Block IPs – Podręcznik użytkownika

Firewall sklepu, ochrona back-office i narzędzia antybotowe · wersja 5.5 · PrestaShop od 1.6 do 9.2

Spis treści

1. Co robi Block IPs
2. Instalacja i pierwsze kroki
3. Overview
4. Blokowanie adresów IP, zakresów i krajów
5. Firewall (limit zapytań)
6. User-agenty i boty AI
7. Ochrona back-office
8. Fałszywe konta
9. Reputacja (AbuseIPDB i Slack)
10. Opcje wydajności
11. Pytania i rozwiązywanie problemów

1. Co robi Block IPs

Block IPs chroni Twój sklep przed niepożądanym ruchem. Blokuje pojedyncze adresy IP, zakresy adresów, kraje oraz fragmenty nagłówków user-agent. Jego firewall automatycznie blokuje adresy IP wysyłające zbyt wiele zapytań. Panel pokazuje ruch i zablokowane zapytania.

Wersja 5.5.0 oferuje również uwierzytelnianie dwuskładnikowe dla pracowników, reguły dostępu do back-office, ochronę przed fałszywymi kontami oraz opcjonalne sprawdzanie reputacji w AbuseIPDB.

> Firewall sklepu obsługuje PrestaShop od 1.6 do 9.2. Ochrona back-office wymaga PrestaShop 1.7.8 lub nowszego. Kontrola fałszywych kont wykorzystuje hooki rejestracji dostępne w PrestaShop od 1.7 do 9.

2. Instalacja i pierwsze kroki

1. Zainstaluj Block IPs z poziomu menedżera modułów swojego sklepu. Otwórz stronę konfiguracji modułu. Menu składa się z pięciu sekcji: **„Overview”**, **„Shop”** (IP addresses, Countries, Bots & AI, Firewall, Manual blocking), **„Back office”**, **„Registrations”** oraz **„Settings”** (Options & Cron, Reputation, About).
2. W trybie multistore wybierz pojedynczy sklep. Strona konfiguracji poprosi o wskazanie sklepu, jeśli znajdujesz się w kontekście grupy lub wszystkich sklepów.
3. Otwórz **„Shop › Firewall”** i sprawdź limit zapytań. Przy nowej instalacji firewall i alert e-mail są domyślnie włączone. Domyślny próg to 100 zapytań w 60 sekund.
4. Otwórz **„Shop › Manual blocking”** i w razie potrzeby dodaj zaufane adresy do **„Whitelist”**.
5. Otwórz **„Settings › Options & Cron”**. W sekcji **„Cron links”** użyj przycisku **„Copy”**, aby skopiować wymagany adres URL do harmonogramu zadań na swoim hostingu. Użyj pełnego adresu URL, łącznie z tokenem.
6. Wejdź na stronę sklepu i sprawdź **„Overview”** oraz **„Shop › IP addresses”**.

Zaplanowane zadania

Link	Zadanie
Cleanup	Usuwa stare dane zgodnie ze skonfigurowanym czasem przechowywania.
Summary	Wysyła oczekujące raporty podsumowujące na adres e-mail.
Reputation	Sprawdza nowe adresy IP w AbuseIPDB w ramach dziennego limitu.
Run all	Uruchamia te zadania, importuje zapytania zablokowane przez serwer, tworzy dzienne podsumowania, odświeża dane IP wyszukiwarek i czyści rejestr logowań back-office.

Sekcja **„Cron configuration examples”** zawiera gotowe polecenia dla curl, PHP CLI i wget. Wybierz metodę obsługiwaną przez Twój hosting. Regularne uruchamianie zadania Run all stanowi praktyczny punkt wyjścia; harmonogram cogodzinny jest zalecany, lecz nie wymagany sztywno przez moduł. Sprawdzanie reputacji i raporty podsumowujące mogą obejmować kilka sklepów, dlatego nie należy zakładać, że każdy adres URL jest ograniczony wyłącznie do aktualnie wybranego sklepu.

> Token jest na ekranie zamaskowany. Kliknięcie **„Show token”** powoduje jego odsłonięcie. Zachowaj adresy URL cron w tajemnicy: token autoryzuje wykonanie zadania.

Zakres w trybie multistore

Ruch, rejestr zablokowanych adresów IP, reguły krajów, ustawienia firewalla i opcje reputacji działają w kontekście pojedynczego sklepu. Ochrona back-office, ustawienia fałszywych kont, biała lista oraz opcje wydajności są współdzielone w całej instalacji. Reguły Apache wykorzystują zablokowane user-agenty ze wszystkich sklepów, ponieważ główny plik .htaccess jest wspólny.

3. Overview

Otwórz **„Overview”** dla wybranego sklepu. Baner **„Your shop is protected”** informuje o stanie funkcji **„Firewall (request limit)”**, **„Two-factor authentication”**, **„AI crawlers blocked”** oraz **„Anti fake accounts”**, oferując przycisk **„Activate”** dla brakujących zabezpieczeń. Wybierz **„Today”**, **„7 days”**, **„30 days”** lub **„Custom”**; w przypadku własnego zakresu wprowadź daty i kliknij **„Apply”**. Cztery liczniki: **„Requests”**, **„Blocked”** (z wartością procentową), **„Back-office login failures”** oraz **„Refused registrations”**, otwierają odpowiadające im rejestry zdarzeń.

Wykres **„Traffic: total and blocked”** porównuje zapytania **„Total”** oraz **„Blocked”**; użyj kontrolek serii, aby pokazać lub ukryć krzywe. Sekcja **„Blocks by reason”** prezentuje powody: **„Blocked IP”**, **„Country”**, **„Bots”**, **„Too many requests”**, **„Back-office login”** oraz **„Registration”**. Blokady w sklepie są zliczane według powodów od aktualizacji 5.5. Na mapie **„Where blocked requests come from”** kliknij kraj, aby przefiltrować dane. Sekcja **„Top 5”** zawiera zakładki **„IPs”**, **„Bots”** i **„Pages”**. W **„Recent activity”** dostępne są widoki **„Blocked requests”**, **„Back-office logins”** oraz **„Refused registrations”** z akcjami **„Block”**, **„Unblock”** i **„IP card”**.

Przycisk **„IP card”** otwiera panel boczny z krajem, pierwszą i ostatnią wizytą, liczbą odsłon, zablokowanymi zapytaniami, nieudanymi logowaniami, oceną AbuseIPDB (jeśli jest dostępna), ostatnimi

stronami i user-agentem oraz przyciskami **„Block”**/**„Unblock”** i **„Always allow”**. Liczby te opisują zapytania, a nie unikalnych użytkowników. Przy lekkim logowaniu dane o normalnym ruchu są szacunkowe. Zapytania zablokowane przed PrestaShop pojawiają się po zaimportowaniu plików dziennika.

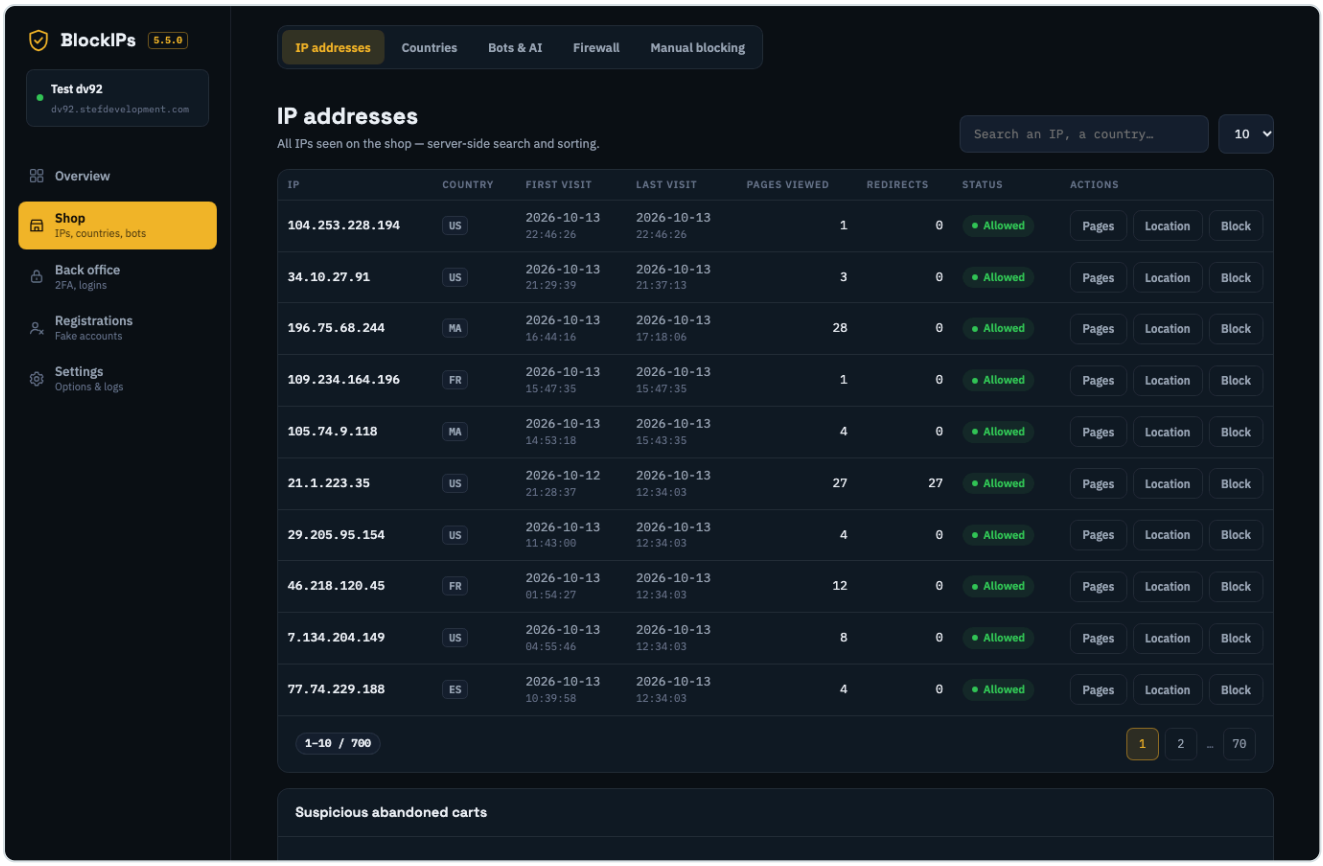


Overview: zabezpieczenia, ruch i zablokowane zapytania w wybranym okresie

4. Blokowanie adresów IP, zakresów i krajów

Pojedyncze adresy

Sekcja **„IP addresses”** zawiera listę adresów zarejestrowanych w sklepie. Możesz wyszukiwać według adresu IP lub kraju. Sprawdź kolumny **„First visit”**, **„Last visit”**, **„Pages viewed”**, **„Redirects”** oraz **„Status”**. W akcjach wiersza użyj opcji **„Block”** lub **„Unblock”**.



Adresy IP i ich aktywność

Aby wprowadzić adresy ręcznie, otwórz **„Shop › Manual blocking”**. W polu **„Block addresses”** wpisz po jednym adresie IPv4 lub IPv6 w wierszu i kliknij **„Block”**. Jeśli dany adres już istnieje, formularz wyświetli powiadomienie; użyj wtedy akcji wiersza w IP addresses, aby go zablokować.

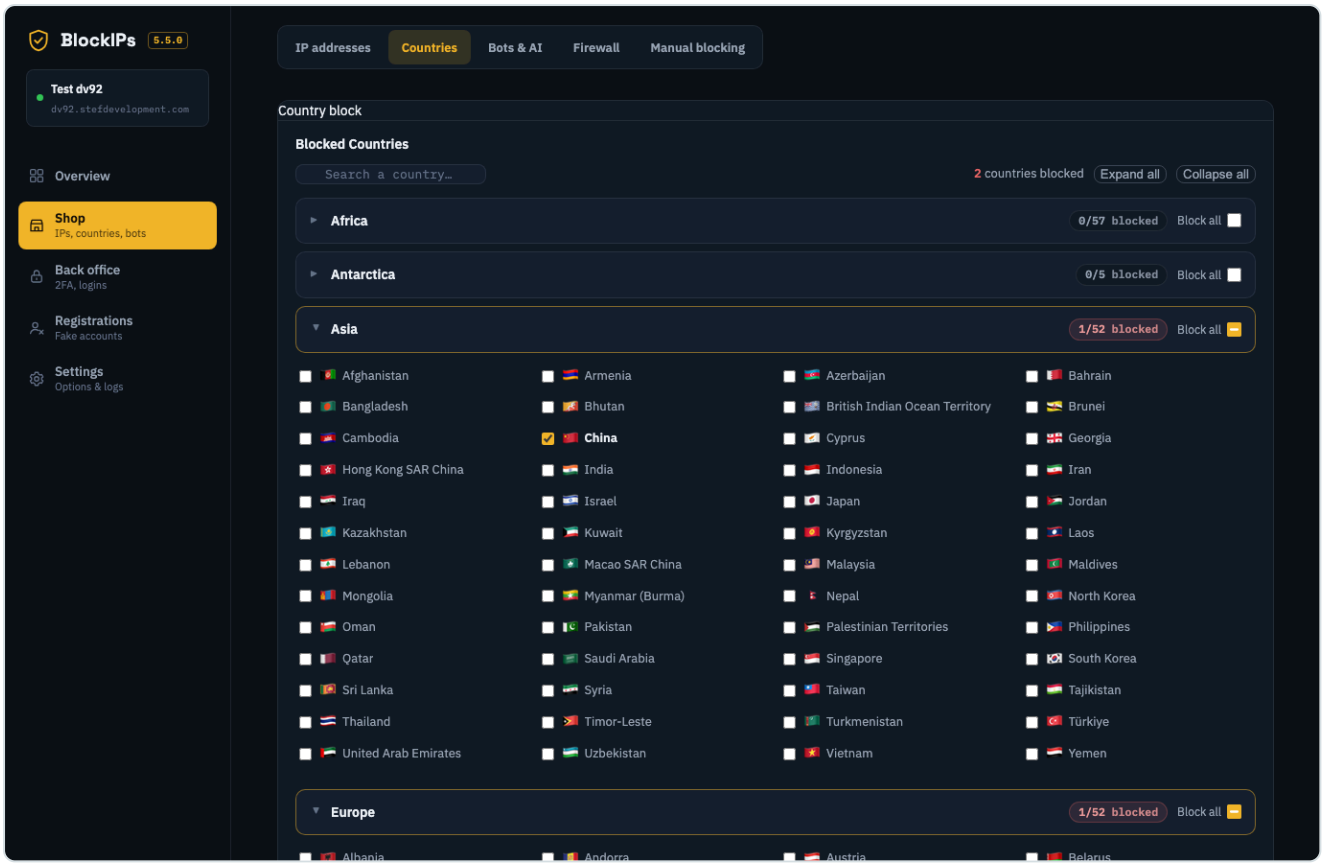
Zaufane adresy i zakresy

W sekcji **„Whitelist”** wprowadź zaufane adresy i kliknij **„Add to whitelist”**. Adresy te omijają blokady sklepu, w tym firewall zapytań. Adresy z białej listy są również wyłączone z limitu nieudanych logowań do back-office.

W sekcji **„IP ranges and wildcards”** wpisz zakres IPv4, np. 192.168.1.1-192.168.1.100, lub maskę z gwiazdką, np. 192.168.*.*. Kliknij **„Add range”**. Lista wyświetli adres początkowy i końcowy. Użyj **„Delete”**, aby usunąć zakres.

Kraje

Otwórz **„Shop › Countries”**. Ekran nosi nagłówek **„Country block”**. Wyszukaj kraj lub rozwiń kontynent. Zaznacz kraje, które chcesz odrzucać, i kliknij **„Save”**. Główne pole wyboru dla kontynentu zaznacza lub odznacza wszystkie należące do niego kraje. Przyciski **„Expand all”** i **„Collapse all”** sterują widokiem listy.



Blokowanie krajów według państwa lub kontynentu

Co widzi zablokowany użytkownik

W **„Settings › Options & Cron”**, w sekcji **„Redirection”**, skonfiguruj **„Behavior for blocked IPs”**. Wybierz **„Show a forbidden message”** lub **„Redirect to a URL”**. Zmodyfikuj **„Forbidden message”** lub **„Redirect URL”**, a następnie kliknij **„Save”**. Domyślnym działaniem jest wyświetlenie komunikatu o braku dostępu.

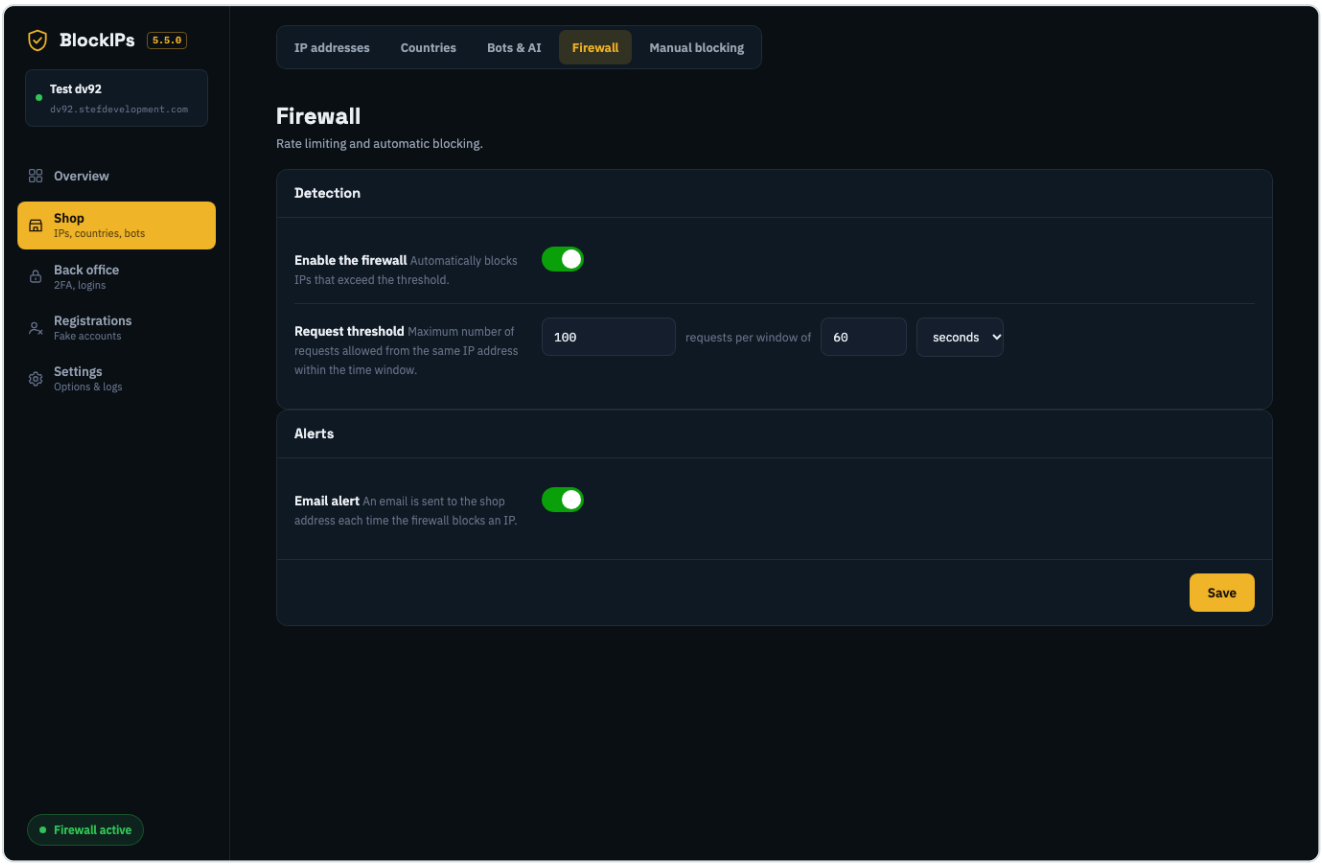
5. Firewall (limit zapytań)

Otwórz **„Shop › Firewall”**. Opcja **„Enable the firewall”** włącza lub wyłącza automatyczną blokadę. **„Request threshold”** określa maksymalną liczbę zapytań z jednego adresu IP w zadanym oknie czasu. Wybierz **„seconds”** lub **„minutes”** i kliknij **„Save”**.

Domyślna wartość po nowej instalacji wynosi **100 zapytań w 60 sekund**. Gdy zarejestrowana liczba zapytań osiągnie próg, adres IP zostaje dodany do zablokowanych adresów sklepu. Jest to blokada IP sklepu, niezależna od tymczasowej blokady nieudanych logowań do back-office. Użyj opcji **„Unblock”** w IP addresses, aby ją zdjąć.

Opcja **„Email alert”** wysyła powiadomienie na adres e-mail sklepu, gdy firewall zablokuje dany adres IP. Jest ona domyślnie włączona. Sprawdź zdarzenia firewalla w panelu głównym, aby przejrzeć wykryte próby.

> Wielu klientów może współdzielić jeden adres IP. Przeanalizuj ich aktywność przed wprowadzeniem bardziej rygorystycznego limitu. Dla zaufanych adresów użyj Whitelist. Lekkie logowanie sprawia, że liczba zapytań jest przybliżona, ponieważ próbkowane wizyty mają przypisaną wagę.



Próg zapytań firewalla i alert e-mail

6. User-agenty i boty AI

Otwórz **„Shop › Bots & AI”**. W sekcji **„Ban a user agent”** wprowadź fragment ciągu, np. GPTBot, i kliknij **„Ban”**. Wielkość liter nie ma znaczenia. Fragment dopasowywany jest w dowolnym miejscu ciągu user-agent. Użyj **„Remove”** w sekcji **„Banned user agents”**, aby cofnąć blokadę.

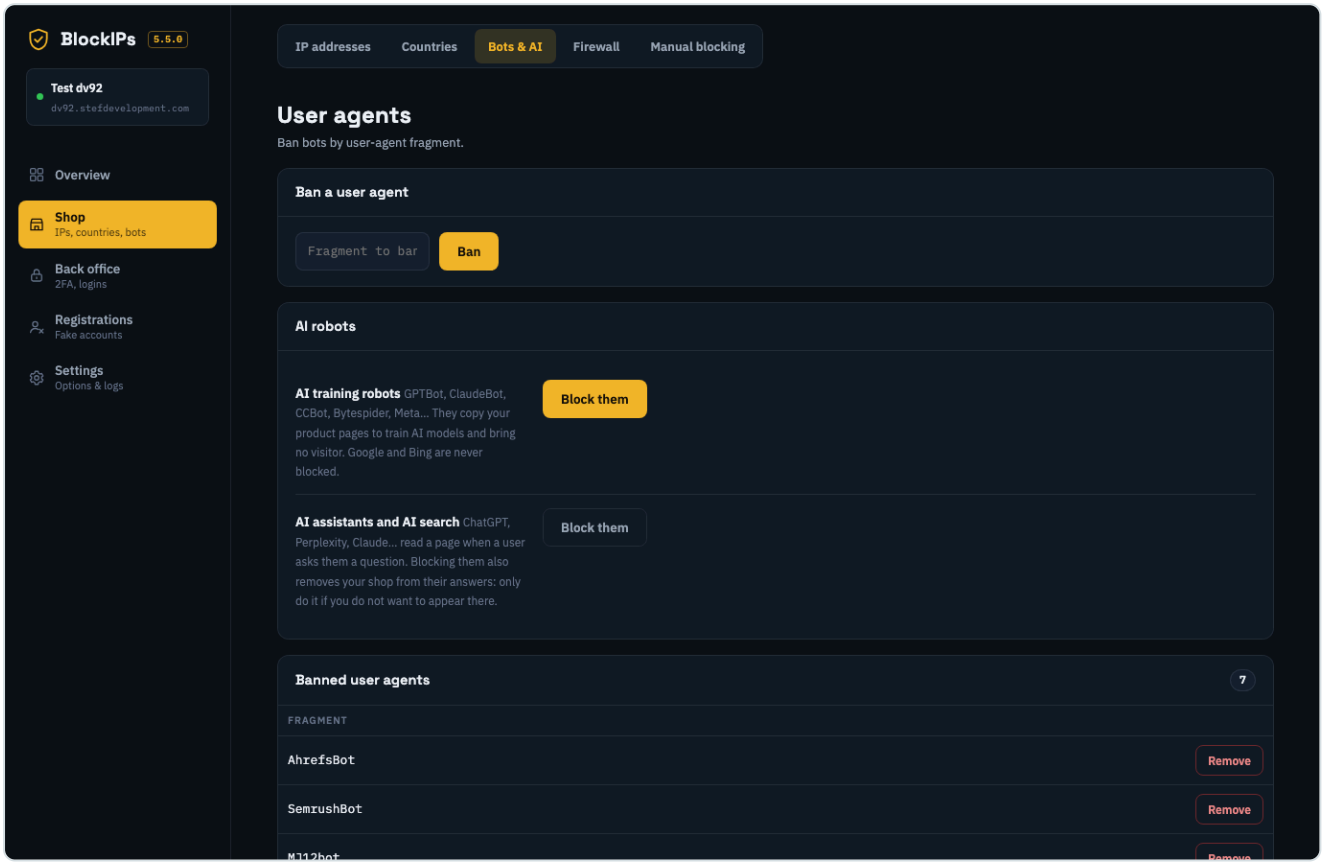
Boty AI

- **„AI training robots”**: kliknij **„Block them”**, aby dodać przygotowaną grupę fragmentów robotów trenujących modele, w tym GPTBot, ClaudeBot, CCBot i Bytespider.
- **„AI assistants and AI search”**: oddzielny przycisk **„Block them”** dodaje fragmenty asystentów oraz wyszukiwarek AI, w tym ChatGPT-User, OAI-SearchBot i PerplexityBot. Zablokowanie ich może uniemożliwić pojawianie się Twoich stron w generowanych odpowiedziach.

Roboty Googlebot i Bingbot nie należą do tych grup AI. Każdy przycisk dodaje fragmenty do listy zablokowanych. Jeśli zechcesz ponownie zezwolić na dany bot, usuń odpowiednie fragmenty pojedynczo.

Podejrzane sieci

Sekcja **„Suspicious networks (last 24 hours)”** wyróżnia pojedynczego user-agenta rozproszonego na wiele adresów IP, wysyłających zaledwie po kilka zapytań każdy. Pomaga to zidentyfikować scraping przez serwery proxy, który stara się utrzymać poniżej limitu firewalla na pojedyncze IP. Przed zablokowaniem sprawdź user-agenta, liczbę adresów oraz łączną liczbę zapytań. Wyszukiwarki internetowe są wykluczone z tej listy.



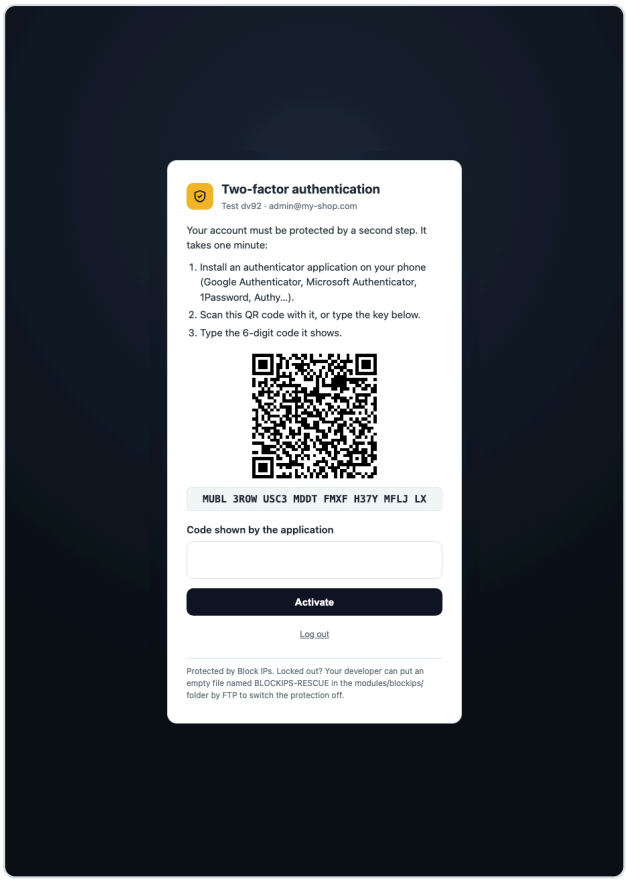
Blokady user-agentów, grupy botów AI i podejrzane sieci

7. Ochrona back-office

Otwórz **„Back-office protection”**. Ten ekran wymaga PrestaShop 1.7.8 lub nowszego. Jego ustawienia oraz ochrona pracowników są współdzielone w całej instalacji.

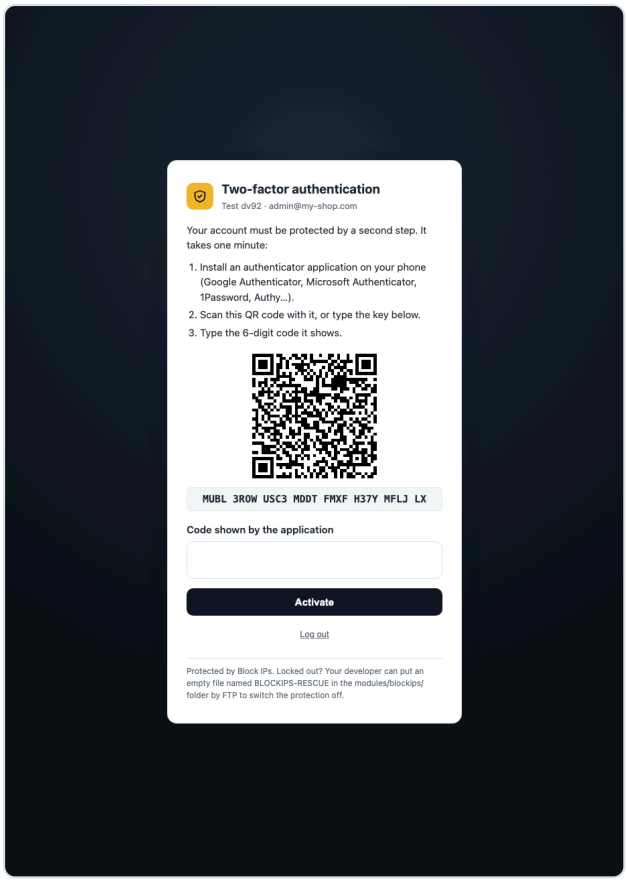
Włączanie uwierzytelniania dwuskładnikowego

1. W sekcji **„My account”** kliknij **„Turn on for my account”**.
2. Zainstaluj aplikację uwierzytelniającą. Zeskanuj kod QR lub wprowadź wyświetlony klucz.
3. Wpisz sześciocyfrowy kod w polu **„Code shown by the application”** i kliknij **„Activate”**.
4. Zapisz kody odzyskiwania w bezpiecznym miejscu. Są one wyświetlane tylko raz. Każdy kod może jednorazowo zastąpić kod z telefonu.
5. Kliknij **„I saved my codes, continue”**.



Konfiguracja w aplikacji uwierzytelniającej

Podczas kolejnych logowań podaj hasło, a następnie kod z aplikacji w polu **„Code”** i kliknij **„Verify”**. W tym samym polu możesz również wpisać niewykorzystany kod odzyskiwania. Oczekujący drugi krok weryfikacji wygasa po dziesięciu minutach.



Etap weryfikacji kodu

Wymóg ochrony dla wybranych profili pracowników

W sekcji **„Mandatory for these profiles”** zaznacz profile, które muszą korzystać z uwierzytelniania dwuskładnikowego, i kliknij **„Save”**. Pracownicy przypisani do tych profili będą musieli skonfigurować 2FA przy kolejnym logowaniu. Najpierw zabezpiecz własne konto. Domyślnie żaden profil nie jest oznaczony jako obowiązkowy.

Ograniczanie nieudanych logowań

Opcja **„Limit failed logins”** jest domyślnie włączona. Domyślny **„Limit”** to **5 nieudanych prób na 15 minut**. Błędne hasła oraz błędne kody wliczają się do tego limitu. Adres IP, który go osiągnie, musi odczekać przed kolejną próbą. Adresy z białej listy są zwolnione z blokady. Dostosuj limit i okno czasowe, a następnie kliknij **„Save”**.

Dozwolone adresy

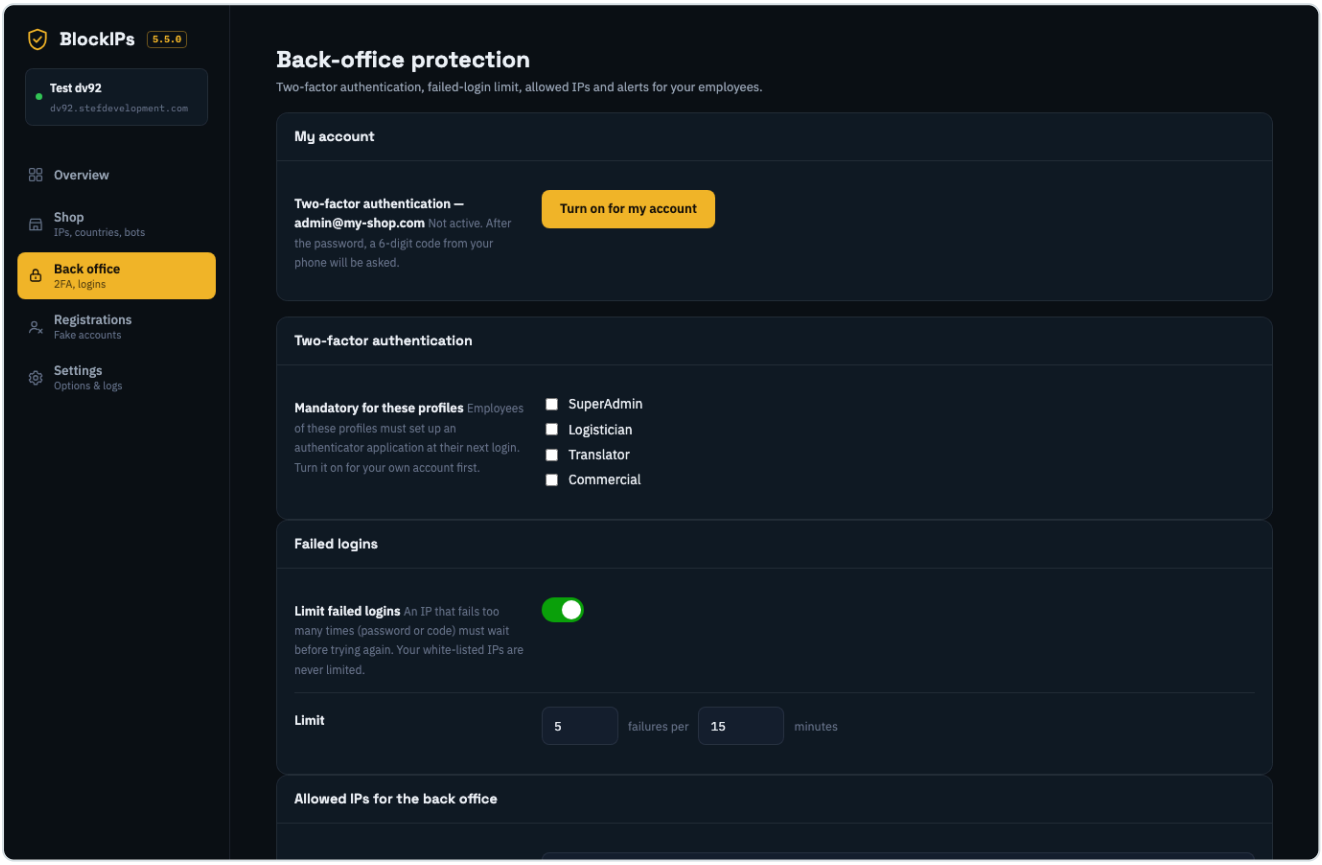
W sekcji **„Allowed IPs for the back office”** uzupełnij pole **„Only these IPs can open the back office”**. Wpisz po jednym adresie IPv4 lub IPv6 albo zakresie CIDR w wierszu. Pozostaw listę pustą, aby zezwolić na dostęp z dowolnego adresu IP — jest to zachowanie domyślne. Moduł wyświetla Twój bieżący adres IP i odrzuca listę, która go nie zawiera. Kliknij **„Save”**.

> Lista dozwolonych adresów IP do back-office jest niezależna od sekcji Whitelist. Wpis na białej liście zwalnia z ograniczeń nieudanych logowań, ale nie zastępuje listy dostępu do back-office ani uwierzytelniania dwuskładnikowego.

Alerty i rejestr logowań

Opcja **„Login from a new device”** wysyła wiadomość e-mail, gdy pracownik zaloguje się przy użyciu kombinacji adresu IP i przeglądarki niewidzianej od 90 dni. **„Logins blocked”** informuje mailowo, gdy adres IP osiągnie limit nieudanych prób logowania. Oba alerty są domyślnie aktywne. Wypełnij pole **„Send the alerts to”** lub pozostaw je puste, aby użyć adresu e-mail sklepu, a następnie kliknij **„Save”**.

Sekcja **„Employees”** przedstawia stan 2FA każdego pracownika oraz liczbę pozostałych kodów odzyskiwania. **„Login journal”** rejestruje daty, zdarzenia, pracowników, adresy IP i przeglądarki. Domyślny okres przechowywania rejestru wynosi 90 dni.



Ustawienia ochrony pracowników, alerty i rejestr logowań

Utrata telefonu lub brak dostępu

Użyj niewykorzystanego kodu odzyskiwania. Inny administrator może również kliknąć **„Reset (lost phone)”** na liście Employees. Jeśli Twój profil wymaga uwierzytelniania dwuskładnikowego, konieczne będzie ponowne przejście konfiguracji. Opcja **„Turn off for my account”** wyłącza zabezpieczenie dla Twojego konta.

Jeśli nikt nie ma dostępu do back-office, połącz się przez FTP i utwórz pusty plik o nazwie **BLOCKIPS-RESCUE** w katalogu **modules/blockips/**. Spowoduje to wyłączenie ochrony back-office modułu na czas istnienia tego pliku. Zaloguj się, popraw ustawienia lub zresetuj konfigurację konta, a następnie usuń plik, aby przywrócić ochronę. Gdy plik jest obecny, na ekranie wyświetla się ostrzeżenie o aktywnym trybie ratunkowym.

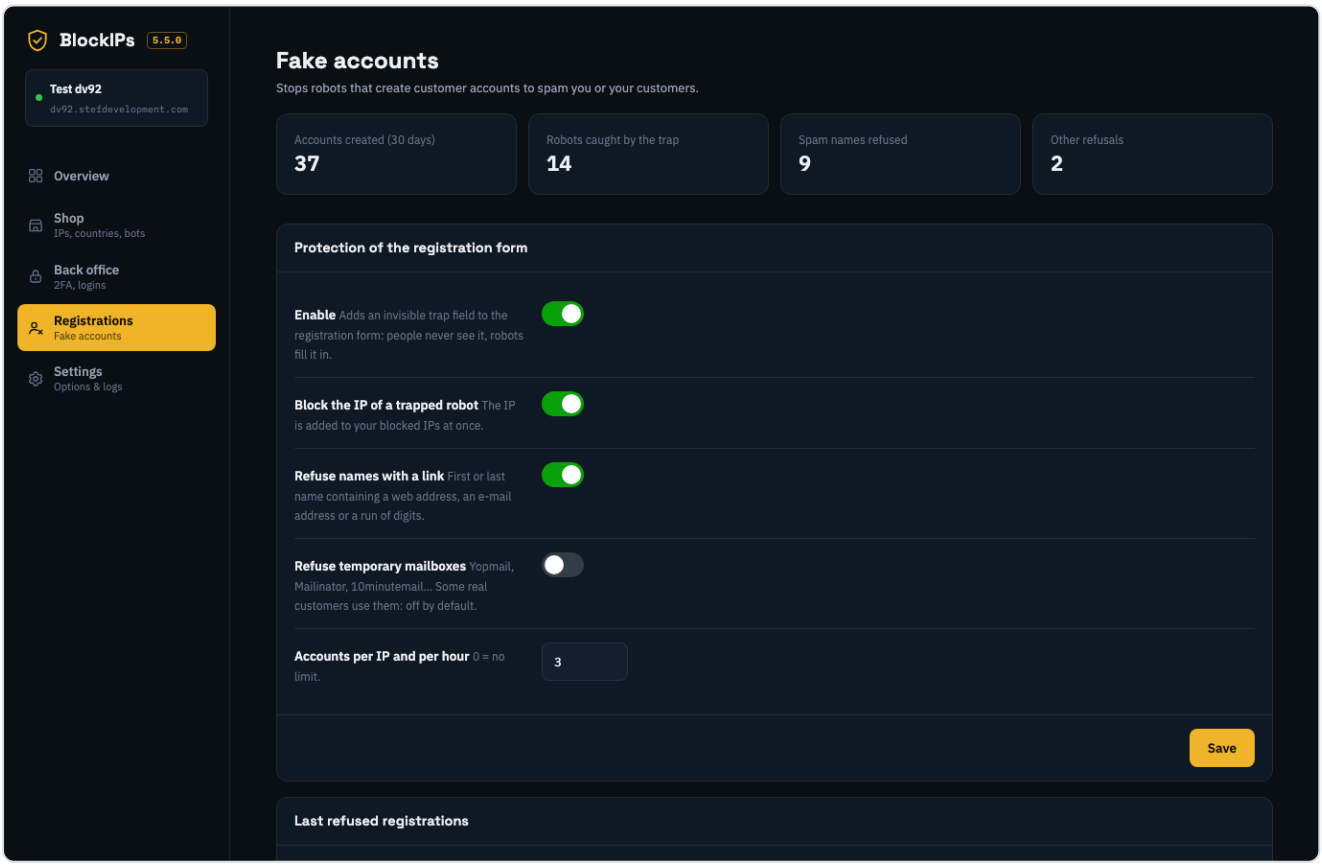
> Tryb ratunkowy wyłącza także sprawdzanie fałszywych kont. Pamiętaj o usunięciu pliku ratunkowego po odzyskaniu dostępu.

8. Fałszywe konta

Otwórz **„Fake accounts”**, aby zabezpieczyć formularz rejestracji klientów. Funkcja ta kontroluje zgłoszenia za pomocą standardowych hooków rejestracji PrestaShop od 1.7 do 9. Jej ustawienia są współdzielone w całej instalacji.

- **„Enable”**: dodaje niewidoczne pole-pułapkę. Formularz, w którym pole to zostanie wypełnione, zostaje odrzucony. Domyślnie włączone.
- **„Block the IP of a trapped robot”**: dodaje adres IP złapanego bota do zablokowanych adresów. Domyślnie włączone.
- **„Refuse names with a link”**: sprawdza, czy imię lub nazwisko zawiera adres strony internetowej, adres e-mail lub ciąg cyfr. Domyślnie włączone.
- **„Refuse temporary mailboxes”**: odrzuca znane domeny jednorazowych skrzynek e-mail. Domyślnie wyłączone, ponieważ mogą z nich korzystać rzeczywiści klienci.
- **„Accounts per IP and per hour”**: domyślnie wynosi **3**. Ustaw **0**, aby wyłączyć limit.

Kliknij **„Save”**. Liczniki pokazują aktywność w ciągu ostatnich 30 dni. Tabela **„Last refused registrations”** prezentuje datę, powód, adres e-mail i adres IP ostatnich odrzuconych rejestracji. Sprawdzanie to działa na nowe rejestracje i nie usuwa kont już istniejących.



Ustawienia fałszywych kont i odrzucone rejestracje

9. Reputacja (AbuseIPDB i Slack)

Sekcja **„Reputation”** umożliwia sprawdzanie zarejestrowanych adresów IP w AbuseIPDB za pomocą zaplanowanego zadania cron. Wprowadź własny **„AbuseIPDB API key”** dla wybranego sklepu. Pozostawienie pustego klucza wyłącza sprawdzanie. Skonfiguruj opcje i kliknij **„Save”**.

- **„High-score threshold”**: domyślnie wynosi **80**. Wynik równy lub wyższy od tej wartości jest uznawany za wysoki. Punktacja mieści się w zakresie od 0 do 100.
- **„Daily cap”**: domyślnie wynosi **1 000** sprawdzeń na sklep. Dostosuj wartość do limitu swojego pakietu API. Sprawdzanie zatrzymuje się po osiągnięciu limitu i może zostać wznowione następnego dnia.
- **„Automatically block high-score IPs”**: domyślnie wyłączone. Po włączeniu adresy spełniające kryterium są automatycznie dodawane do zablokowanych IP.
- **„Email alert for new high-score IPs”**: domyślnie wyłączone. Wysyła podsumowanie nowo wykrytych adresów IP o wysokim wskaźniku ryzyka na adres e-mail sklepu.
- **„Slack alert for new high-score IPs”**: domyślnie wyłączone. Wpisz **„Slack webhook URL”** i włącz tę opcję, aby otrzymywać powiadomienia przez przychodzący webhook. Obsługiwane są również punkty końcowe kompatybilne ze Slack.

Zaplanuj zadanie **„Reputation”** lub **„Run all”** w sekcji Options & Cron. Zadanie przetwarza kwalifikujące się adresy IP niemające jeszcze zapisanego wyniku. Pomija adresy z białej listy oraz adresy już zablokowane. Sprawdzanie odbywa się w tle, bez spowalniania zapytań klientów.

Ekran wyświetla **„Daily quota”**, **„Checks over the last 10 days”** oraz **„High-score IPs”**. Przeanalizuj ocenę i status przed wykonaniem dostępnych akcji: **„Block”**, **„Unblock”** lub **„Whitelist”**. Jeśli wywołanie API nie powiedzie się lub zwróci nieprawidłowy wynik, adres IP pozostaje bez oceny do kolejnej próby.

10. Opcje wydajności

Otwórz **„Options & Cron”**, a następnie **„Performance and advanced protection”**. Ustawienia te są współdzielone w całej instalacji.

Blokowanie przed uruchomieniem PrestaShop (.htaccess)

Włącz opcję **„Block before PrestaShop”** i kliknij **„Save”**. Na serwerze Apache moduł zapisuje reguły w głównym pliku .htaccess sklepu. Zablokowane user-agenty są odrzucane, zanim PrestaShop w ogóle się uruchomi. Zapobiega to wykonywaniu zapytań do bazy danych przy każdym zablokowanym żądaniu. Rozwiązanie to nie przenosi jednak wszystkich reguł adresów IP, krajów ani limitów zapytań do konfiguracji Apache.

Plik .htaccess musi istnieć i posiadać uprawnienia do zapisu. Po zapisaniu sprawdź parametr **„Status”**. Jeśli reguł nie można zapisać, moduł pozostawia tę opcję wyłączoną. Serwery takie jak Nginx nadal realizują blokowanie wewnątrz PrestaShop.

Zapytania zablokowane przez serwer są zapisywane w plikach i importowane partiami. Zwykły ruch w sklepie może wywołać import najwyżej raz na pięć minut. Zadanie **„Run all”** również je importuje. Użyj przycisku **„Import blocked requests now”**, aby natychmiast zaktualizować dane w „Overview”.

Przestarzałe przeglądarki na stronach filtrów

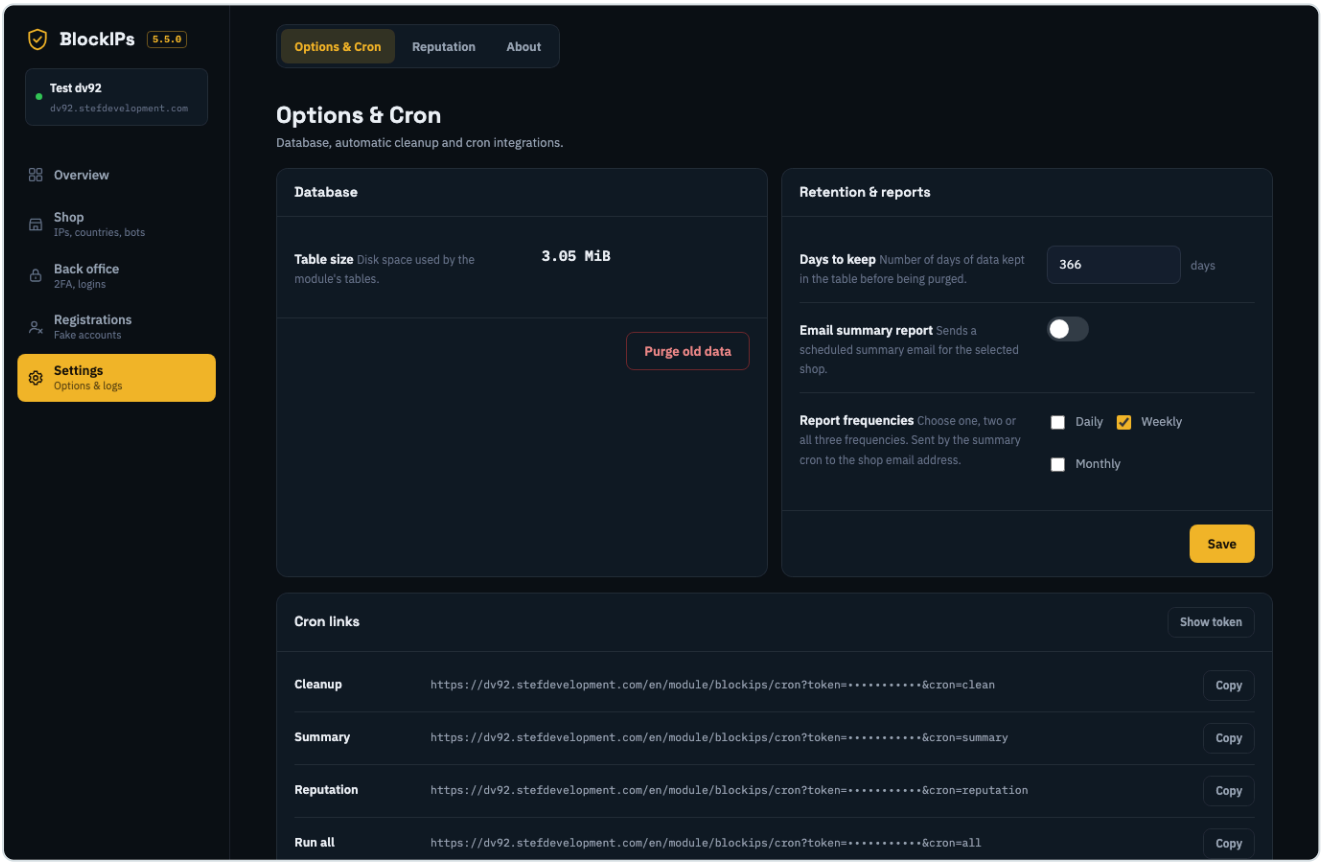
Wybierz **„Do not block”**, **„Older than 1 year”**, **„Older than 18 months”** lub **„Older than 2 years”**. Reguła ta sprawdza stare wersje Chrome na stronach wyszukiwania fasetowego zawierających w adresie URL parametr ?q=. Nie blokuje zwykłych stron sklepu tylko dlatego, że przeglądarka jest nieaktualna. Domyślnie reguła ta jest wyłączona.

Lekkie logowanie

Ustawienie **„Off: record every visit”** zachowuje pełne logowanie. Opcja próbkowania rejestruje jedną zwykłą wizytę na N i zlicza ją N-krotnie. Statystyki pozostają średnio prawidłowe, lecz indywidualne zliczenia ruchu oraz limit zapytań stają się wartościami przybliżonymi. Zablokowane wizyty, zalogowani klienci oraz odwiedzający z koszykiem są rejestrowani zawsze. Po wybraniu ustawień kliknij **„Save”**.

Prawdziwe IP Cloudflare

Moduł automatycznie odczytuje nagłówek CF-Connecting-IP, gdy łączący się serwer należy do znanych zakresów Cloudflare, a nagłówek zawiera prawidłowy adres IP. Dotyczy to zarówno ruchu w sklepie, jak i ochrony back-office. Zapobiega to traktowaniu wszystkich odwiedzających jako pochodzących z tego samego serwera Cloudflare. Żaden dodatkowy przełącznik nie jest wymagany.



Opcje, zaplanowane zadania i ustawienia wydajności

Przechowywanie danych i raporty

W sekcji **„Retention & reports”** ustaw wartość **„Days to keep”**. Domyślna wartość wynosi **366 dni**. Kliknij **„Save”**, a następnie użyj przycisku **„Purge old data”** lub zaplanuj zadanie Cleanup. Pole **„Table size”** pokazuje rozmiar bazy danych zajmowany przez moduł.

Opcja **„Email summary report”** jest domyślnie wyłączona. Włącz ją i wybierz częstotliwość: **„Daily”**, **„Weekly”**, **„Monthly”** lub kilka z nich. Początkowo wybrana jest opcja Weekly. Zadanie Summary lub Run all wysyła należne raporty na adres e-mail sklepu.

11. Pytania i rozwiązywanie problemów

Prawidłowy użytkownik został zablokowany

Wyszukaj adres w sekcji „Shop › IP addresses” i przeanalizuj jego aktywność. Sprawdź status wiersza, reguły zakresów, wybrane kraje oraz zablokowane user-agenty. Użyj Unblock, aby zdjąć pojedynczą blokadę. Usuń lub dostosuj każdą inną pasującą regułę. W razie potrzeby dodaj zaufany adres do Whitelist.

Firewall blokuje zbyt wielu klientów

Sprawdź Request threshold i jednostkę czasu. Współdzielone adresy mogą łączyć ruch wielu klientów. W razie potrzeby zwiększ limit. Jeśli włączone jest lekkie logowanie, pamiętaj, że liczba zapytań jest wartością ważoną, a nie dokładną.

Zapytania zablokowane przez serwer nie pojawiają się w „Overview”

Sprawdź Status w opcjach wydajności i kliknij Import blocked requests now. Upewnij się, że zadanie Run all jest zaplanowane w harmonogramie. Zapytania zapisane w plikach dziennika serwera pojawią się dopiero po imporcie.

Nie można włączyć „Block before PrestaShop”

Sprawdź, czy serwer obsługuje reguły przepisywania Apache oraz czy główny plik .htaccess istnieje i posiada uprawnienia do zapisu. Przeczytaj komunikat o stanie. Blokowanie w sklepie nadal działa wewnątrz PrestaShop, nawet gdy reguły serwera są niedostępne.

Sprawdzanie reputacji nie zwraca wyników

Sprawdź klucz API dla wybranego sklepu, Daily cap oraz zaplanowane zadanie Reputation lub Run all. Przejrzyj odpowiedź zadania. Adresy już ocenione, znajdujące się na białej liście lub już zablokowane nie są kwalifikowane jako nowi kandydaci.

Wiadomości z podsumowaniem nie docierają

Sprawdź Email summary report, wybrane częstotliwości oraz adres e-mail sklepu. Zaplanuj zadanie Summary lub Run all. Raporty są wysyłane w wyznaczonych terminach, a nie przy każdym wywołaniu zadania. Sprawdź również konfigurację poczty e-mail w swoim sklepie.

Formularz rejestracji omija zabezpieczenia

Upewnij się, że opcja Fake accounts jest włączona i nie pozostał żaden plik ratunkowy. Niestandardowy proces rejestracji musi wywoływać standardowe hooki rejestracji konta, aby sprawdzanie mogło zadziałać.

Kod z aplikacji uwierzytelniającej jest odrzucany

Sprawdź czas w telefonie i upewnij się, że używasz aktualnego kodu dla tego sklepu. W razie potrzeby wprowadź niewykorzystany kod odzyskiwania. Poproś innego administratora o kliknięcie Reset (lost phone), a następnie skonfiguruj konto ponownie. W razie całkowitej utraty dostępu postępuj zgodnie z procedurą BLOCKIPS-RESCUE opisaną w rozdziale Ochrona back-office.

Ustawienia wpływają na inny sklep

Przed konfiguracją reguł wybierz pojedynczy sklep. Ochrona back-office, ustawienia fałszywych kont, Whitelist oraz opcje wydajności są współdzielone. Reguły Apache łączą blokady user-agentów ze wszystkich sklepów w danej instalacji.

Kontakt z pomocą techniczną

Skontaktuj się ze sprzedawcą modułu za pośrednictwem swojego konta PrestaShop Addons. Podaj wersję PrestaShop, wersję modułu, ekran, którego dotyczy problem, oraz kroki pozwalające go odtworzyć. Przed przesłaniem jakichkolwiek materiałów usuń tokeny, klucze API, kody odzyskiwania oraz sekrety aplikacji uwierzytelniającej.