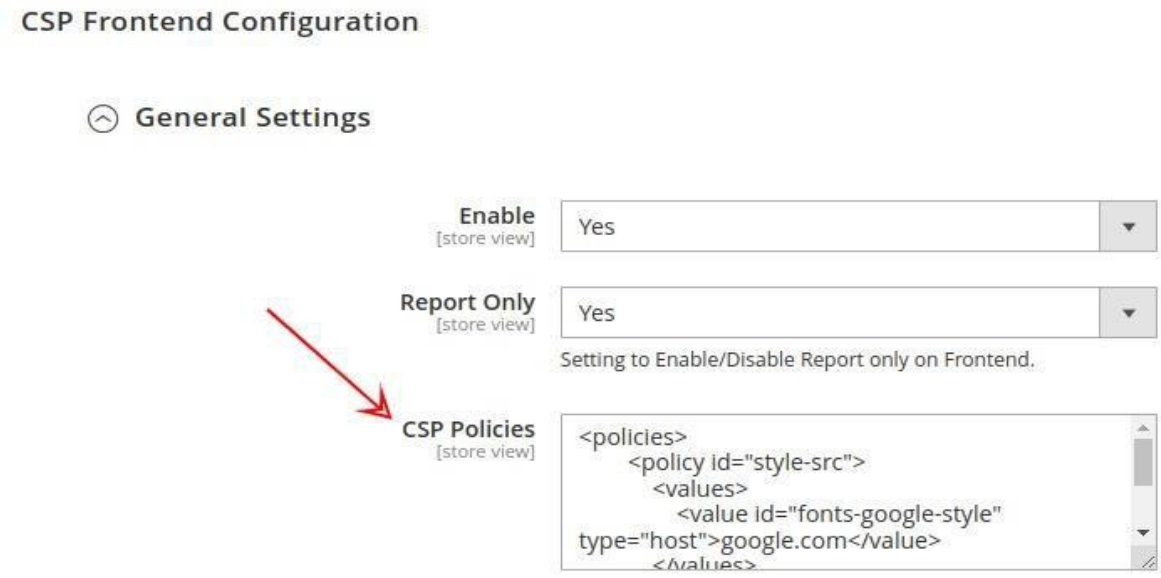
Magento reports policy violations but doesn’t block. By default, CSP violations are written to the browser console.



For the field, **‘Reports Only’**, select No, if you want enable the “Restrict mode”. By default it contains “Report Only” mode. So you can prepare the list of violated policies from browser console.

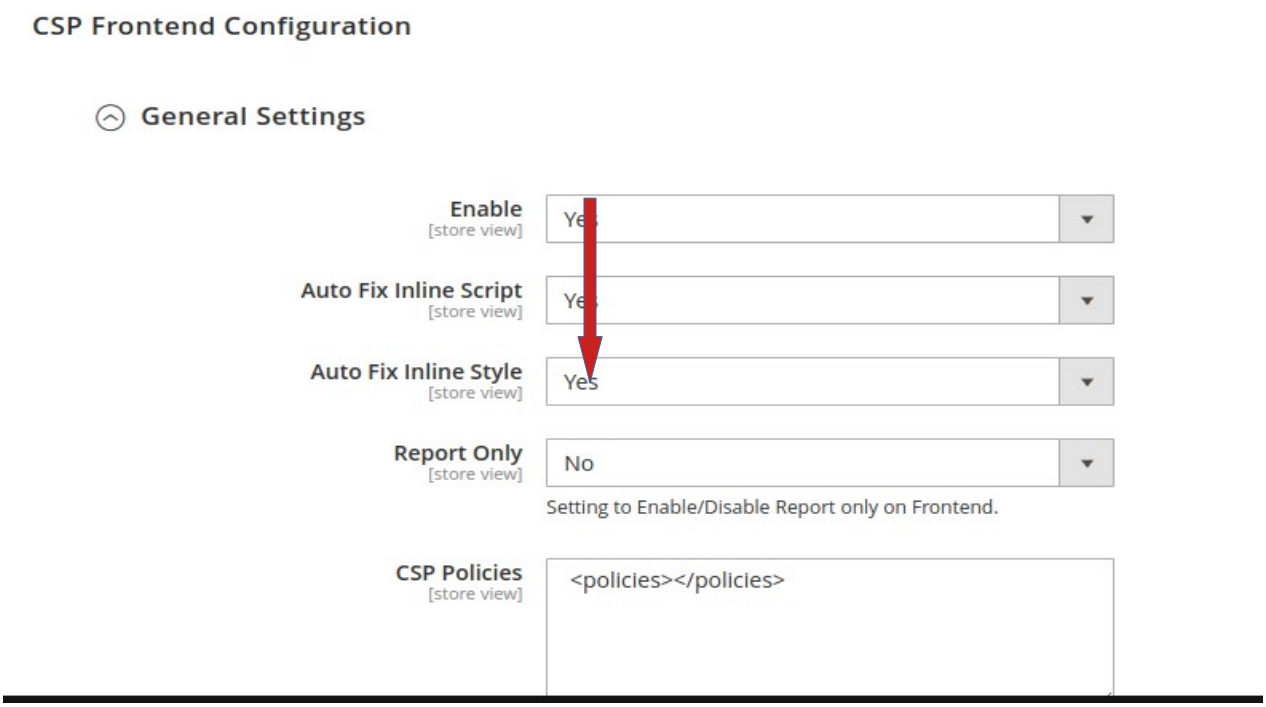


Earlier, we had to add our policies in magento csp_whitelist.xml. But now, With the help of given field named **'CSP Policies'** we can directly add the policies in our configuration setting. As we used to add policies in csp_whitelist.xml with the same format as followed to add policies in this. And, the CSP policies that is written in csp_whitelist.xml by default and policies added here through provided configuration will be merged.



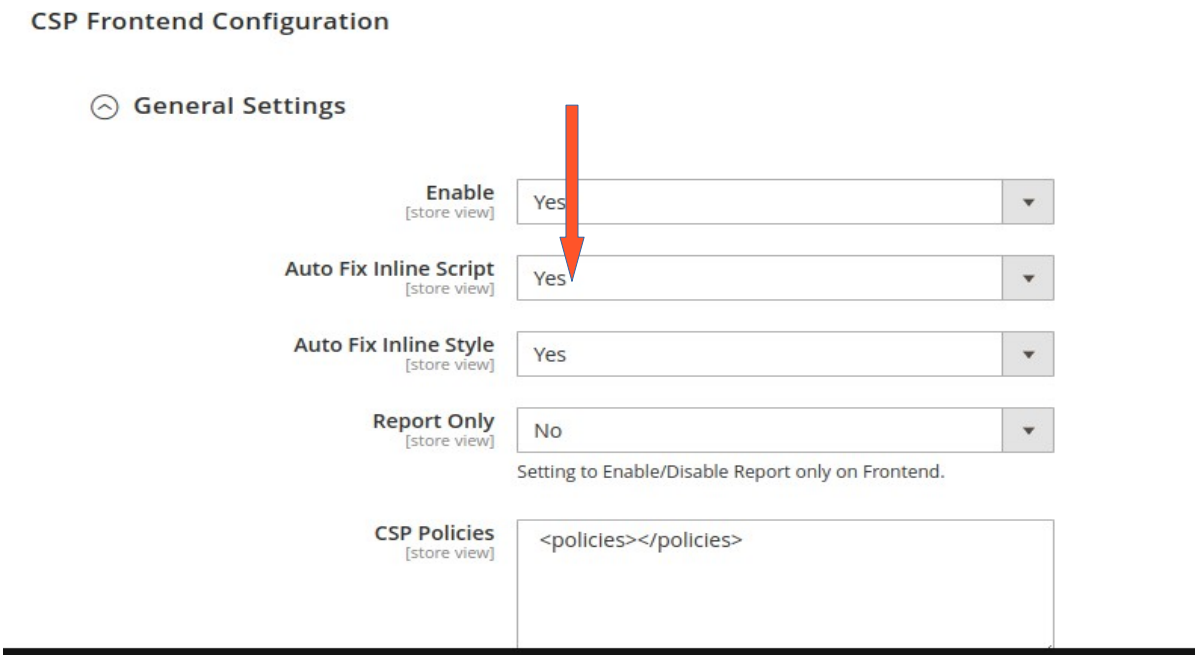
Auto Fix Inline Style:

Select “Yes” for the “Auto Fix Inline Style” field to autofix all the inline css.



Auto Fix Inline Script:

Select “Yes” for the “Auto Fix Inline Script” field to autofix all the inline script.

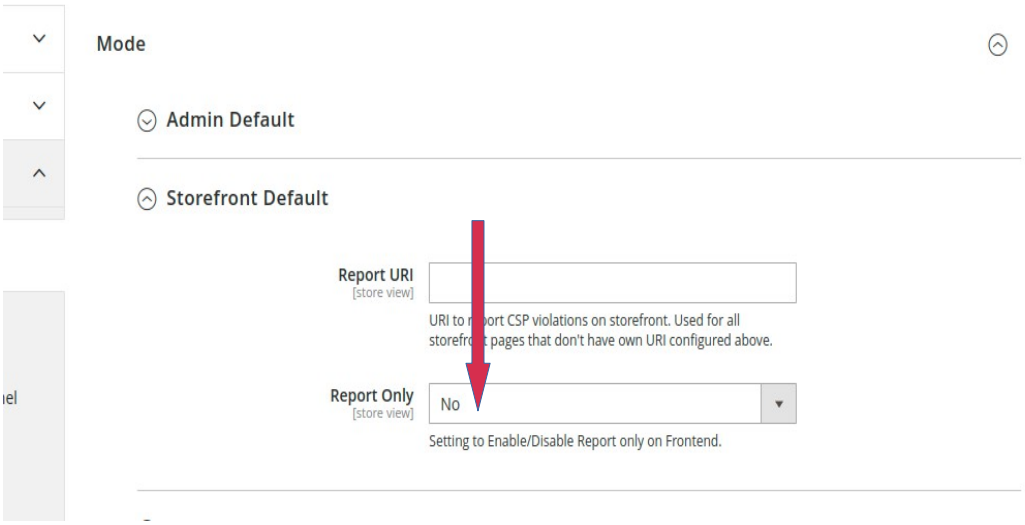


To Configure the Magento CSP module for your stores follow the path given below:

STORES -> Configuration -> SECURITY -> Content Security Policy(CSP)

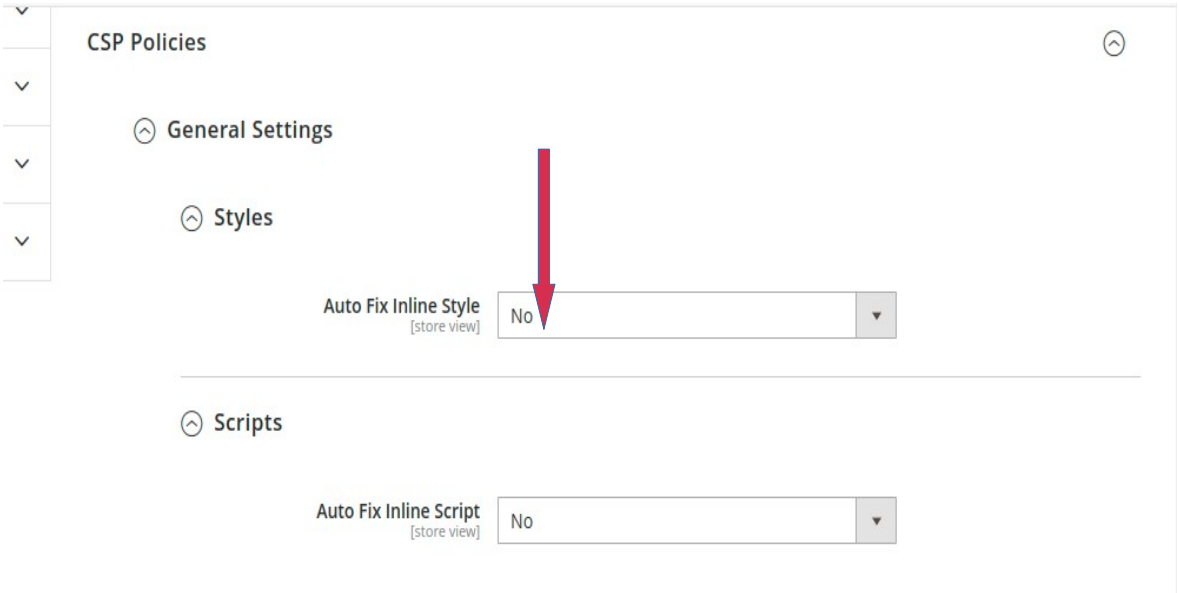
Report Only:

Stores -> Configuration -> Security -> Content Security Policy(CSP) -> Mode -> Storefront Default -> Report Only Select “No”.



Auto Fix Inline style:

Stores -> Configuration -> Security -> Content Security Policy(CSP) -> CSP Policies -> General Settings -> Styles -> Auto Fix Inline Style Select “No” .



Auto Fix Inline Script:

Stores -> Configuration -> Security -> Content Security Policy(CSP) -> CSP Policies -> General Settings -> Scripts -> Auto Fix Inline Script Select “No” .