

Magento 2 Content Security Policy (CSP) Whitelist Manager

[Installation and User Guide for Magento 2 Content Security Policy \(CSP\) Whitelist Manager](#)

Table of Contents

1. [Installation](#)
 - *Download Extension*
 - *Installation via app/code*
 - *Installation via Composer*
2. [Configuration Settings for Content Security Policy \(CSP\) Whitelist](#)
 - *General Settings*
 - *CSP Directives*
 - *Critical Security Overrides*
3. [CSP Reports Grid](#)
4. [Working of the extension](#)
 - *Steps to Check and Fix Console CSP Errors through CSP Grid*
 - *Steps to Check and Fix Console CSP Errors*
5. [Fixing Inline Script and Inline Style Content Security Policy Issues](#)
 - *Inline Style Error Example*
 - *Inline Script Error Example*

Installation

- **Download Extension:** Once you have placed the order from our site then go to My Account section and click on My Downloadable Products and download the extension package.

Configuration Settings for Content Security Policy (CSP) Whitelist

Go to **Admin > Stores > Configuration > Scommerce Configuration > CSP Whitelist**

General Settings

- **IMPORTANT INFORMATION**- When adding or changing whitelist, ensure to include only those domains that are recognized and trustworthy. This precaution is crucial because unauthorized or compromised domains may contain malicious scripts.
- **Enabled** - Select "Yes" or "No" to enable or disable the module.
- **License Key** - Please add the license for the extension which is provided in the order confirmation email. Please note license keys are site URL specific. If you require license keys for dev/staging sites then please email us at support@scommerce-mage.com.
- **Report Only Mode** - Set "Yes" to enable Report Only mode for CSP (it will only report CSP vulnerabilities in the CSP reports grid and browser console. Make sure to add Report URL in Configuration>Security>CSP for the CSP grid to collect reports. Set "No" to enable Strict Mode (it will prevent data from loading or code from getting executed to prevent vulnerabilities).
- **Report Collection Enabled:-** Set "Yes" to enable collecting CSP reports in the CSP grid, Set "No" these errors will only be available in the browser console
- **Report URL Configuration:-** Please add following URLs in *Security > CSP* section of your Store config **Admin Default** - https://BASE_URL/scommercereporturi/report/admin
Storefront Default**** - https://BASE_URL/scommercereporturi/report/storefront

General

Important Information <small>[store view]</small>	When adding or changing whitelist, ensure to include only those domains that are recognised and trustworthy. This precaution is crucial because unauthorised or compromised domains may contain malicious scripts.
Enabled <small>[store view]</small>	<input type="text" value="Yes"/> <input type="checkbox"/> Use system value <small>This setting will be used to enable or disable module</small>
License Key <small>[store view]</small>	<input type="text" value="cs6XioTaO62Nk"/> <small>This setting will be used to verify your license key for the given domain</small> N.B. License keys are domain specific so for your testing or staging sites please email us at support@scommerce-mage.com
Report Only Mode <small>[store view]</small>	<input type="text" value="Yes"/> <input type="checkbox"/> Use system value <small>This setting will be used to switch CSP mode</small> <small>YES - Report Only (Only report potential vulnerability)</small> <small>Please add Report URI in Configuration > Security > CSP to collect reports</small> <small>NO - Strict Mode (Refuse to execute code or load data to prevent vulnerability)</small>
Report Collection enabled <small>[store view]</small>	<input type="text" value="Yes"/> <input type="checkbox"/> Use system value <small>Enable this setting to collect CSP reports</small>
Report Uri Configuration <small>[store view]</small>	<small>Please add following URLs in Security > CSP section of your Store config</small> <small>Admin Default - https://BASE_URL/scommercereporturi/report/admin</small> <small>Storefront Default - https://BASE_URL/scommercereporturi/report/storefront</small>

CSP Directives

- **Default Src**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for default-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Default Src



Enabled
[store view]

Yes Use system value

This setting will be used to enable or disable csp whitelist for default-src
The default policy.

Whitelist entries
[store view]

URL	Type	Action
<input type="text" value="eadn-wc03-5796437.nxedge.io"/>	host <input type="checkbox"/>	
<input type="text" value="*.sharethis.com"/>	host <input type="checkbox"/>	

Please add URLs that you want to whitelist

- **Base Uri**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for base-uri
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Base Uri

Enabled
[store view]

Yes Use system value

This setting will be used to enable or disable csp whitelist for base-uri
Defines which URLs can appear in a page's **base** HTML element.

Whitelist entries
[store view]

URL	Type	Action
<input type="button" value="Add Record"/>		

Please add URLs that you want to whitelist

- **Child Src**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for child-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Child Src ⤴

Enabled [store view] Use system value

This setting will be used to enable or disable csp whitelist for child-src
Defines the sources for workers and embedded frame contents.

- **Connect Src**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for connect-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Connect Src ⤴

Enabled [store view] Use system value

This setting will be used to enable or disable csp whitelist for connect-src
Defines the sources that can be loaded using script interfaces.

Whitelist entries [store view]

URL	Type	Action
<input type="text" value="l.sharethis.com"/>	<input type="text" value="host"/> ▼	
<input type="text" value="*.stape.io"/>	<input type="text" value="host"/> ▼	
<input type="text" value="*.google-analytics.com"/>	<input type="text" value="host"/> ▼	
<input type="text" value="https://data.stbuttons.click"/>	<input type="text" value="host"/> ▼	

- **Font Src**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for font-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Font Src

Enabled
[store view] Use system value

This setting will be used to enable or disable csp whitelist for font-src
Defines which sources can serve fonts.

- **Form Action**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for form-action
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Form Action

Enabled
[store view] Use system value

This setting will be used to enable or disable csp whitelist for form-action
Defines valid endpoints for submission from **form** tags.

- **Frame Ancestors**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for frame-ancestors
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Frame Ancestors

Enabled
[store view] Use system value

This setting will be used to enable or disable csp whitelist for frame-ancestors
Defines the sources that can embed the current page.

Whitelist entries
[store view]

URL	Type	Action
<input type="text" value="https://www.googletagmanager."/>	<input type="text" value="host"/>	
<input type="button" value="Add Record"/>		

Please add URLs that you want to whitelist

- **Frame Src**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for frame-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Frame Src

Enabled [store view] Use system value

This setting will be used to enable or disable csp whitelist for frame-src
 Defines the sources for HTML elements such as **frame** and **iframe**.

• Img Src

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for img-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Img Src

Enabled [store view] Use system value

This setting will be used to enable or disable csp whitelist for img-src
 Defines the sources from which images can be loaded.

Whitelist entries [store view]

URL	Type	Action
<input type="text" value="eadn-wc03-5796437.nxedge.io"/>	<input type="text" value="host"/>	
<input type="text" value="*.sharethis.com"/>	<input type="text" value="host"/>	
<input type="text" value="www.facebook.com"/>	<input type="text" value="host"/>	
<input type="button" value="Add Record"/>		

Please add URLs that you want to whitelist

• Manifest Src

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for manifest-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Manifest Src

Enabled [store view] Use system value

This setting will be used to enable or disable csp whitelist for manifest-src
Defines the allowable contents of web app manifests.

- **Media Src**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for media-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Media Src

Enabled [store view] Use system value

This setting will be used to enable or disable csp whitelist for media-src
Defines the sources from which images can be loaded.

Whitelist entries [store view]

URL	Type	Action
<input type="button" value="Add Record"/>		

Please add URLs that you want to whitelist

- **Object Src**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for object-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Object Src

Enabled [store view] Use system value

This setting will be used to enable or disable csp whitelist for object-src
Defines the sources for the **object**, **embed**, and **applet** HTML elements.

- **Script Src**

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for script-src

- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Script Src



Enabled
[store view]

Yes

Use system value

This setting will be used to enable or disable csp whitelist for script-src
Defines the sources for JavaScript **script** HTML elements.

Whitelist entries
[store view]

URL/HASH	Type	Action
Pq3KG9KpfoqxdFBPx9qXjjawgSz	hash	
<input type="button" value="Add Record"/>		

Please add URLs or HASH that you want to whitelist

• Style Src

- **Enabled**- Select "Yes" or "No" to enable or disable csp whitelist for style-src
- **Whitelist entries**- Please add URLs that you want to whitelist. By default, the type of entry added would be host. You can also delete this entry and add multiple entries.

Style Src



Enabled
[store view]

Yes

Use system value

This setting will be used to enable or disable csp whitelist for style-src
Defines the sources for stylesheets.

Whitelist entries
[store view]

URL/HASH	Type	Action
lovcoObfHv0RELo8jMY/7tQivhjTj	hash	
<input type="button" value="Add Record"/>		

Please add URLs or HASH that you want to whitelist

Critical Security Overrides

- **Enable Unsafe Inline Script**- This setting permits the execution of unsafe inline scripts, which can be introduced by your developers / third party extensions / attackers. Make

sure you assess these unsafe inline scripts before setting this to YES.

Caution: Enabling unsafe inline scripts is a temporary measure and should only be done under the guidance of your developer. You must ask your developers or third party extension providers to whitelist their inline scripts. This setting must NOT be left on 'YES' permanently, as it significantly increases the risk of security vulnerabilities, making your site an easy target for attackers. Always prioritise the security of your site and user data.

Critical Security Overrides

Enable unsafe inline for scripts [store view] Use system value

This setting permits the execution of unsafe inline scripts, which can be introduced by your developers / third party extensions / attackers. Make sure you assess these unsafe inline scripts before setting this to YES.

Enabling unsafe inline scripts is a temporary measure and should only be done under the guidance of your developer. You must ask your developers or third party extension providers to whitelist their inline scripts. This setting must NOT be left on 'YES' permanently, as it significantly increases the risk of security vulnerabilities, making your site an easy target for attackers. Always prioritise the security of your site and user data.

CSP Reports Grid

The CSP Reports Grid collects and displays all the CSP errors on both frontend and backend. To enable report collection please make sure to add the following URLs in *Security > CSP* section of your Store config:-

- **Admin Default** - https://BASE_URL/scommercereporturi/report/admin
- **Storefront** Default**** - https://BASE_URL/scommercereporturi/report/storefront

Configuration

Scope: Default Config ? Save Config

GENERAL ▼ Mode ⌵

SECURITY ▲

Content Security Policy (CSP)

Security.txt

Google reCAPTCHA Admin Panel

Google reCAPTCHA Storefront

CATALOG ▼

⌵ Admin Default

Report URI [store view] URI to report CSP violations in admin area. Used for all admin pages that don't have own URI configured above.

⌵ Storefront Default

Report URI [store view] URI to report CSP violations on storefront. Used for all storefront pages that don't have own URI configured above.

To access the grid go to Admin>System>Scommerce CSP Records> CSP Report Only Grid

Filters

Actions	11 records found		20 per page	1 of 1		
ID	Blocked URL	Report Type	Source URLs	Policy violation	Last report date	
<input type="checkbox"/>	902	https://www.google.com/pagead/landing?gcs=G111&gcd=13r3r3r3r5l1&tag_exp=0&rnd=852104419.1727279261&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2F&dma=0&npa=0>m=45He49n0n71PTN7FNv727398892a200&aid=108111819.1727170941	Store Front	https://qa2.scommerce-mage.co.uk/	connect-src	2024-09-25 15:47:48
<input type="checkbox"/>	903	https://www.google.com/pagead/landing?gcs=G111&gcd=13t3t3t3t5l1&tag_exp=0&rnd=880174514.1727279267&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2Fmen%2Ftops-men%2Fjackets-men.html&dma=0&npa=0>m=45He49n0n71PTN7FNv727398892a200&aid=108111819.1727170941	Store Front	https://qa2.scommerce-mage.co.uk/men/tops-men/jackets-men.html	connect-src	2024-09-25 15:47:52
<input type="checkbox"/>	904	https://pagead2.googleadsyndication.com/pagead/landing?gcs=G100&gcd=13p3p3p3p5l1&tag_exp=101671035-101747727&rnd=1081916902.1727327762&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2F&dma_cps=&dma=0&npa=1>m=45He49n0n71PTN7FNv727398892a200	Store Front	https://qa2.scommerce-mage.co.uk/	connect-src	2024-09-26 05:16:05
<input type="checkbox"/>	905	https://pagead2.googleadsyndication.com/pagead/landing?gcs=G100&gcd=13p3p3p3p5l1&tag_exp=101671035-101747727&rnd=30621933.1727327770&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2Fcollections%2Fyoga-new.html&dma_cps=&dma=0&npa=1>m=45He49n0n71PTN7FNv7273988	Store Front	https://qa2.scommerce-mage.co.uk/collections/yoga-new.html	connect-src	2024-09-26 05:16:15
<input type="checkbox"/>	906	https://pagead2.googleadsyndication.com/pagead/landing?gcs=G100&gcd=13p3p3p3p5l1&tag_exp=101671035-101747727&rnd=43187354.1727327782&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2Ffiona-fitness-short.html&dma_cps=&dma=0&npa=1>m=45He49n0n71PTN7FNv727398892a	Store Front	https://qa2.scommerce-mage.co.uk/fiona-fitness-short.html	connect-src	2024-09-26 05:16:24

- **ID:-** Id of the record
- **Blocked URL:-** The URL reported in the CSP error
- **Report Type:-** Store Front (frontend) or Admin(backend), where the error was reported
- **Source URLs:-** The Source URL of the page where this error was reported
- **Policy violation:-** The CSP directive which was violated in this record.
- **Last report date:-** When was this error last reported.

Working of the extension

Steps to Check and Fix Console CSP Errors thurgh CSP Reports Grid

Go to Admin>System>Scommerce CSP Records> CSP Report Only Grid, select the error records that you want to whitelist then from the Actions dropdown, select whitelist.

Filters

Actions	11 records found (4 selected)		20 per page	1 of 1		
ID	Blocked URL	Report Type	Source URLs	Policy violation	Last report date	
<input checked="" type="checkbox"/>	902	https://www.google.com/pagead/landing?gcs=G111&gcd=13r3r3r3r5l1&tag_exp=0&rnd=852104419.1727279261&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2F&dma=0&npa=0>m=45He49n0n71PTN7FNv727398892a200&aid=108111819.1727170941	Store Front	https://qa2.scommerce-mage.co.uk/	connect-src	2024-09-25 15:47:48
<input checked="" type="checkbox"/>	903	https://www.google.com/pagead/landing?gcs=G111&gcd=13t3t3t3t5l1&tag_exp=0&rnd=880174514.1727279267&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2Fmen%2Ftops-men%2Fjackets-men.html&dma=0&npa=0>m=45He49n0n71PTN7FNv727398892a200&aid=108111819.1727170941	Store Front	https://qa2.scommerce-mage.co.uk/men/tops-men/jackets-men.html	connect-src	2024-09-25 15:47:52
<input checked="" type="checkbox"/>	904	https://pagead2.googleadsyndication.com/pagead/landing?gcs=G100&gcd=13p3p3p3p5l1&tag_exp=101671035-101747727&rnd=1081916902.1727327762&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2F&dma_cps=&dma=0&npa=1>m=45He49n0n71PTN7FNv727398892a200	Store Front	https://qa2.scommerce-mage.co.uk/	connect-src	2024-09-26 05:16:05
<input checked="" type="checkbox"/>	905	https://pagead2.googleadsyndication.com/pagead/landing?gcs=G100&gcd=13p3p3p3p5l1&tag_exp=101671035-101747727&rnd=30621933.1727327770&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2Fcollections%2Fyoga-new.html&dma_cps=&dma=0&npa=1>m=45He49n0n71PTN7FNv7273988	Store Front	https://qa2.scommerce-mage.co.uk/collections/yoga-new.html	connect-src	2024-09-26 05:16:15
<input type="checkbox"/>	906	https://pagead2.googleadsyndication.com/pagead/landing?gcs=G100&gcd=13p3p3p3p5l1&tag_exp=101671035-101747727&rnd=43187354.1727327782&url=https%3A%2F%2Fqa2.scommerce-mage.co.uk%2Ffiona-fitness-short.html&dma_cps=&dma=0&npa=1>m=45He49n0n71PTN7FNv727398892a	Store Front	https://qa2.scommerce-mage.co.uk/fiona-fitness-short.html	connect-src	2024-09-26 05:16:24

Please clear caches as prompted:-

A total of 4 record(s) have been whitelisted. Please Flush Magento Cache.

7 records found (4 selected)

20 per page 1 of 1

Actions	Report Type	Source URLs	Policy violation	Last report date
<input checked="" type="checkbox"/> 906 Whitelist Delete	Store Front	https://qa2.scommerce-mage.co.uk/fiona-fitness-short.html	connect-src	2024-09-26 05:16:24
<input checked="" type="checkbox"/> 907	Store Front	https://qa2.scommerce-mage.co.uk/	connect-src	2024-09-26 05:16:42
<input checked="" type="checkbox"/> 908	Store Front	https://qa2.scommerce-mage.co.uk/collections/yoga-new.html	img-src	2024-09-26 05:17:15
<input checked="" type="checkbox"/> 909	Store Front	https://qa2.scommerce-mage.co.uk/collections/yoga-new.html	connect-src	2024-09-26 05:17:15

Once done all the selected entries will be whitelisted into their specific CSP directive and should be visible in the admin configuration.

Connect Src

Enabled (store view) Yes Use system value

This setting will be used to enable or disable csp whitelist for connect-src
 Defines the sources that can be loaded using script interfaces.

URL/HASH	Type	Action
<input type="text" value="bat.bing.com"/>	<input type="text" value="host"/>	<input type="button" value="Delete"/>
<input type="text" value="ct.pinterest.com"/>	<input type="text" value="host"/>	<input type="button" value="Delete"/>
<input type="text" value="pixel-config.reddit.com"/>	<input type="text" value="host"/>	<input type="button" value="Delete"/>
<input type="text" value="tczinyq.euv.stape.io"/>	<input type="text" value="host"/>	<input type="button" value="Delete"/>
<input type="text" value="www.google.com"/>	<input type="text" value="host"/>	<input type="button" value="Delete"/>
<input type="text" value="www.redditstatic.com"/>	<input type="text" value="host"/>	<input type="button" value="Delete"/>
<input type="text" value="pagead2.google syndication.com"/>	<input type="text" value="host"/>	<input type="button" value="Delete"/>
<input type="button" value="Add Record"/>		

Please add URLs that you want to whitelist

Activate Windows
Go to Settings to activate Windows.

Note:- If you have already whitelisted the entries manually in the configuration then you can delete these records from the grid by selection the records that you want to delete and then click on Action dropdown and select delete.

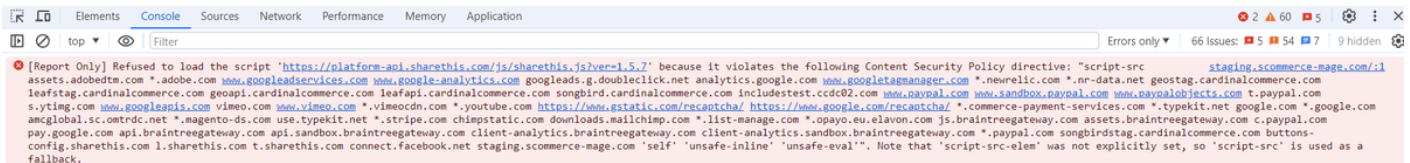
7 records found (3 selected)

20 per page 1 of 1

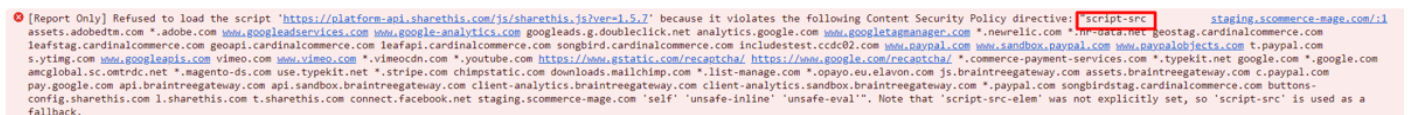
Actions	Report Type	Source URLs	Policy violation	Last report date
<input checked="" type="checkbox"/> 906 Whitelist Delete	Store Front	https://qa2.scommerce-mage.co.uk/fiona-fitness-short.html	connect-src	2024-09-26 05:16:24
<input checked="" type="checkbox"/> 907	Store Front	https://qa2.scommerce-mage.co.uk/	connect-src	2024-09-26 05:16:42
<input checked="" type="checkbox"/> 908	Store Front	https://qa2.scommerce-mage.co.uk/collections/yoga-new.html	img-src	2024-09-26 05:17:15

Steps to Check and Fix Console CSP Errors Manually

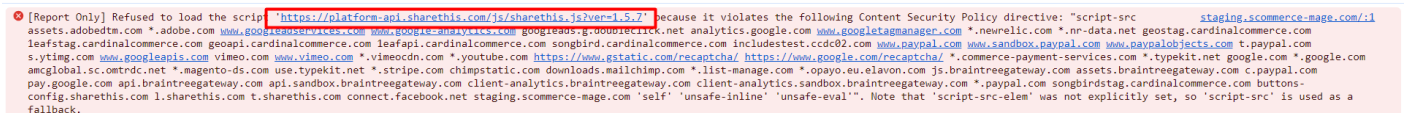
- Check the errors present in the frontend's console.



- Check the source of these errors.



- Check the URL present in these errors.

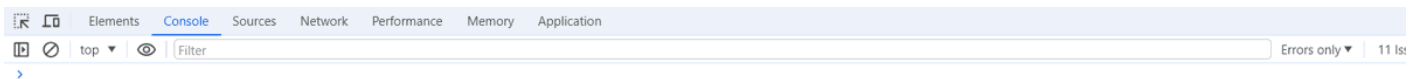


- In the backend, add the URL to the source to which that error belongs to.

Whitelist entries
[store view]

URL	Type	Action
<input type="text" value="buttons-config.sharethis.com"/>	host	
<input type="text" value="l.sharethis.com"/>	host	
<input type="text" value="t.sharethis.com"/>	host	
<input type="text" value="connect.facebook.net"/>	host	
<input type="text" value="https://platform-api.sharethis.cc"/>	host	
<input type="button" value="Add Record"/>		

- You would no longer see the error on the frontend



Fixing Inline Script and Inline Style Content Security Policy Issues

In this section, we will show you how to fix the inline script and style related console errors for Content Security Policy. Please check the image below:



- Identify the script or style tag that's causing the console error.
- Create SHA256 hash of contents of with the script or style tag and then use bas64 to encode this hash. It can be done all together :- <https://emn178.github.io/online-tools/sha256.html>
- Alternatively you can generate the hash using PHP as shown below.

```
$whitelistHash = base64_encode(hash('sha256', $content, true));
```

- Next we add this hash to our module in the correct section i.e either style or script.

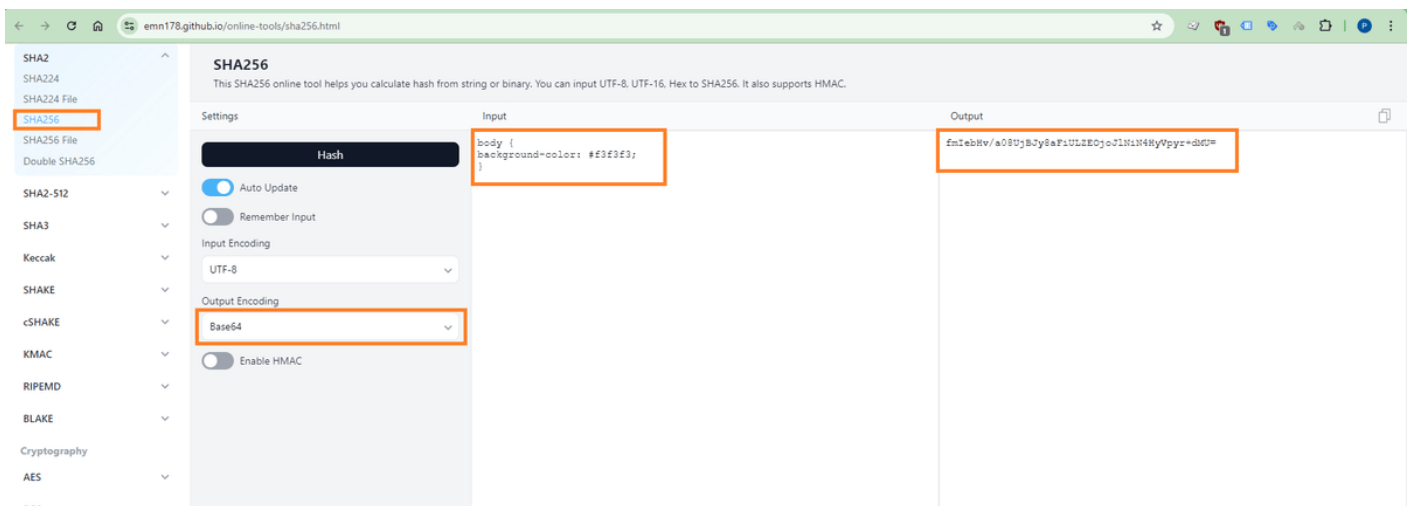
Let us look at examples to understand this process better:

Inline Style Error Example

- Suppose we identified the style thats causing the issue as follows:

```
<style>
body {
background-color: #f3f3f3;
}
</style>
```

- Next we will go the site and create a SHA256 hash as well as the base64 encode of this hash of the contents of the style tag as shown in screengrab below:



- Now copy this hash and go to **Stores>Configuration>Scommerce Configuration>CSP Whitelist** and scroll down to find the **Style Src** section. Add the hash here as shown in the image below:

Style Src



Enabled
[store view]

Yes

Use system value

This setting will be used to enable or disable csp whitelist for style-src
Defines the sources for stylesheets.

Whitelist entries
[store view]

URL/HASH	Type	Action
<input type="text" value="lovcoObfHv0RELo8jMY/7tQivhjTj"/>	<input type="text" value="hash"/>	
<input type="button" value="Add Record"/>		

Please add URLs or HASH that you want to whitelist

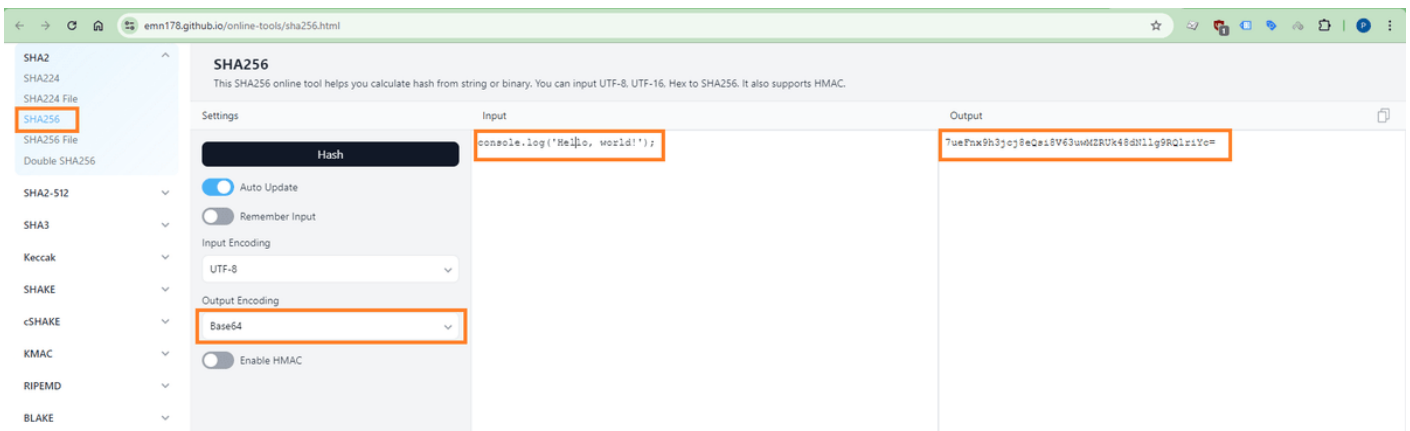
- Please make sure hash is selected in the type dropdown. This should resolve the console error.

Inline Script Error Example

- The identified script tag causing the issue is as follows:

```
<script>  
console.log('Hello, world!');  
</script>
```

- We will go the site(<https://emn178.github.io/online-tools/sha256.html>) and create a SHA256 hash as well as the base64 encode of this hash of the contents of the style tag as shown in screengrab below:



- Now copy this hash and go to **Stores>Configuration>Scommerce Configuration>CSP Whitelist** and scroll down to find the **Script Src** section. Add the hash here as shown in the image below:

Script Src



Enabled
[store view]

Yes



Use system value

This setting will be used to enable or disable csp whitelist for script-src
Defines the sources for JavaScript **script** HTML elements.

Whitelist entries
[store view]

URL/HASH	Type	Action
<input type="text" value="Pq3KG9KpfoqxdFBPx9qXjjawgSz"/>	<input type="text" value="hash"/>	
<input type="button" value="Add Record"/>		

Please add URLs or HASH that you want to whitelist

- Please make sure hash is selected in the type dropdown. This should resolve the console error.

If you have a question related to this extension please check out our **FAQ Section** first. If you can't find the answer you are looking for then please contact **support@scommerce-mage.com**.

Revision #6

Created 12 May 2025 11:40:41 by scommerce

Updated 24 October 2025 09:42:44 by scommerce