

Dokumentation Configurable CSP (v2.x)

Beschreibung

Das Modul Configurable CSP ermöglicht es, bestimmte URLs oder Ressourcen über die Konfiguration in der CSP (Content Security Policy) von Magento zuzulassen.

Warum Configurable CSP?

Dieses Modul könnte für techdivision/tracking-google-analytics-4 notwendig sein.

Es ermöglicht, CSP-Einstellungen über die Konfiguration festzulegen. Es ist keine Bereitstellung neuer CSP-XML-Dateien erforderlich.

Was ist CSP?

Die Content Security Policy (CSP) ist ein Sicherheitskonzept zur Vermeidung von Cross-Site-Scripting und anderen Angriffen, die durch das Einspeisen von Daten in Webseiten erfolgen. Sie ist eine von der W3C empfohlene Richtlinie für die Sicherheit von Webanwendungen. CSP wurde ursprünglich von der Mozilla Foundation entworfen und erstmals experimentell in Firefox 4.0 unterstützt.

Funktionsmerkmale

Funktion	Beschreibung
URLs zur Content Security Policy hinzufügen	Um bestimmte URLs zu erlauben, können diese im Backend in das CSP-Mapping eingetragen werden.
URL Hashes zur Content Security Policy hinzufügen	Um bestimmte Hashes zu erlauben, können diese im Backend in das CSP-Mapping eingetragen werden.
Report-Only Funktion	Erweiterung der Magento Konfigurationseinstellungen um CSP-Verletzungen nur zu reporten und nicht blockieren
CSP Reporting	API Funktion und Backend-Ansicht um CSP-Verletzungen aufzulisten

Contributors

Patrick Mehringer	p.mehringer@techdivision.com	Developer / Maintenance
Kenza Yamlaoui	k.yamlaoui@techdivision.com	Developer / Maintenance
Josef Kaffl	j.kaffl@techdivision.com	Documentation

Requirements / Installation

Magento Version Compatibility

Magento Version	Latest Version
Magento >= 2.4.4 Commerce (CE/EE)	<code>composer require techdivision/configurable-csp ^2.0.0</code>

PHP Version

Compatible zu PHP Version PHP 8.1 / PHP 8.2 / PHP 8.3

Installation mit Composer

- Um im **TechDivision** Context ein Modul mittels Composer zu installieren, bitte per folgenden Befehl das Repo entsprechend einbinden

```
composer config repositories.repo.met.tdintern.de composer https://repo.met.tdintern.de/
```

Modul Installationsbefehle

- Nach Einbindung des **MET-Composer-Repository** folgende Befehle zur Installation ausführen

```
# add to composer require
composer require techdivision/configurable-csp ^2.0.0

# run magento setup to activate the module
bin/magento set:up
```

Deinstallation

Folgende Punkte sind bei einer Deinstallation eines Moduls stets zu beachten:

- Gibt es Einträge in der Datenbank, die vor der Deinstallation bereinigt werden müssen?
- Sind evtl. Medien-Dateien (Bilder, Videos ect.) vorhanden, die vorab gelöscht werden müssen?
- Gibt es Konfigurationspfade in der Konfiguration (DB), die entfernt werden müssen?
- Müssen Zwischenspeicher (Caches) geleert werden?
- Müssen Indizes (Magento_Indexer) erneuert werden?

```
# uninstall Module  
bin/magento module:uninstall techdivision/configurable-csp
```

Configurable Csp Optionen

Navigieren Sie zu **Techdivision >> Configurable CSP**

Section	Option	Value	Default	Beschreibung
Configurable Content Security Policies	CSP-Mapping	Map	Null	Map von URLs zu CSP-Typen.

Configurable Content Security Policies



Module Version 1.2.2
[website]

CSP Mapping
[global]

CSP - ID	Type	Value	Action
base-uri	host		
Add Mapping			

☐ Use system value

Nach **Stores > Configuration > Security > Content Security Policy CSP** navigieren

- report urls für das report grid setzen
- report only gibt an ob nur reports gesendet werden oder ob die url auch gesperrt wird

Section	Option	Value	Default	Beschreibung
Admin Default	Report Uri	Null	Null	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	Null	Null	URI to report CSP violations on storefront. Used for all storefront pages that don't have own URI configured above.
Admin > Create Order	Report Uri	Null	Null	If empty, Default Report URI for admin area will be used.
Storefront > One Page Checkout	Report Uri	Null	Null	If empty, Default Report URI for storefront will be used.

- Beispiel Konfiguration für Report UrIs

Configuration

   admin ▾

Scope: Default Config ▾ ?

Save Config

GENERAL ▾

SECURITY ▴

Content Security Policy (CSP)

Security.txt

Google reCAPTCHA Admin Panel

Google reCAPTCHA Storefront

CATALOG ▾

CUSTOMERS ▾

SALES ▾

ADOBE SERVICES ▾

Mode



⌵ 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.

Report Only
[store view] ▾☒ Use system value

PCI v4 specs require value "No" from 31/03/2025.

⌵ 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.

Report Only
[store view] ▾☐ Use system value

PCI v4 specs require value "No" from 31/03/2025.

Bedienungsanleitung Modul-Funktionen

CSP Mapping

- Im Backend nach [TechDivision](#) > [Configurable CSP](#) > [CSP Mapping](#) navigieren.
- Url zum Mapping hinzufügen

Configurable Content Security Policies



Module Version 1.2.2
[website]

CSP Mapping
[global]

CSP - ID	Type	Value	Action
base-uri	host		
<button>Add Mapping</button>			

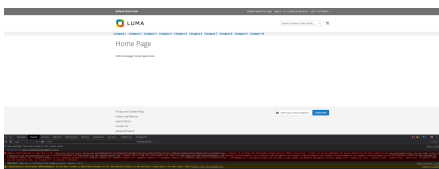
☐ Use system value

Die hinzugefügte URL wird automatisch zur Content Security Policy (CSP) hinzugefügt. Dies ermöglicht es, dass Ressourcen von dieser URL geladen werden dürfen. Bitte prüfen Sie jede URL sorgfältig bevor Sie sie freigeben, ansonsten kann dies zu Sicherheitsrisiken führen.

Beispiel

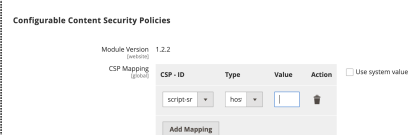
Standard

Ausgangspunkt sind die Fehlermeldungen bzgl. CSP-Verstößen in der Browser-Console:



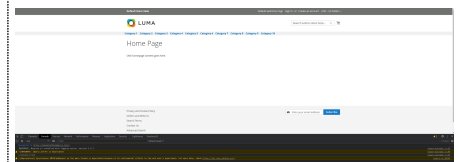
Konfiguration

Pflegen Sie nun die gewünschten Ressourcen für die Freigabe in der Magento CSP:



Ausgabe

Die Ressourcen werden akzeptiert und es werden keine CSP-Verstöße mehr gemeldet.



CSP Modus

Standardmäßig ist es in Adobe Commerce nicht möglich den Modus von CSPs einzustellen. Mit dem Modul Configurable CSP werden Backend-Konfigurationen für diese Standard-Optionen angeboten.

Configuration Search admin

Scope: Default Config ? Save Config

GENERAL

SECURITY

Content Security Policy (CSP)

Security.txt

Google reCAPTCHA Admin Panel

Google reCAPTCHA Storefront

CATALOG

ELASTICSUITE

CUSTOMERS

SALES

ADOBE SERVICES

TECHDIVISION

PACEMAKER

SERVICES

ADVANCED

AMASTY EXTENSIONS

Mode

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.

Report Only (store view)

Yes

Use system value

PCI v4 specs require value "No" from 31/03/2025.

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.

Report Only (store view)

Yes

Use system value

PCI v4 specs require value "No" from 31/03/2025.

Admin > Create Order

Report URI (store view)

If empty, Default Report URI for admin area will be used.

Report Only (store view)

Yes

Use system value

PCI v4 specs require value "No" from 31/03/2025.

Storefront > One Page Checkout

Report URI (store view)

If empty, Default Report URI for storefront will be used.

Report Only (store view)

Yes

Use system value

PCI v4 specs require value "No" from 31/03/2025.

WARNING

Bitte beachten Sie, dass ab 31.03.2025 der Report-Only-Modus nach PCI DSS v4.0 nicht mehr zulässig ist.

CSP Reports

Das Modul bietet eine Api-Schnittstelle, welche die CSP-Verletzungen speichert, um sie so prüfen und ggf. freigeben zu können.

1. Dazu muss die Api-URL im Backend unter **Stores >> Configuration >> Security >> CSP** bei den jeweiligen Einstellungsmöglichkeiten eingetragen werden.

Configuration

Save Config

GENERAL

SECURITY

Content Security Policy (CSP)

Security.txt

Google reCAPTCHA Admin Panel

Google reCAPTCHA Storefront

CATALOG

ELASTICSUITE

CUSTOMERS

SALES

ADOBE SERVICES

TECHDIVISION

PACEMAKER

SERVICES

ADVANCED

AMASTY EXTENSIONS

Mode

Admin Default

Storefront Default

Admin > Create Order

Storefront > One Page Checkout

Report URI

https://magento247commerce.test/rest/V1/configurable-csp/request

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

Yes

PCI v4 specs require value "No" from 31.03/2025.

Use system value

Report URI

https://magento247commerce.test/rest/V1/configurable-csp/request

URI to report CSP violations on storefront, Used for all storefront pages that don't have own URI configured above.

Yes

PCI v4 specs require value "No" from 31.03/2025.

Use system value

Report URI

https://magento247commerce.test/rest/V1/configurable-csp/request

If empty, Default Report URI for admin area will be used.

Yes

PCI v4 specs require value "No" from 31.03/2025.

Use system value

Report URI

https://magento247commerce.test/rest/V1/configurable-csp/request

If empty, Default Report URI for storefront will be used.

Yes

PCI v4 specs require value "No" from 31.03/2025.

Use system value

Copyright © 2025 Adobe. All rights reserved.

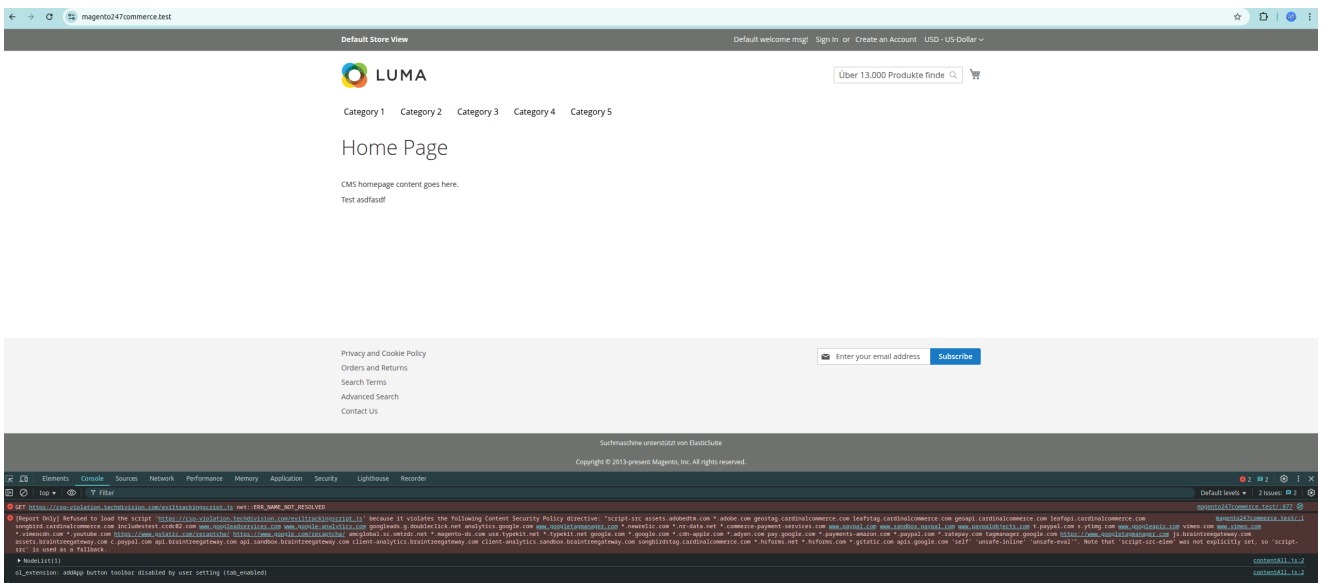
ElasticSuite

Open Source ver. 2.11.9.2 (on elasticsearch ver. 7.7.0)

Magento 2.4.7

Adobe Commerce ver. 2.4.7-p3

2. Wird eine Frontend-Seite mit einem nicht erlaubten Script aufgerufen, so wird die CSP-Verletzung an die Api gesendet und diese speichert nun die Informationen ab. Es werden keine Verletzungen mehrfach gespeichert.



3. Im Backend sind die CSP-Verletzungen unter **TechDivision >> Configurable CSP Reports** einsehbar.

Configurable CSP Reports

Clear Reports

Filters Default View Columns

1 records found 20 per page 1 of 1

ID	Disposition	Blocked Url	Effective Directive	Original Policy	Remove
3	report	https://csp-violation.techdivision.com/newtrackingscript.js	script-src:elem	expand	remove

Copyright © 2025 Adobe. All rights reserved.

Adobe Commerce ver. 2.4.7-p3
ElasticSuite Open Source ver. 2.11.9.2 (on elasticsearch ver. 7.7.0)
[Privacy Policy](#) | [Account Activity](#) | [Report an Issue](#)

Glossar

Begriff	Beschreibung
*xxx	XXXXXX XXXXX