



Dokumentation Restrict Frontend (v2.1)

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.x Opensource (CE) / Commerce (EE)	composer require techdivision/restrict-frontend
Magento < = 2.3.x Opensource (CE) / Commerce (EE)	composer require techdivision/restrict-frontend

PHP Version

Kompatibel zu PHP Version **>=7.3**

Installation mit Composer

Um im TechDivision Context ein Modul mittels Composer zu installieren, bitte per Befehl das Repo 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

```
composer require techdivision/restrict-frontend ~2.1.0  
  
bin/magento set:up
```

Aktivieren des Moduls

TIP

Das Modul ist bei Default nach der Installation im Magento Backend aktiviert, das bedeutet, dass das Modul nun im Backend sichtbar ist und zur weiteren Konfiguration bereit steht.

Deinstallation

Modul Deinstallationsbefehl

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 [menu:\[TECHDIVISION > UTIL > \[Restrict Frontend \] \]](#)
- Nehme Sie die benötigten Einstellung vor

Section	Option	Value	Scope	Beschreibung
General	Enabled	No	store view	Enable/Disable ermöglicht Frontend-Einschränkung des <i>aktuellen Scopes</i>
	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. <ul style="list-style-type: none"> • Protokolliert Hinweise in der Datei restrict-frontend.log. • Geloggt wird jeweils eine Notice Message, falls jemand versucht eine geblockte IP aufgerufen. oder wenn eine URL/Domain nicht zulässig ist.

- [\[Save Config \]](#)

The screenshot shows the 'Configuration' page in a Magento 2 admin interface. 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 shows the 'Restrict Frontend' configuration for the 'Default Config' store view. A 'Save Config' button is visible in the top right of the configuration area.

Configuration Summary:

- Enabled (store view):** No. Whether frontend access shall be restricted. Use system value.
- Allowed IP addresses (store view):** (Empty text area). 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](#). Use system value.
- CMS page (store view):** Privacy and Cookie Policy. Defines the CMS page to which a request will be forwarded in case it does not originate from the list of allowed IP addresses. Use system value.

Logging

Manual

Initiale Modul Konfiguration nach Installation

- Die Initiale Installation ist erfolgt
- Das Modul ist im Backend aktiv und enabled
- Auswählen der erforderlichen allgemeinen und storeview spezifischen Optionen
- Einstellen der erforderlichen Default/Storeview Optionen

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 displays the Magento 2 Configuration interface for the 'Restrict Frontend' module. On the left, a vertical sidebar contains navigation icons for various system areas. The main configuration area is titled 'Configuration' and shows the 'Restrict Frontend' settings for the 'Default Config' store view. The 'General' section is expanded, revealing three configuration options: 'Enabled' (a dropdown menu set to 'No'), 'Allowed IP addresses' (a text area), and 'CMS page' (a dropdown menu set to 'Privacy and Cookie Policy'). Each option has a 'Use system value' checkbox. A 'Save Config' button is located in the top right corner of the configuration area.

- Zur gewünschten **Store View** wechseln

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

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

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

Referenzen

Hilfreiche Links zu Tutorials, Manuals und allgemeinen Infos

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