



# Block Ips

Benutzerhandbuch für PrestaShop

Version 4.3.0 · [stefdevelopment.com](http://stefdevelopment.com)

# Inhaltsverzeichnis

1. [Einführung](#)
2. [Installation und erster Start](#)
3. [Übersicht](#)
4. [Tab IPs](#)
5. [Firewall](#)
6. [Länder](#)
7. [Manuell blockieren / Whitelist](#)
8. [User-Agent sperren](#)
9. [Optionen / Cron](#)
10. [Über / Dokumentation](#)
11. [FAQ](#)
12. [Support](#)

## Einführung

**Block Ips** schützt Ihren PrestaShop-Shop vor unerwünschten Besuchern: missbräuchlichen IP-Adressen, unerwünschten Ländern, Bots mit gefälschten User-Agents und Besuchern, die Ihre Website mit Anfragen überfluten. Alles wird über eine einzige Konfigurationsseite in Ihrem PrestaShop-Backoffice verwaltet – kein Serverzugriff, keine .htaccess -Bearbeitung.

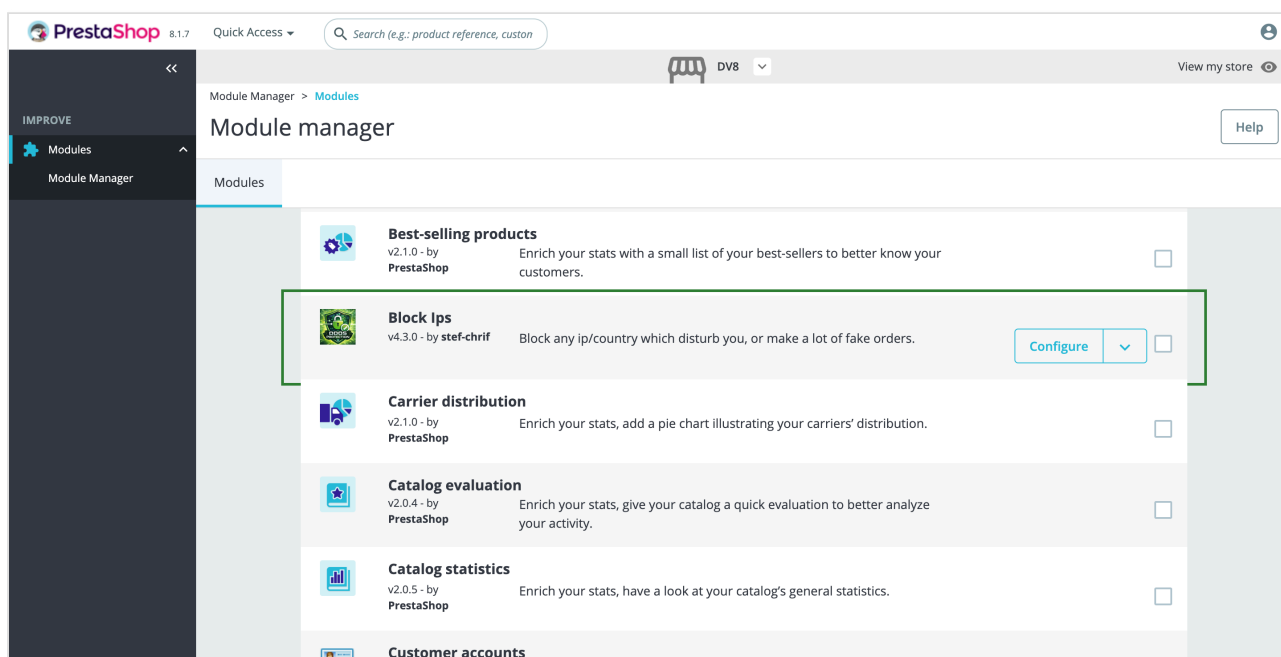
Typische Anwendungsfälle:

- Ein Besucher gibt Dutzende gefälschter Bestellungen auf – blockieren Sie seine IP mit einem Klick.
- Ihr Shop liefert nur innerhalb Europas – blockieren Sie alle anderen Länder auf einmal.
- Ein Scraping-Bot belastet Ihre Produktseiten – stoppen Sie ihn anhand seines User-Agent-Strings.
- Ein Warenkorbabbruch-Muster sieht nach einem Bot aus – die Firewall erkennt ihn automatisch.

Das Modul führt ein detailliertes Besucherprotokoll, damit Sie Blockaden im Lauf der Zeit prüfen und anpassen können, und liefert eine IP-zu-Land-Datenbank (IP2Location) mit, sodass jede angezeigte IP mit einer Länderflagge versehen ist.

## Installation und erster Start

1. Laden Sie das Archiv `blockips.zip` aus Ihrem Kaufbereich auf `stefdevelopment.com` herunter.
2. Öffnen Sie im PrestaShop-Backoffice **Module** → **Modulverwaltung**, klicken Sie auf **Modul hochladen** und wählen Sie die ZIP-Datei aus.
3. Klicken Sie nach der Installation auf der Kachel des Block-Ips-Moduls auf **Konfigurieren**.



Eintrag in der Modulverwaltung – klicken Sie auf **Konfigurieren**, um die Block-Ips-Übersicht zu öffnen.

Sobald die erste Konfigurationsseite geladen ist, schützt Block Ips Ihren Shop bereits mit sicheren Standardeinstellungen (Firewall deaktiviert, keine Länder blockiert, keine IPs blockiert). Von hier aus passen Sie das Modul an Ihre Bedürfnisse an – beginnen Sie mit der **Übersicht**.

**Tipp:** Wenn Ihre Installation mehrere Shops umfasst, konfiguriert Block Ips jeden Shop unabhängig. Wählen Sie oben im Dropdown-Menü den gewünschten Shop aus, bevor Sie Einstellungen anpassen.

## Übersicht

Die Übersicht bietet Ihnen einen täglichen Aktivitätsüberblick: wie viele Besucher kamen, wie viele blockiert wurden, welche Länder Ihren Traffic dominieren und welche IPs sich verdächtig verhalten.

PrestaShop 8.1.3 Quick Access Modules / blocks / Configure

## Configure Block ips

Dashboard | IPs | Firewall | Countries | Manually Block/Whitelist | Ban user-agent | Options/Cron | About / Documentation

30 Days | 7 Days | Yesterday | Today | From 23/03/2026 to 22/04/2026

**TOTAL REQUESTS** 591 | **TOTAL BLOCKED REQUESTS** 81 | **BLOCK RATE** 13.71% | **TOP COUNTRY** France | **TOP PATH** https://dv8.stefdevelopment.com/ | **LAST FIREWALL EVENT** 2026-04-01 20:18:54 | **ABANDONED CARTS** 3

Compare blocked traffic against total traffic for the selected date range.

### Countries

Requests by countries

Country	Requests
France	50
Japan	49
United States of America	48
Australia	44
Ireland	35
India	29
Romania	8
Spain	8
Morocco	7
Poland	6
Netherlands (Kingdom of the)	4
Lithuania	3
China	3
United Kingdom of Great Britain and Northern Ireland	2
Ukraine	1

### Firewall

1 attempts blocked automatically by the firewall

ID	IP	Page	User-Agent	Country	Total Requests	Date	Action
81	160.178.23.95	https://dv8.stefdevelopment.com/mfa/con/ko	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36	FR	95	2026-04-01 20:18:54	OK

### Abandoned Carts

IP	Country	Abandoned Carts	Last Cart	Action
160.178.23.95	FR	0	2026-04-01 14:27:37	OK

### User-Agent

User-Agent	Requests
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36	158
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36	118
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36	73
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36	49
colly - https://github.com/gocolly/colly	35
Mozilla/5.0 (compatible; CMS Checker/1.0; https://rexxample.com)	25
Go-http-client/1.0	14
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/147.0.0.0 Safari/537.36 Edg/147.0.0.0	12
Mozilla/5.0 (compatible; Googlebot/2.1; http://www.google.com/bot.html)	10
Helio from Palo Alto Networks, find out more about our scans in https://docs-cortex.paloaltonetworks.com/IT/Cortex-Xpanse/Scanning-activity	8
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36	7
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36	6
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36	6
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15; rv:149.0) Gecko/20101001 Firefox/149.0	5
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36	4

### Paths

Path	Requests
https://dv8.stefdevelopment.com/	147
https://dv8.stefdevelopment.com/en/	112
https://dv8.stefdevelopment.com/en/	26
https://dv8.stefdevelopment.com/module/block-invest/fmg/fmg.php	7
https://dv8.stefdevelopment.com/en/module/block-whitelist/action/action/manager/Whitelist	5
https://dv8.stefdevelopment.com/en/module/products/comments/CommentGrade?id_product%5B%5D=1&id_product%5B%5D=2&id_product%5B%5D=3&id_product%5B%5D=4&id_product%5B%5D=5&id_product%5B%5D=6&id_product%5B%5D=7&id_product%5B%5D=8	5
https://dv8.stefdevelopment.com/en/gip/gip.php	4
https://dv8.stefdevelopment.com/en/profiler/gip/info	4
https://dv8.stefdevelopment.com/en/gip/info.php	4
https://dv8.stefdevelopment.com/en/module/notifications/gip/_environment	4
https://dv8.stefdevelopment.com/en/gip/info.php	4
https://dv8.stefdevelopment.com/en/gip/version.php	4
https://dv8.stefdevelopment.com/en/gip/info.php	4
https://dv8.stefdevelopment.com/en/_environment	4

Configuration:  Activate module for this shop context: shop ->strang-DV8-strang-

Die Übersicht – filtern Sie nach Zeitraum mithilfe der Schaltflächen oben (30 Tage, 7 Tage, Gestern, Heute).

## Diagramme lesen

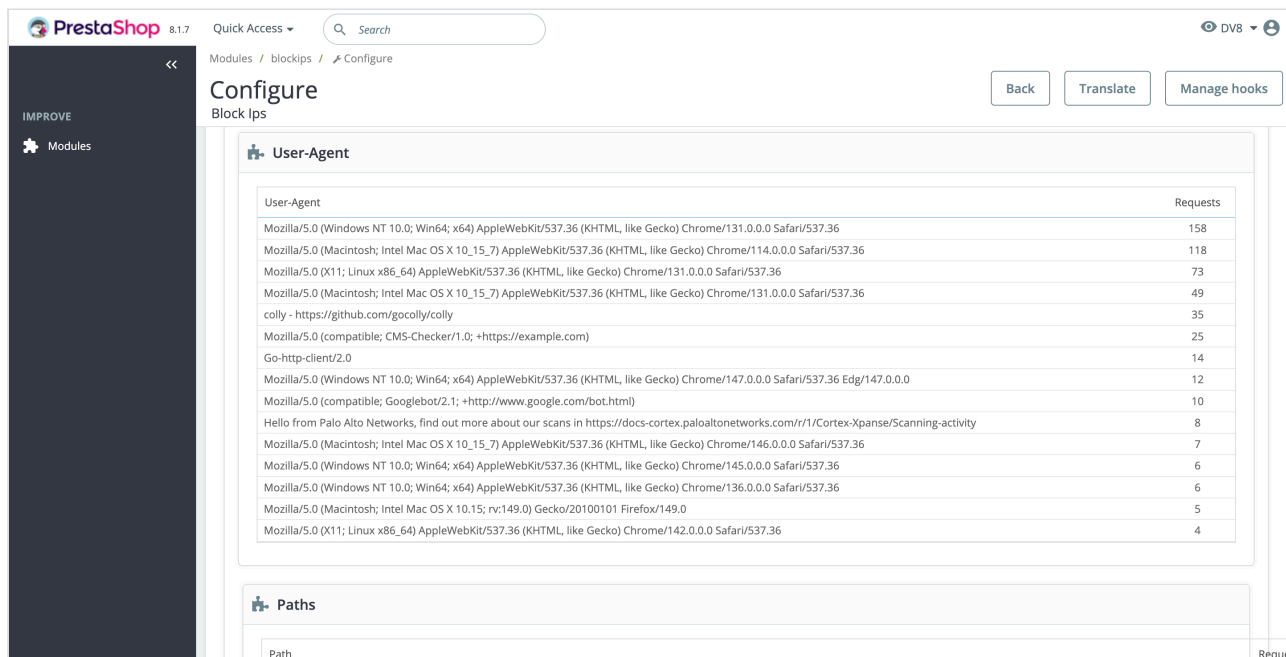
- **Besuche-Liniendiagramm** – Gesamtbesuche pro Tag im gewählten Zeitraum. Ein starker Ausschlag an einem einzelnen Tag deutet meist auf einen Crawler, eine Aktion oder einen Angriff hin.
- **Top-Länder-Kreisdiagramm** – die Herkunftsverteilung Ihrer Besucher. Hilft Ihnen zu entscheiden, ob das Blockieren ganzer Länder (siehe Abschnitt [Länder](#)) für Ihren Shop sinnvoll ist.
- **Tabelle der meistblockierten IPs** – die IPs, die die meisten Blockierungen ausgelöst haben. Klicken Sie auf eine IP, um zu sehen, welche Seiten sie aufzurufen versuchte.

## Datumsfilter

Oben in der Übersicht stehen vier Schnellbereiche zur Verfügung: **30 Tage**, **7 Tage**, **Gestern**, **Heute**. Jedes Diagramm und jede Tabelle in der Übersicht wird neu berechnet, wenn Sie den Zeitraum ändern. Für Zeiträume über 30 Tage verwendet das Modul eine tägliche Aggregationstabelle, die ein schnelles Laden ermöglicht (in unter 5 Sekunden, selbst bei stark frequentierten Shops).

## Top-IPs nach abgebrochenen Warenkörben

Ein Unterbereich der Übersicht ist besonders nützlich, um **Warenkorbabbruch-Bots** zu erkennen – Besucher, die wiederholt Produkte in den Warenkorb legen und ohne Bezahlung wieder verschwinden, oft um Preise auszulesen oder Lagerreservierungen zu blockieren.



User-Agent	Requests
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36	158
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36	118
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36	73
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36	49
colly - https://github.com/gocolly/colly	35
Mozilla/5.0 (compatible; CMS-Checker/1.0; +https://example.com)	25
Go-http-client/2.0	14
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/147.0.0.0 Safari/537.36 Edg/147.0.0.0	12
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/botL.html)	10
Hello from Palo Alto Networks, find out more about our scans in https://docs-cortex.paloaltonetworks.com/r/r1/Cortex-Xpanse/Scanning-activity	8
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36	7
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36	6
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36	6
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:149.0) Gecko/20100101 Firefox/149.0	5
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36	4

*Top-IPs nach abgebrochenen Warenkörben – klicken Sie auf das rote Schildsymbol, um eine IP in einem Schritt zu blockieren.*

Die Tabelle zeigt jede auffällige IP mit ihrer Länderflagge, der Anzahl der erzeugten abgebrochenen Warenkörbe und dem Datum des letzten Warenkorbs. Um die IP sofort zu blockieren, klicken Sie auf das rote Schildsymbol in der Spalte **Aktion**. Um zuerst den Verlauf der IP zu prüfen, klicken Sie auf die IP selbst – es öffnet sich ein Popup mit der Liste der besuchten Seiten.

**Wann dies anwenden:** Wenn eine einzelne IP in den letzten 30 Tagen 10 oder mehr abgebrochene Warenkörbe zeigt, handelt es sich fast sicher um einen Bot. Blockieren Sie sie. Wenn Sie viele IPs mit jeweils 3–5 Warenkörben aus demselben Land sehen, sollten Sie stattdessen dieses Land blockieren.

# Tab IPs

Der Tab IPs ist das **vollständige Protokoll** jedes Besuchers, den das Modul gesehen hat, sortierbar und durchsuchbar. Wo die Übersicht aggregierte Statistiken zeigt, zeigt dieser Tab einzelne Zeilen.

The screenshot shows the PrestaShop 8.1.7 interface for configuring the 'Block ips' module. The 'IPs' tab is selected, displaying a table of visitor records. The table has the following columns: Ip, Id customer, Id guest, Date first visit, Date last visit, Nbr pages viewed, Nbr redirect after block, Location, Pages, and State. The first 10 entries are shown, with a search bar and pagination controls at the bottom of the table. Below the table is a 'Configuration' section with a checkbox to 'Activate module for this shop context: shop <strong>DVB</strong>'. The 'State' column contains shield icons, which are used to toggle the blocking status of each IP.

Ip	Id customer	Id guest	Date first visit	Date last visit	Nbr pages viewed	Nbr redirect after block	Location	Pages	State
3.7.66.249	0	0	2025-07-24 17:58:38	2025-07-24 17:58:38	1	0		1	
3.67.197.2	0	0	2025-12-12 19:40:13	2025-12-12 19:40:20	2	0		1	
3.68.215.245	0	6834	2026-03-04 07:35:55	2026-03-04 07:36:08	3	0		1	
3.72.18.89	0	5973	2025-12-10 14:37:53	2025-12-10 14:38:01	2	0		1	
3.76.45.20	0	6866	2026-03-07 16:12:51	2026-03-07 16:12:51	3	0		1	
3.82.163.255	0	0	2025-12-16 08:53:25	2025-12-19 18:11:16	4	0		1	
3.83.207.96	0	0	2025-11-01 00:32:34	2025-11-01 00:32:34	1	0		1	
3.86.65.120	0	0	2025-07-21 00:40:38	2025-07-21 05:32:47	2	0		1	
3.86.149.202	0	0	2025-08-16 10:36:43	2025-08-16 10:36:43	1	0		1	
3.89.196.216	0	0	2025-09-25 12:44:36	2025-09-25 12:44:36	1	0		1	

Jede Zeile steht für eine Besucher-IP. Klicken Sie auf das Schildsymbol, um zwischen blockiert/entsperrt umzuschalten.

## Spalten

Spalte	Bedeutung
<b>IP</b>	Die IPv4- oder IPv6-Adresse des Besuchers. Klicken Sie darauf, um zu sehen, welche Seiten er besucht hat.
<b>Land</b>	Flagge + Ländername, ermittelt aus der eingebetteten IP2Location-Datenbank.
<b>Datum erster Besuch</b>	Wann diese IP zum ersten Mal in Ihrem Shop gesehen wurde.
<b>Datum letzter Besuch</b>	Letzter Besuch.
<b>Anz. Seiten angesehen</b>	Gesamtzahl der Seitenaufrufe dieser IP.
<b>Anz. Weiterleitungen nach Blockierung</b>	Wie oft diese IP Ihren Shop <i>nach</i> der Blockierung erneut getroffen hat (d.h. wie hartnäckig sie es weiter versucht).
<b>Status</b>	Grünes Häkchen = erlaubt, rotes Schild = blockiert. Klicken zum Umschalten.

## Häufige Aktionen

- **Eine bestimmte IP finden** – verwenden Sie das Suchfeld oberhalb der Tabelle.
- **Nach Weiterleitungen nach Blockierung sortieren** – die IPs, die Sie auch nach der Blockierung weiter angreifen, sind die hartnäckigen; hier lohnt es sich, die Firewall-Regeln zu verschärfen.
- **Eigene IP auf die Whitelist setzen** – wenn Sie Ihre eigene Büro-IP in der Liste sehen, klicken Sie auf das Schildsymbol, damit die Firewall Sie niemals versehentlich blockiert. (Siehe auch [Manuell blockieren / Whitelist](#) für eine explizitere Whitelist.)

**Hinweis zur Leistung:** In Shops mit Millionen protokollierter IPs verwendet dieser Tab serverseitige Paginierung – es werden nur die aktuell sichtbaren Zeilen an Ihren Browser gesendet. Wenn die Seite bei Ihnen langsam wirkt, sehen Sie im Tab **Optionen / Cron** nach, wie sich alte Einträge automatisch bereinigen lassen.

# Firewall

Die Firewall ist die **automatische** Seite von Block Ips: Anstatt dass Sie IPs nach Fehlverhalten manuell blockieren, überwacht die Firewall die Anfragerate in Echtzeit und blockiert IPs automatisch, die von Ihnen definierte Schwellenwerte überschreiten.

**Configure**  
Block ips

Dashboard | IPs | **Firewall** | Countries | Manually Block/Whitelist | Ban user-agent | Options/Cron | About / Documentation

**Firewall configuration**

Enable the firewall

Enable alert by mail

Maximum requests   
Enter the maximum number of requests allowed from a single IP address within the time window.  
For example, a value of "100" with a time window of "60 seconds" would mean a user can make up to 100 requests per minute.

Time window

Specify the duration of the time window for rate limiting.  
For example, a value of "5" with "minutes" selected means the request limit applies within a 5-minute window.

**Last attempts blocked automatically by the firewall**

ID	IP	Page	User-Agent	Country	Total Requests	Date	Action
81	160.178.230.95	https://dv8.stefdevelopment.com/favicon.ico	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36		95	2026-04-01 20:18:54	
80	74.7.242.3	https://dv8.stefdevelopment.com/9-art	Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; GPTBot/1.3; +https://openai.com/gptbot)		12	2026-03-20 16:22:06	
77	139.59.101.58	https://dv8.stefdevelopment.com/news/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36		16	2026-03-18 06:45:57	
76	174.138.30.27	https://dv8.stefdevelopment.com/news/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36		11	2026-03-18 03:54:15	
75	74.7.227.36	https://dv8.stefdevelopment.com/best-sellers	Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; GPTBot/1.3; +https://openai.com/gptbot)		16	2026-03-12 06:13:27	
74	104.164.126.174	https://dv8.stefdevelopment.com/https%3A/www.prestashop-project.org	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36		42	2026-03-05 13:28:22	
73	136.117.161.236	https://dv8.stefdevelopment.com/2018/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36		12	2026-03-04 10:10:04	
72	34.57.146.22	https://dv8.stefdevelopment.com/2018/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36		11	2026-03-03 16:41:04	
71	35.221.56.18	https://dv8.stefdevelopment.com/news/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36		11	2026-03-01 14:29:51	
70	35.184.89.2	https://dv8.stefdevelopment.com/news/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36		11	2026-02-28 12:35:20	

**Configuration**

Activate module for this shop context: shop <strong>DV8</strong>.

Firewall-Konfiguration – legen Sie Schwellenwerte für Anfragen pro Zeitfenster fest und aktivieren Sie dann.

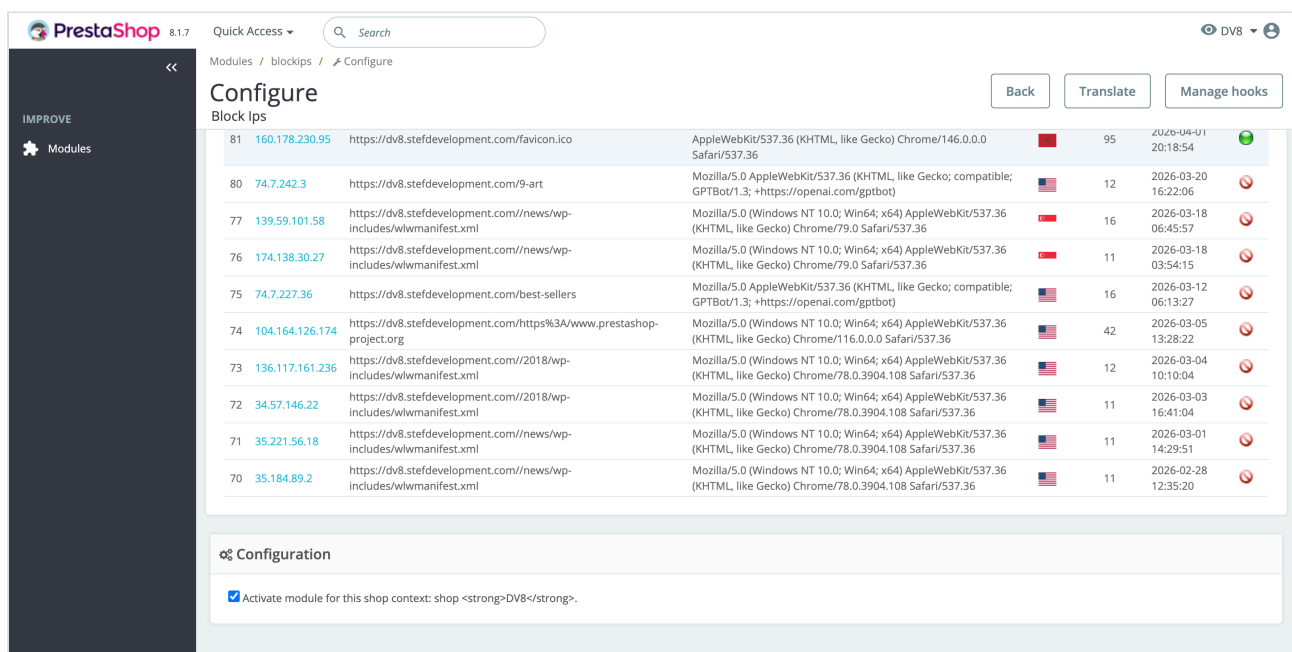
## Funktionsweise

Für jede Besucher-IP verfolgt die Firewall, wie viele Anfragen sie in den letzten  $N$  Minuten gestellt hat. Überschreitet dieser Wert Ihren Schwellenwert, wird die IP automatisch blockiert – ohne Ihr Zutun.

## Einstellungen

- **Firewall aktivieren** – Hauptschalter. Lassen Sie ihn beim Feintuning aus und schalten Sie ihn ein, sobald Ihre Schwellenwerte passen.
- **Maximale Anfragen pro Zeitfenster** – der Schwellenwert. Beginnen Sie großzügig (z.B. 200 Anfragen / 1 Minute) und senken Sie ihn, falls weiterhin Missbrauch auftritt.
- **Zeitfenster (Minuten)** – das rollierende Fenster zur Zählung der Anfragen. Kürzere Fenster erkennen Bursts schneller; längere Fenster glätten normale Traffic-Spitzen.
- **Automatisch entsperren nach** – wie lange eine von der Firewall ausgelöste Blockierung andauert. 60 Minuten sind ein sinnvoller Standardwert – lang genug, um einen Bot abzuschrecken, kurz genug, damit ein Fehlalarm einen echten Kunden nicht über Nacht aussperrt.
- **Suchmaschinen auf die Whitelist setzen** – wenn aktiviert, werden IPs aus Crawler-Bereichen von Google, Bing, Yahoo und DuckDuckGo niemals von der Firewall blockiert. Lassen Sie diese Option **aktiviert**, sofern Sie keinen Grund haben, Crawler zu sperren.

## Firewall-Aktivität



The screenshot shows the PrestaShop 8.1.7 interface for configuring the Firewall. The page title is "Configure Block Ips". Below the title, there are buttons for "Back", "Translate", and "Manage hooks". The main content is a table listing blocked IPs with columns for ID, IP address, URL, user agent, country, request count, and last activity. At the bottom, there is a "Configuration" section with a checkbox to "Activate module for this shop context: shop <strong>DV8</strong>".

ID	IP	URL	User Agent	Country	Count	Last Activity
81	160.178.230.95	https://dv8.stefdevelopment.com/favicon.ico	AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36	🇺🇸	95	2026-04-01 20:18:54
80	74.7.242.3	https://dv8.stefdevelopment.com/9-art	Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; GPTBot/1.3; +https://openai.com/gptbot)	🇺🇸	12	2026-03-20 16:22:06
77	139.59.101.58	https://dv8.stefdevelopment.com/news/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36	🇺🇸	16	2026-03-18 06:45:57
76	174.138.30.27	https://dv8.stefdevelopment.com/news/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0 Safari/537.36	🇺🇸	11	2026-03-18 03:54:15
75	74.7.227.36	https://dv8.stefdevelopment.com/best-sellers	Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; GPTBot/1.3; +https://openai.com/gptbot)	🇺🇸	16	2026-03-12 06:13:27
74	104.164.126.174	https://dv8.stefdevelopment.com/https%3A/www.prestashop-project.org	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36	🇺🇸	42	2026-03-05 13:28:22
73	136.117.161.236	https://dv8.stefdevelopment.com/2018/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36	🇺🇸	12	2026-03-04 10:10:04
72	34.57.146.22	https://dv8.stefdevelopment.com/2018/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36	🇺🇸	11	2026-03-03 16:41:04
71	35.221.56.18	https://dv8.stefdevelopment.com/news/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36	🇺🇸	11	2026-03-01 14:29:51
70	35.184.89.2	https://dv8.stefdevelopment.com/news/wp-includes/wlmanifest.xml	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36	🇺🇸	11	2026-02-28 12:35:20

Firewall-Aktivität – jede Zeile entspricht einer automatischen Blockierung. Klicken Sie auf die IP, um zu sehen, was sie getan hat.

Jede automatische Blockierung wird hier mit IP, Land, Anzahl der auslösenden Anfragen und Zeitstempel protokolliert. Prüfen Sie diesen Bereich nach Aktivierung der Firewall, um Ihre Schwellenwerte anzupassen: Wenn Sie legitim wirkende Muster sehen (ein einzelner Kunde, der zügig viele Seiten durchsieht), ist Ihr Schwellenwert zu streng.

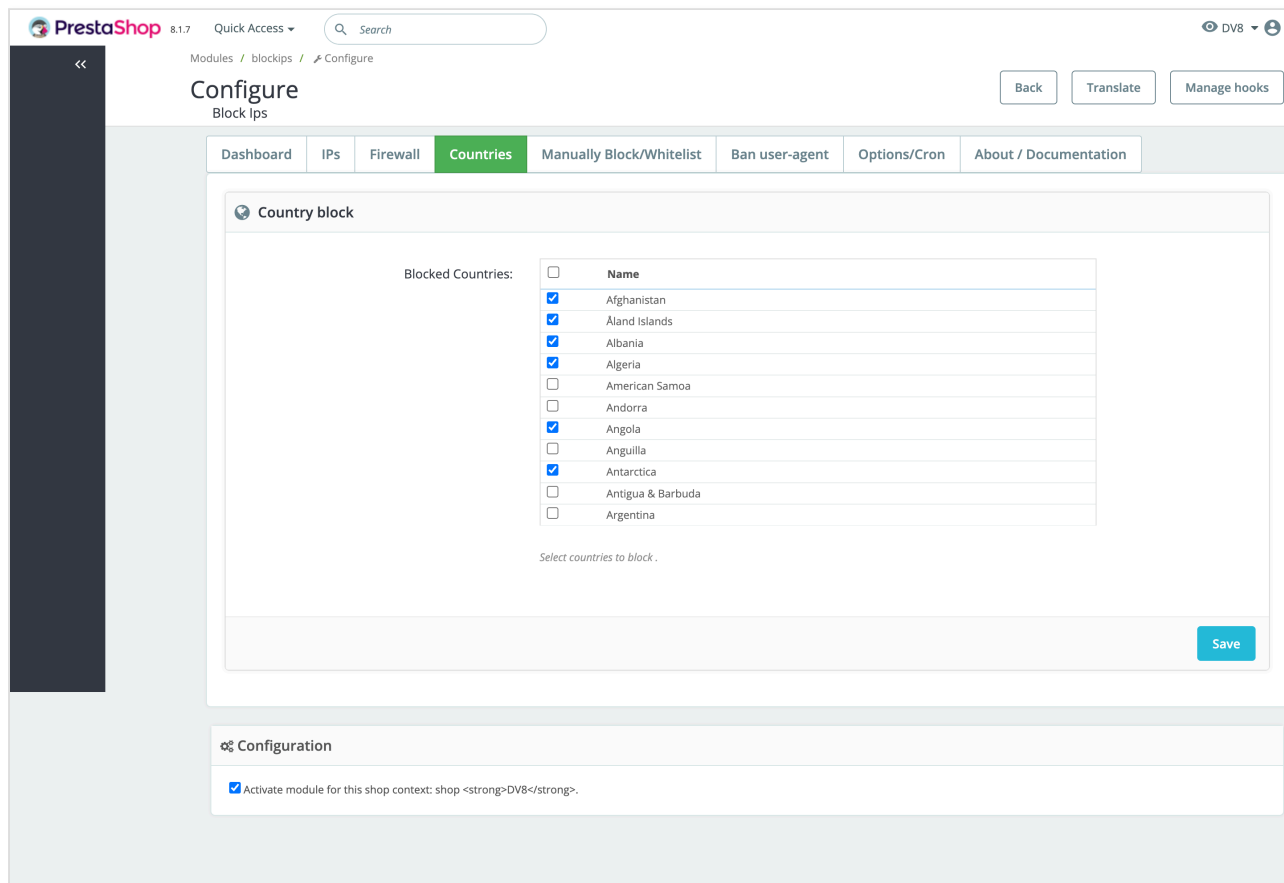
## Empfehlungen zur Feinabstimmung

Shop-Profil	Beginnen Sie mit
Boutique mit wenig Traffic (< 500 Besucher/Tag)	100 Anfragen / 5 Min.
Shop mit mittlerem Traffic (500–5.000 Besucher/Tag)	200 Anfragen / 1 Min.
Shop mit hohem Traffic auf einem CDN	500 Anfragen / 1 Min.
Aktuell unter Angriff	60 Anfragen / 1 Min., erst nach 24 h Beobachtung aktivieren

**Wichtig:** Lassen Sie die Firewall stets 24 Stunden mit dem Schalter **Aktivieren** AUS laufen und beobachten Sie zunächst den Aktivitätsbereich. Es wird protokolliert, was blockiert *worden wäre*, sodass Sie prüfen können, dass kein legitimer Traffic erfasst wird, bevor Sie sie aktivieren.

# Länder

Wenn Ihr Shop nur in eine bestimmte Region liefert oder wenn eine Flut von Missbrauch aus einem Land kommt, können Sie dieses gesamte Land mit zwei Klicks blockieren.



*Länderliste – setzen Sie ein Häkchen, um zu blockieren; entfernen Sie es, um zu entsperren. Wird automatisch gespeichert.*

## So blockieren Sie ein Land

1. Suchen Sie das Land in der Liste (das Suchfeld filtert beim Tippen).
2. Setzen Sie das Häkchen.
3. Die Änderung wird sofort gespeichert – es gibt keine separate Schaltfläche zum Speichern.

Besucher aus einem blockierten Land sehen eine einfache Seite „Zugriff verweigert“ anstelle Ihres Shops. Bots geben meist auf; echte Kunden bemerken es selten, da sie sich ohnehin nicht in einer blockierten Region befinden.

## Wichtige Überlegungen

- **Zuerst das eigene Land.** Blockieren Sie niemals Ihr eigenes Land. Prüfen Sie doppelt, bevor Sie das Häkchen setzen.
- **VPN-Kunden.** Einige Ihrer echten Kunden nutzen möglicherweise VPNs, die in blockierten Ländern ausgehen. Wenn Sie international verkaufen, bevorzugen Sie die Firewall gegenüber Ländersperren.
- **Crawler.** Das Blockieren eines Landes blockiert auch die dort gehosteten Crawler. Die Crawler von Google befinden sich überwiegend in den USA; die von Bing sind global verteilt. Die Option **Suchmaschinen auf die Whitelist setzen** im Firewall-Tab deckt dies für *Firewall*-Blockierungen ab, umgeht aber KEINE Ländersperre. Wenn SEO wichtig ist, ziehen Sie stattdessen den Firewall-Ansatz in Betracht.
- **Jederzeit umkehrbar.** Das Entfernen des Häkchens entsperrt das Land sofort.

**Typische Anwendung:** Ein EU-only-Shop blockiert Nicht-EU-Länder. Eine plötzliche Welle von Kreditkartenbetrug aus einem Land führt dazu, dass dieses Land für 48 Stunden blockiert wird. Ein Shop, der nur innerhalb des Landes versendet, blockiert jedes ausländische Land.

## Manuell blockieren / Whitelist

Dieser Tab ist für Fälle gedacht, in denen Sie die IP, mit der Sie sich befassen möchten, bereits kennen – ohne darauf zu warten, dass die Firewall sie erwischt, und ohne im IP-Protokoll zu suchen.

PrestaShop 8.1.7 Quick Access  DV8

Modules / blockips / Configure

## Configure

Block ips

Back Translate Manage hooks

Dashboard IPs Firewall Countries **Manually Block/Whitelist** Ban user-agent Options/Cron About / Documentation

**Manually block**

List of Ip

an IP address per line

Add

**Whitelist**

List of Ip

127.0.0.1


List of IP to never block, an IP address per line

Add


**Block IP Ranges & Wildcards**

Range or Wildcard

Enter a range (e.g., 192.168.1.1-192.168.1.100) or a wildcard (e.g., 192.168.\*.\*)

 Add Range

Existing Ranges

Range / Wildcard	Start IP	End IP	Action
196.74.215.1-196.74.215.255	196.74.215.1	196.74.215.255	 Delete

**Configuration**

Activate module for this shop context: shop <strong>DVB</strong>.

Fügen Sie eine einzelne IP, einen Bereich (CIDR) oder Dutzende IPs gleichzeitig ein – eine pro Zeile.

## Drei Eingabemodi

**1. Einzelne IP** – geben Sie eine IP-Adresse (IPv4 oder IPv6) ein oder fügen Sie sie ein. Klicken Sie auf **Hinzufügen**, um zu blockieren.

**2. IP-Bereich (CIDR)** – geben Sie einen Bereich wie `192.168.1.0/24` ein, um 256 Adressen auf einmal zu blockieren. Nützlich, um ein ganzes Subnetz eines Hosting-Anbieters zu blockieren.

**3. Sammelweise einfügen** – fügen Sie eine beliebige Anzahl von IPs ein, eine pro Zeile. Das Modul prüft jede einzelne und teilt Ihnen vor dem Speichern mit, welche ungültig oder bereits blockiert sind.

## Whitelist

Eine auf die Whitelist gesetzte IP wird **niemals** blockiert, weder manuell noch durch die Firewall oder Länderregeln. Verwenden Sie dies für:

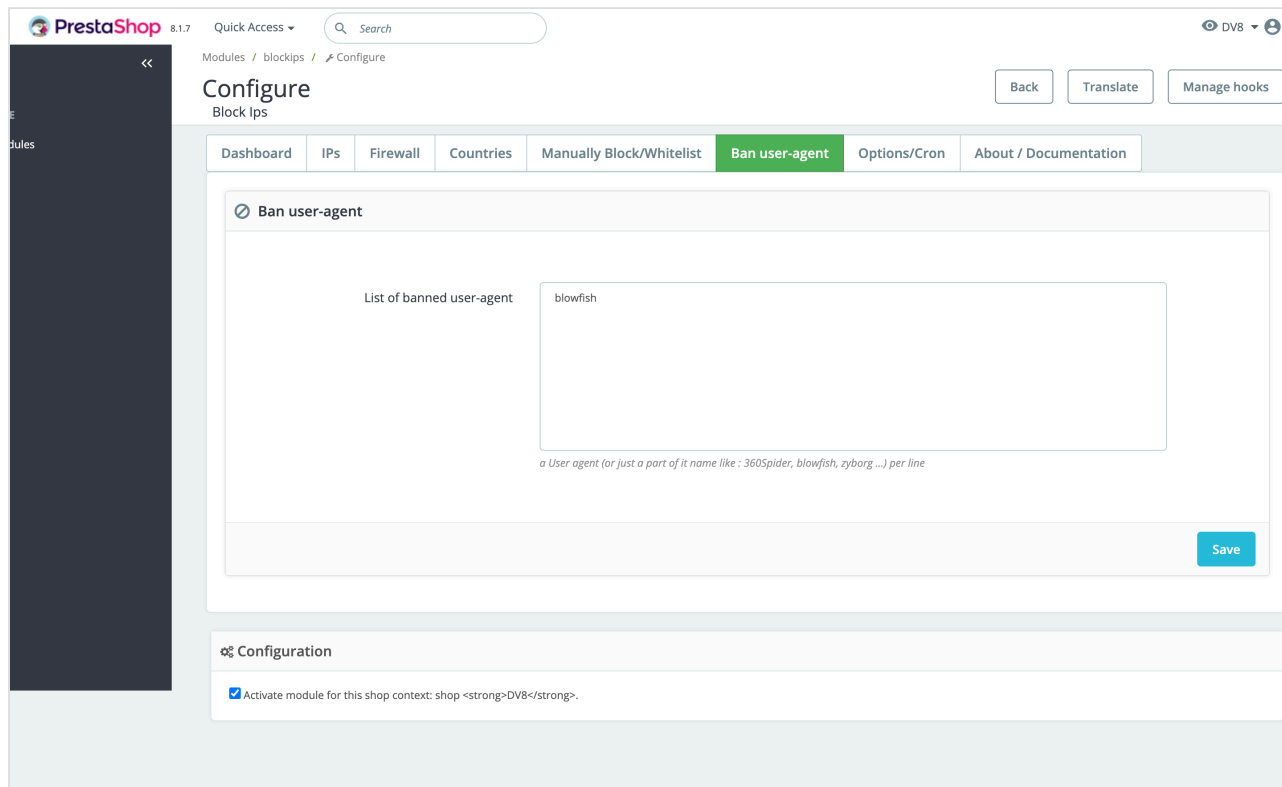
- Ihre eigene Büro-/Heim-IP (damit Sie sich niemals selbst aussperren).
- Die IP Ihres Überwachungsdienstes (UptimeRobot, Pingdom usw.).
- Vertrauenswürdige Partner-APIs, die Ihren Shop häufig abfragen.

Die Whitelist-Eingabe befindet sich im selben Tab unterhalb des Blockierungsformulars. Gleiche drei Modi (einzeln / Bereich / Sammel).

**Prioritätsregel:** Die Whitelist gewinnt immer. Ist eine IP sowohl auf der Whitelist als auch in einem blockierten Land, wird sie durchgelassen. Ist sie auf der Whitelist und überschreitet den Firewall-Schwellenwert, wird sie durchgelassen. Verwenden Sie die Whitelist sparsam und prüfen Sie sie regelmäßig – ein veralteter Whitelist-Eintrag ist ein Sicherheitsrisiko.

## User-Agent sperren

Einige Bots lassen sich leichter anhand des Browser-Strings identifizieren, den sie senden, als anhand der IP, von der sie kommen. Dieser Tab ermöglicht es Ihnen, Besucher zu blockieren, deren **User-Agent**-Header eine bestimmte Zeichenkette enthält.



*Fügen Sie die User-Agent-Teilzeichenkette (Groß-/Kleinschreibung ignoriert) ein – jede Anfrage, deren User-Agent-Header sie enthält, wird blockiert.*

### So funktioniert das Matching

Sie geben eine **Teilzeichenkette** ein, nicht den vollständigen User-Agent. Der Abgleich ist **unabhängig von Groß-/Kleinschreibung**.

Beispiele:

- AhrefsBot – blockiert jede Anfrage, die „AhrefsBot“ an beliebiger Stelle im User-Agent enthält. Passt zu Mozilla/5.0 (compatible; AhrefsBot/7.0; ...).
- semrush – blockiert Semrush-Crawler (Hinweis: ohne Berücksichtigung der Groß-/Kleinschreibung, erfasst SemrushBot, Semrush, semrush).
- python-requests – blockiert Skripte, die den Standard-User-Agent der Python-Requests-Bibliothek verwenden.

## Häufige Einsatzgebiete

- SEO-Crawler, die Ihre Website nicht indexieren sollen (AhrefsBot, SemrushBot, MJ12bot).
- Scraping-Skripte mit erkennbaren UAs (python-requests, curl, wget).
- Scraper mobiler Apps, die sich als iPhones ausgeben – schwieriger; prüfen Sie den UA zuerst über den Tab IPs.

**Vorsicht:** Blockieren Sie NICHT Googlebot , bingbot , DuckDuckBot oder andere legitime Suchmaschinen-Crawler – Ihr Shop verschwindet sonst aus deren Ergebnissen. Schlagen Sie den User-Agent im Zweifel zuerst auf einer Referenzseite wie user-agents.net nach.

## Optionen / Cron

In diesem Tab sind die Wartungs- und Verhaltenseinstellungen des Moduls zusammengefasst: wie lange Protokolle aufbewahrt werden, was einem blockierten Besucher angezeigt wird und wie die automatische Bereinigung geplant wird.

PrestaShop 6.1.7 Quick Access Search DV8

Modules / blockips / Configure

## Configure

### Block ips

Back Translate Manage hooks

Dashboard IPs Firewall Countries Manually Block/Whitelist Ban user-agent **Options/Cron** About / Documentation

**Database**

Table size 5.72 MiB

Clean

**Cron - Clean / Summary report**

Clean cron link <https://dv8.stefdevelopment.com/en/module/blockips/cron?token=qgBV0FGCKXNDFSIBvEKPYQyU07Zur&cron=clean>  
Use this cron URL to clean old data according to the number of days to keep.

Summary cron link <https://dv8.stefdevelopment.com/en/module/blockips/cron?token=qgBV0FGCKXNDFSIBvEKPYQyU07Zur&cron=summary>  
Use this cron URL to send all due daily, weekly, and monthly summary reports.

Run all cron link <https://dv8.stefdevelopment.com/en/module/blockips/cron?token=qgBV0FGCKXNDFSIBvEKPYQyU07Zur&cron=all>  
Use this optional cron URL if you want one task to run both cleaning and summary delivery.

Days to keep   
Number of days to keep data in the table

Enable summary report by email   
Send a scheduled email summary for the selected shop.

Summary report schedules  Daily  Weekly  Monthly  
Select one, two, or all three schedules. Reports are sent by the summary cron task to the current shop email address.

The following are sample commands using different tools. You need to copy the one that suits your needs and setup CRON in your server.

CURL PHP WGET

```
Clean: wget -i /dev/null "https://dv8.stefdevelopment.com/en/module/blockips/cron?token=qgBV0FGCKXNDFSIBvEKPYQyU07Zur&cron=clean"
Summary: wget -i /dev/null "https://dv8.stefdevelopment.com/en/module/blockips/cron?token=qgBV0FGCKXNDFSIBvEKPYQyU07Zur&cron=summary"
Run all: wget -i /dev/null "https://dv8.stefdevelopment.com/en/module/blockips/cron?token=qgBV0FGCKXNDFSIBvEKPYQyU07Zur&cron=all"
```

Save

**Redirect URL**

Show forbidden or redirect  Show forbidden message  Redirect to an URL  
Show forbidden message or redirect to an url!

Url   
Url to redirect to when a user is blocked

Forbidden Message   
Forbidden message to show when a user is blocked

save

**Other options**

Display the customer's location map on the order details page  show  Hide

save

**Configuration**

Activate module for this shop context: shop <strong>DV8</strong>.

Tab Optionen – passen Sie Aufbewahrung, Weiterleitungsverhalten und Cron an.

## Wichtige Optionen

- **Blockierungsseiten-Text** – was ein blockierter Besucher sieht. Standard ist eine einfache Seite „Zugriff verweigert“; Sie können das HTML anpassen.
- **Weiterleitung nach Blockierung** – wohin ein blockierter Besucher geschickt wird. Leer lassen, um auf der Ablehnungsseite zu bleiben; eine URL eintragen, um ihn woandershin umzuleiten (z.B. auf eine statische „Entschuldigung“-Seite).
- **Protokolle aufbewahren für (Tage)** – wie lange Besucherprotokolle in der Datenbank verbleiben. 90 Tage sind ein guter Standardwert. Länger bedeutet umfangreichere historische Statistiken; kürzer bedeutet eine schlankere Datenbank.
- **Aggregierte Statistiken** – aktivieren Sie bei Shops mit starkem Traffic die tägliche Aggregationstabelle (ab v4.3.0) für Ladezeiten der Übersicht unter 5 Sekunden.

## Cron-Bereinigung

Alte Besucherprotokolle summieren sich schnell. Block Ips enthält ein Cron-Bereinigungsskript, das Einträge, die älter als Ihre Aufbewahrungseinstellung sind, schrittweise Tag für Tag entfernt – mit einem Fortschrittsbalken, den Sie mitverfolgen können.

Die Cron-URL wird im Tab Optionen angezeigt. Kopieren Sie sie und fügen Sie sie in den Cron-Planer Ihres Hosting-Panels ein:

- **cPanel** – Erweitert → Cron-Jobs → Neuen Cron-Job hinzufügen. Zeitplan: täglich ( 0 3 \* \* \* um 3:00 Uhr).
- **Plesk** – Tools & Einstellungen → Geplante Aufgaben → Aufgabe hinzufügen. Verwenden Sie den Modus „URL abrufen“ mit der Cron-URL.
- **Kommandozeile** – sofern Sie Shell-Zugriff haben:

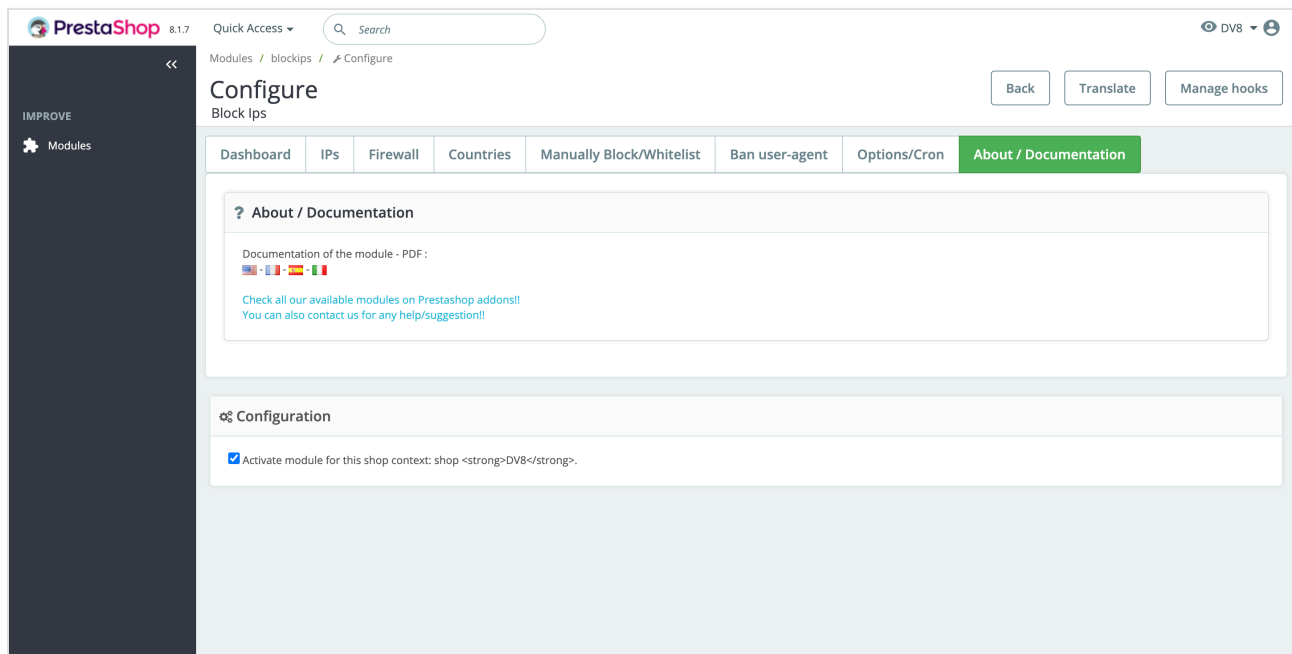
```
0 3 * * * /usr/bin/curl -s "https://yourshop.com/modules/blockips/cron-
```

Einmal täglich um 3:00 Uhr bereinigt der Cron einen Tagesumfang alter Protokolleinträge. Nach einigen Tagen ist er aufgeholt und bleibt dann dauerhaft auf dem neuesten Stand.

**Wenn Sie keinen Cron einrichten können:** Verwenden Sie alle paar Wochen manuell die Schaltfläche **Jetzt bereinigen** im Tab Optionen. Sie führt dieselbe Bereinigung auf Anforderung aus. Der Cron ist lediglich eine Bequemlichkeit.

# Über / Dokumentation

Der Tab Über ist der Einstiegspunkt des Moduls zu genau dieser PDF (und ihren Übersetzungen) sowie zum Unternehmen hinter Block Ips.



*Der Tab Über verweist mit jeder Flagge auf das sprachspezifische Benutzerhandbuch.*

Klicken Sie auf eine beliebige Flagge, um die PDF in Ihrer Sprache zu öffnen. Lesezeichen sind willkommen – die PDFs sind pro Modul-Release versioniert (v4.3.0 zum Zeitpunkt der Erstellung).

## FAQ

**F: Ich habe gerade die Firewall aktiviert und kann mich nun nicht mehr in mein eigenes Backoffice einloggen.** Öffnen Sie den Dateimanager Ihres Hostings und bearbeiten Sie `modules/blockips/config.xml`, um das Modul zu deaktivieren, oder kommentieren Sie den Firewall-Aufruf in `blockips.php` aus. Setzen Sie dann im Backoffice Ihre IP unter **Manuell blockieren / Whitelist → Whitelist** manuell auf die Whitelist. Aktivieren Sie die Firewall erneut. Setzen Sie Ihre eigene IP immer auf die Whitelist, bevor Sie die Firewall aktivieren.

**F: Blockiert Block Ips Google oder andere Suchmaschinen?** Nicht, wenn **Suchmaschinen auf die Whitelist setzen** im Firewall-Tab aktiviert ist (was standardmäßig der Fall ist). Das Modul pflegt eine aktuelle Liste der IP-Bereiche von Googlebot, Bingbot, YahooSlurp und DuckDuckBot und überspringt sie. Ländersperrern und User-Agent-Sperrern wenden diese Whitelist NICHT an, blockieren Sie daher nicht manuell „US“ oder Googlebot.

**F: Warum ist der Firewall-Aktivitätsbereich leer?** Entweder (a) hat noch keine IP Ihren Schwellenwert überschritten (am häufigsten bei Seiten mit wenig Traffic) oder (b) Sie haben den Hauptschalter nicht aktiviert. Prüfen Sie beides. Das Modul verfolgt Anfragen nur im aktivierten Zustand.

**F: Mein Shop verwendet Cloudflare – sieht Block Ips trotzdem die echte Besucher-IP?** Ja, solange Cloudflare so konfiguriert ist, dass es die ursprüngliche IP im Header `CF-Connecting-IP` weitergibt (Standard). Block Ips liest diesen Header automatisch aus. Wenn Sie ein anderes CDN nutzen, stellen Sie sicher, dass es `X-Forwarded-For` korrekt setzt.

**F: Wie oft sollte ich die Datenbank bereinigen?** Einmal täglich per Cron – siehe [Optionen / Cron](#). Wenn Sie keinen Cron einrichten können, führen Sie die Schaltfläche **Bereinigen** bei Seiten mit wenig Traffic alle paar Wochen und bei stark frequentierten Seiten wöchentlich manuell aus.

**F: Kann ich meine eigene Büro-IP dauerhaft auf der Whitelist halten?** Ja. Fügen Sie sie unter **Manuell blockieren / Whitelist → Whitelist** hinzu. Whitelist-Einträge laufen nie ab und haben Vorrang vor jeder anderen Regel.

**F: Ich sehe seltsame Schübe von Warenkorbabbrüchen von einer IP. Ist das ein Angriff?** Wahrscheinlich ein Scraper oder ein Lagerüberwachungs-Bot. Blockieren Sie die IP aus der Tabelle **Top-IPs nach abgebrochenen Warenkörben** in der Übersicht. Wenn sich das Muster auf eine neue IP aus demselben Land verlagert, sollten Sie das gesamte Land blockieren.

## Support

Fragen, Funktionswünsche oder Fehler: [mustapha.elat@gmail.com](mailto:mustapha.elat@gmail.com) · stefdevelopment.com

Vielen Dank, dass Sie Block Ips verwenden. Dieses Handbuch wurde für Version 4.3.0 verfasst.