



Dokumentation Restrict Frontend (v2.x)

Beschreibung

Das Modul RestrictFrontend ermöglicht es, den Frontend-Zugriff auf bestimmte Store Views mit einer IP Whitelist einzuschränken.

Dies kann hilfreich sein, wenn ein neuer Shop in einer bestehenden eCommerce-Plattform erstellt wird, da es Redakteuren ermöglicht, ihre Änderungen im Frontend einzusehen, ohne dass tatsächliche Kunden während der laufenden Arbeit im Shop unterwegs sind.

Funktionsmerkmale

Funktion	Beschreibung
IP-Whitelist	Die IP-Whitelist unterstützt sowohl einzelne IPs als auch IP-Bereiche , die in der CIDR-Notation
Unterstützte Standards	Es werden IPv4 und IPv6 unterstützt

Contributors

Jens Scherbl	j.scherbl@techdivision.com	Developer
Jean-Bernard Valentaten	j.valentaten@techdivision.com	Developer
Martin Eisenführer	m.eisenfuehrer@techdivision.com	Maintenance
Ludwig Mair	l.mair@techdivision.com	Documentation
Kenza Yamlahi	k.yamlahi@techdivision.com	Maintenance

Requirements / Installation

Magento Version Compatibility

Magento Version	Latest Version
Magento < = 2.4.0 Opensource (CE) / Commerce (EE)	<code>composer require techdivision/restrict-frontend ^2.2.0</code>
Magento < = 2.3.1 Opensource (CE) / Commerce (EE)	<code>composer require techdivision/restrict-frontend ^1.1.2</code>
Magento < = 2.2.8 Opensource (CE) / Commerce (EE)	<code>composer require techdivision/restrict-frontend</code>

PHP Version

Kompatibel zu PHP Version `~7.3.0 || ~7.4.0`

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/restrict-frontend ^2.2.0

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

Aktivieren des Moduls

Das Modul **Lazyload** ist standardmäßig nach der Installation im Magento Backend verfügbar.

TIP

TechDivision >> Util >> Restrict Frontend

Die Modulfunktionalität ist initial deaktiviert!

Deinstallation

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

- Gibt es Einträge in der Datenbank, die vor dem Deinstallieren bereinigt werden müssen?
- Sind evtl. Media Files (Images, Videos ect.) vorhanden, die vorab bereinigt werden müssen?
- Gibt es Konfigurationspfade in der Config (DB), die entfernt werden müssen?
- Caches entleeren
- Indexer neu starten wenn notwendig

```
# uninstall Module  
bin/magento module:uninstall techdivision_restrict-frontend
```

Modul Konfiguration

Navigieren Sie zu [TECHDIVISION >> UTIL >> Restrict Frontend](#)

Section	Option	Value	Scope	Beschreibung
General	Enabled	No	store view	Aktivieren/Deaktivieren der Frontend-Einschränkung des <i>aktuellen</i> Scopes
	Allowed IP addresses		store view	Definiert die durch Zeilenumbrüche getrennten White-List-IPs
	CMS page	404 Not Found	store view	Definiert die Frontend-Seite, die bei Anfragen von nicht whitelisted IPs ausgeliefert wird.
Logging	Enabled	No	store view	Protokollierung aktivieren/deaktivieren

The screenshot shows the 'Configuration' page for 'Restrict Frontend'. On the left is a vertical sidebar with navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, TechDivision, Stores, System, and Find Partners & Extensions. The main content area is titled 'Configuration' and includes a search icon, a notification bell with '6', and a user profile 'admin'. Below this is a 'Store View' dropdown set to 'Default Config' and a 'Save Config' button. The configuration is divided into sections: 'General' and 'Logging'. Under 'General', there are three settings: 'Enabled' (set to 'No'), 'Allowed IP addresses' (empty text area), and 'CMS page' (set to 'Privacy and Cookie Policy'). Each setting has a 'Use system value' checkbox. The 'Logging' section is partially visible at the bottom.

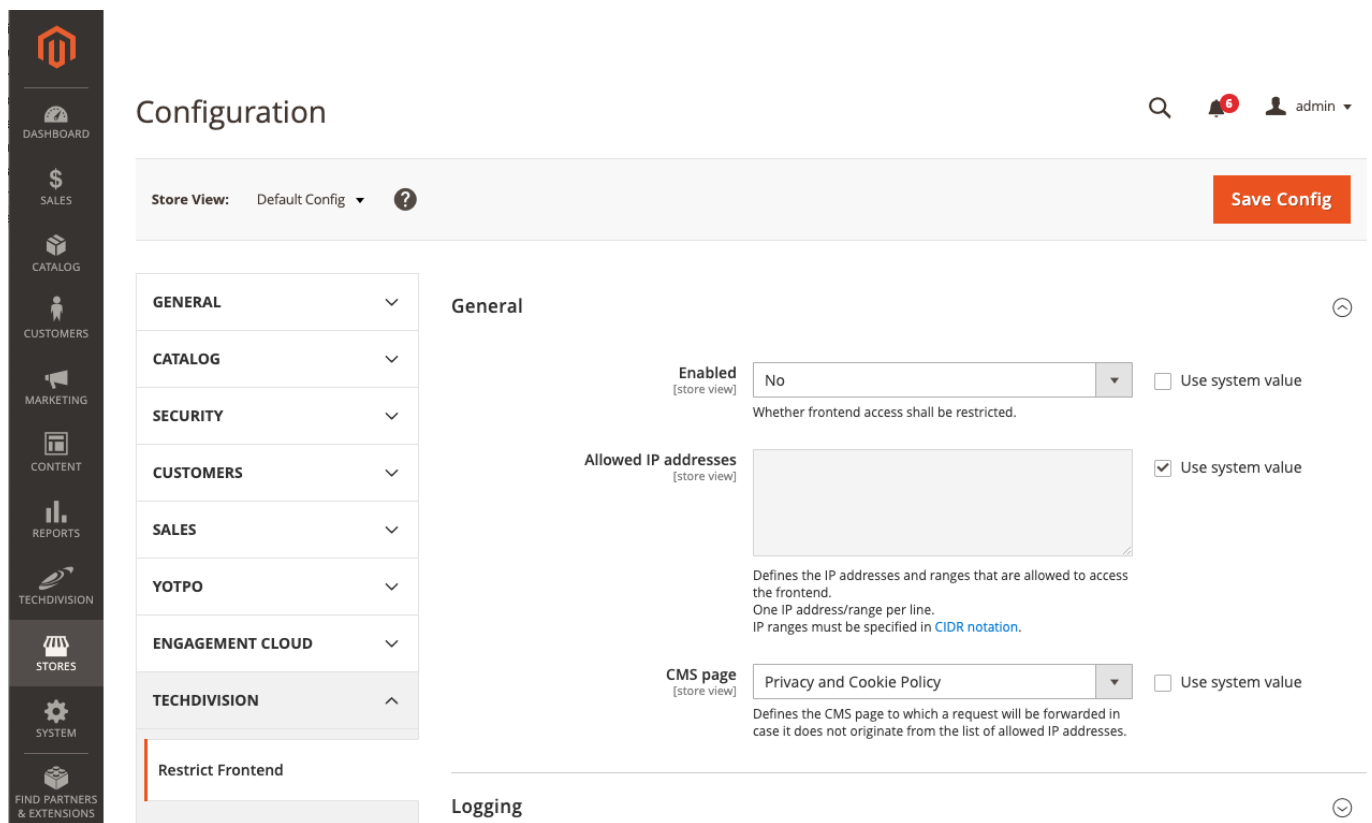
Bedienungsanleitung Modul-Funktionen

Modul-Installation und -Konfiguration

- [Installation des Moduls](#)
- [Konfigurationseinstellungen des Moduls](#)

Einstellen der erforderlichen Default/Storeview Optionen

- Navigieren Sie zu [TECHDIVISION >> Util >> Restrict Frontend](#)
- **Restrict Frontend** unter **Default Config** aktivieren
- Falls Default Einstellungen gesetzt werden müssen, die global gelten, diese bitte unter **Default Config** einstellen



The screenshot shows the Magento configuration interface for the 'Restrict Frontend' module. The left sidebar contains navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Techdivision, Stores, System, and Find Partners & Extensions. The main content area is titled 'Configuration' and shows the 'Default Config' for the 'Restrict Frontend' module. The 'General' section is expanded, showing three settings:

- Enabled [store view]:** A dropdown menu is set to 'No'. Below it, the text reads: 'Whether frontend access shall be restricted.' There is an unchecked checkbox for 'Use system value'.
- Allowed IP addresses [store view]:** A text area is empty. Below it, the text reads: 'Defines the IP addresses and ranges that are allowed to access the frontend. One IP address/range per line. IP ranges must be specified in [CIDR notation](#).' There is a checked checkbox for 'Use system value'.
- CMS page [store view]:** A dropdown menu is set to 'Privacy and Cookie Policy'. Below it, the text reads: 'Defines the CMS page to which a request will be forwarded in case it does not originate from the list of allowed IP addresses.' There is an unchecked checkbox for 'Use system value'.

At the top right of the configuration area, there is a 'Save Config' button. The 'Store View' is set to 'Default Config'.

- Zur gewünschten **Store View** wechseln

- **Restrict Frontend** in **Store View** aktivieren
- Unter **Allowed IP addresses** die erlaubten **IP** Adressen eingeben

CAUTION | Je **IP** Adresse nur eine Zeile verwenden

- Unter **CMS page** die Page einstellen, worauf umgeleitet wird, falls nicht in der erlaubten **IP Whitelist** enthalten

Referenzen

Hilfreiche Links zu Tutorials, Manuals und allgemeinen Infos

- [CIDR-Notation](#)
- [Unterschied zu **ipv4** vs. **ipv6**](#)