



Dokumentation Restrict Frontend (v3.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 >= 2.4.4 Commerce (CE/EE)	composer require techdivision/restrict-frontend ^3.2.0
Magento < = 2.4.0 Opensource (CE) / Commerce (EE)	composer require techdivision/restrict-frontend ^2.2.0
Magento < = 2.3.1 Opensource (CE) / Commerce (EE)	composer require techdivision/restrict-frontend ^1.1.2
Magento < = 2.2.8 Opensource (CE) / Commerce (EE)	composer require techdivision/restrict-frontend

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/restrict-frontend ^3.2.0

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

Aktivieren des Moduls

TIP

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

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 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/deaktivieren

- DASHBOARD
- SALES
- CATALOG
- CUSTOMERS
- MARKETING
- CONTENT
- REPORTS
- TECHDIVISION
- STORES
- SYSTEM
- FIND PARTNERS & EXTENSIONS

Configuration

Store View:
Default Config
?
Save Config

GENERAL
CATALOG
SECURITY
CUSTOMERS
SALES
YOTPO
ENGAGEMENT CLOUD
TECHDIVISION
Restrict Frontend

General

Enabled
[store view]

No

Whether frontend access shall be restricted.

☐ Use system value

Allowed IP addresses
[store view]

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](#).

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

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 'Configuration' page for 'Default Config'. On the left is a sidebar with icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, TechDivision, Stores, System, and Find Partners & Extensions. The main content area has a 'Store View' dropdown set to 'Default Config' and a 'Save Config' button. Below this is a list of configuration categories: GENERAL, CATALOG, SECURITY, CUSTOMERS, SALES, YOTPO, ENGAGEMENT CLOUD, and TECHDIVISION. The 'Restrict Frontend' option is highlighted. The 'General' section is expanded, showing settings for 'Enabled' (set to 'No'), 'Allowed IP addresses' (empty), and 'CMS page' (set to 'Privacy and Cookie Policy'). Each setting has a 'Use system value' checkbox.

- Zur gewünschten **Store View** wechseln

This screenshot shows the 'Configuration' page for a specific 'Store View' named 'Store view 3 - website_id_3 - es_ES'. The 'Store View' dropdown in the top bar is open, showing a list of available store views: 'Default Store View de DE', 'Website 2 it_IT', 'Store Group 2 - website_id_2 it_IT', 'Store view 2 - website_id_2 - it_IT', 'Website es_ES', 'Store Group 3 - es_ES', and 'Store view 3 - website_id_3 - es_ES'. The 'General' section is expanded, showing settings for 'Enabled' (set to 'No'), 'Allowed IP addresses' (empty), and 'CMS page' (set to 'Privacy and Cookie Policy'). Each setting has a 'Use Website' checkbox.

- **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

Anwendungsfalls: "Pre-Live eines Stores"

Hier wird einer der häufigsten Anwendungsfälle des Moduls skizziert. Dabei handelt es sich eher um einen Livegang für dedizierte Benutzer oder Gruppen welche per IP-Adresse den Shop besuchen und testen können. Dieses Vorgehen wird oft bei sog. "Länder-Rollouts" genutzt.

TIP

Hier ist der große Vorteil gegeben über einer Base-Auth-Beschränkung die einfache Konfiguration. Man kann einfach im Backend die Restriktion einstellen und wieder aufheben.

Bei einer Base-Auth-Beschränkung müssen die Server-Zugänge verwaltet sein und es bedarf in fast allen Fällen das manuelle Eingreifen eines Systemadministrators.

TIP

Ein weiterer Vorteil ist das partielle Deaktivieren von Shops, wenn z.B. Wartungsarbeiten vorgenommen werden sollen, welche nur gewissen Stores betreffen, oder wenn Dateninhalte nachgepflegt werden müssen.

1. Anlage und Aktivierung eines Stores

Wir ein neuer Store über das Backend oder durch ein neues Deployment einer aktualisierten config.php bzw. env.php angelegt. So kann dieser als Scope in der Konfiguration ausgewählt werden

Stores

← Back Delete Store View Reset Save Store View

Store View Information

Store * Main Website Store

Name * de_DE

Code * de_DE

Status * Enabled

Sort Order 0

2. Limitierung/Beschränkung des Store-Frontends

Nun da der Store angelegt und aktiviert wurde kann es sein das viele Konfigurationen oder Inhalte noch nicht komplett oder sogar fehlerhaft sind. Damit nun dediziert getestet werden kann, ohne das der Store für alle Nutzer aufrufbar ist, kann im Konfigurationsbackend unter **TECHDIVISION >> UTIL >> Restrict Frontend** der Store-Zugriff limitiert werden

- a. Dazu wählt man zuerst den gewünschten Scope aus. Hier der "de_DE"-Store.
- b. Aktiviert das Modul
- c. und setzt die erlaubten IP-Adressen oder IP-Ranges.

Configuration

pat

Scope: de_DE
Save Config

GENERAL
CATALOG
SECURITY
ELASTICSUITE
CUSTOMERS
SALES
YOTPO
DOTDIGITAL
TECHDIVISION
Product Flags
Disable Shopping

General

Enabled
Yes

☐ Use Website

Whether frontend access shall be restricted.

Allowed IP addresses
95.90.195.10

☐ Use Website

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](#).

CMS page
404 Not Found

☒ Use Website

Defines the CMS page to which a request will be forwarded in case it does not originate from the list of allowed IP addresses.

Logging

Enabled
Yes

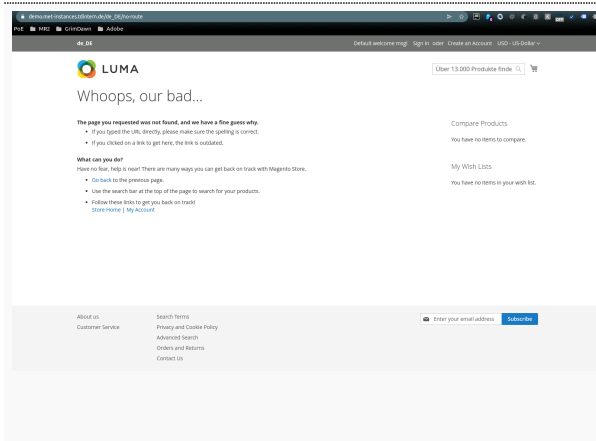
☒ Use Website

3. Verhalten im Frontend

Beschränkter Zugang

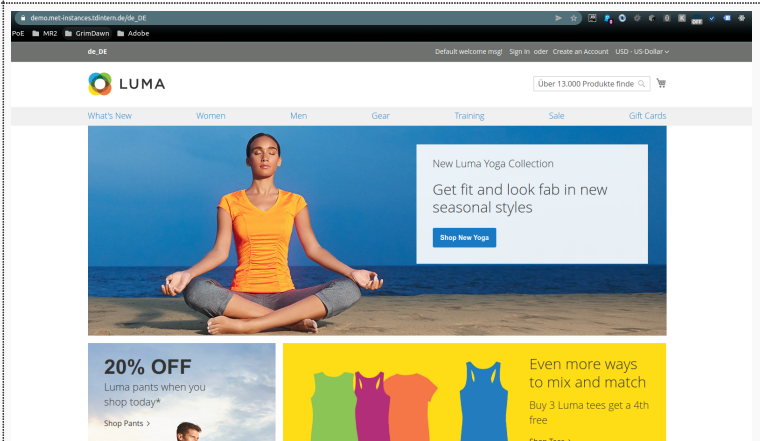
Wenn die IP nicht bei den erlaubten Zugängen vorhanden ist, so wird der Kunde auf die konfigurierte Seite weitergeleitet.

Die hier konfigurierte CMS-Seite ist die "404-Not-Found-Page"



Erlaubter Zugang

Es wird beim Besuch eine Frontend-Seite die Zugriffs-IP ermittelt. Wenn die IP bei den erlaubten Zugängen vorhanden, dann kann der Besucher sich ganz normal im Shop durchnavigieren.



Referenzen

Hilfreiche Links zu Tutorials, Manuals und allgemeinen Infos

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