Total Security Bedienungsanleitung

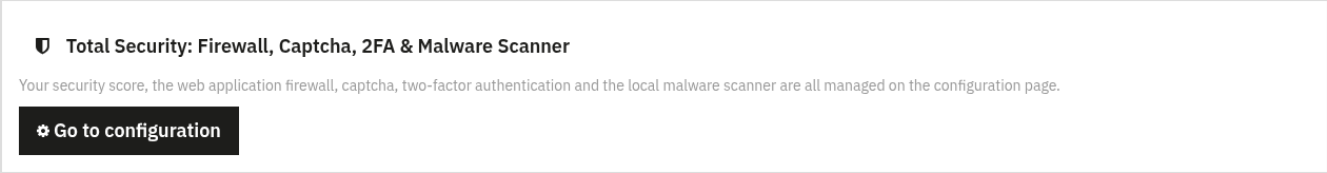
PrestaShop-Modul · Kompatibel mit PrestaShop 1.7 → 9

Firewall, Captcha, 2FA und Malware-Scanner, in einem Modul

Total Security vereint in einem einzigen Modul eine Web Application Firewall, ein Captcha für die Formulare Ihres Shops, die Zwei-Faktor-Authentifizierung (2FA) für Backoffice und Kunden, einen lokalen Malware-/Webshell-Scanner und einen Live-Sicherheits-Score, der Ihnen zeigt, was Sie verbessern können. Alles läuft auf Ihrem eigenen Server: Nichts verlässt Ihren Shop. Keine Programmierung, keine Theme-Anpassungen.

1. Installation

1. Gehen Sie im Backoffice zu **Module → Modul-Manager → Modul hochladen** und wählen Sie die ZIP-Datei des Moduls aus.
2. Klicken Sie nach der Installation auf **Konfigurieren**. Es öffnet sich ein kurzes Panel mit einer Schaltfläche **Zur Konfiguration**, die zur vollständigen Seite führt.



Das Panel „Konfigurieren" öffnet die vollständige Konfigurationsseite

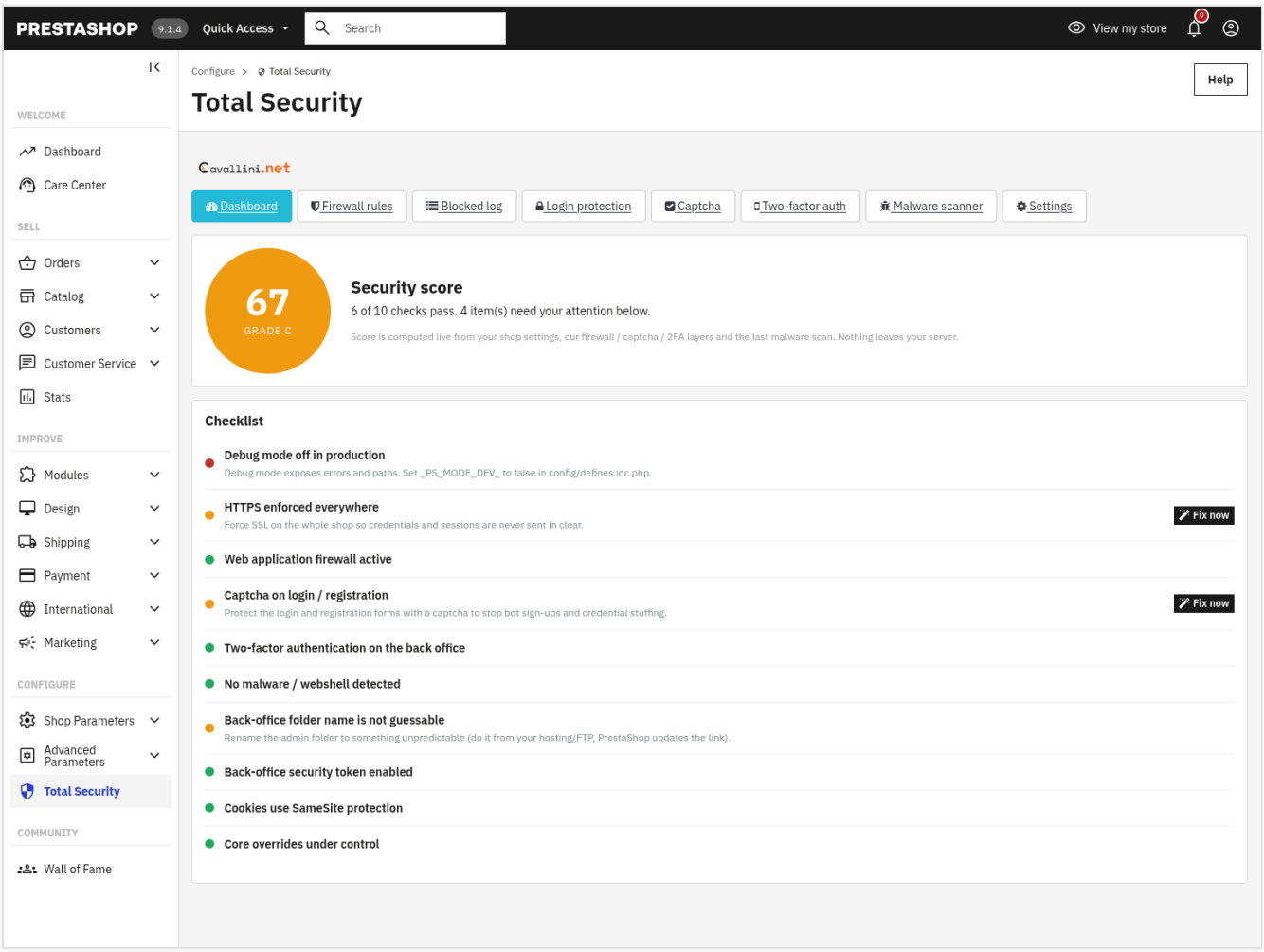
> **Updates erfolgen automatisch.** Updates sind inklusive. Entwicklungsdomains (`.local` , `.test` , `localhost`) sind immer erlaubt. Sobald eine neue Version verfügbar ist, wird sie direkt im Modul angezeigt.

2. Konfiguration — die Tabs

Die Modulseite ist oben in Tabs gegliedert: **Dashboard**, **Firewall-Regeln**, **Blockierungsprotokoll**, **Anmeldeschutz**, **Captcha**, **Zwei-Faktor-Authentifizierung**, **Malware-Scanner** und **Einstellungen**.

Dashboard Sicherheits-Score

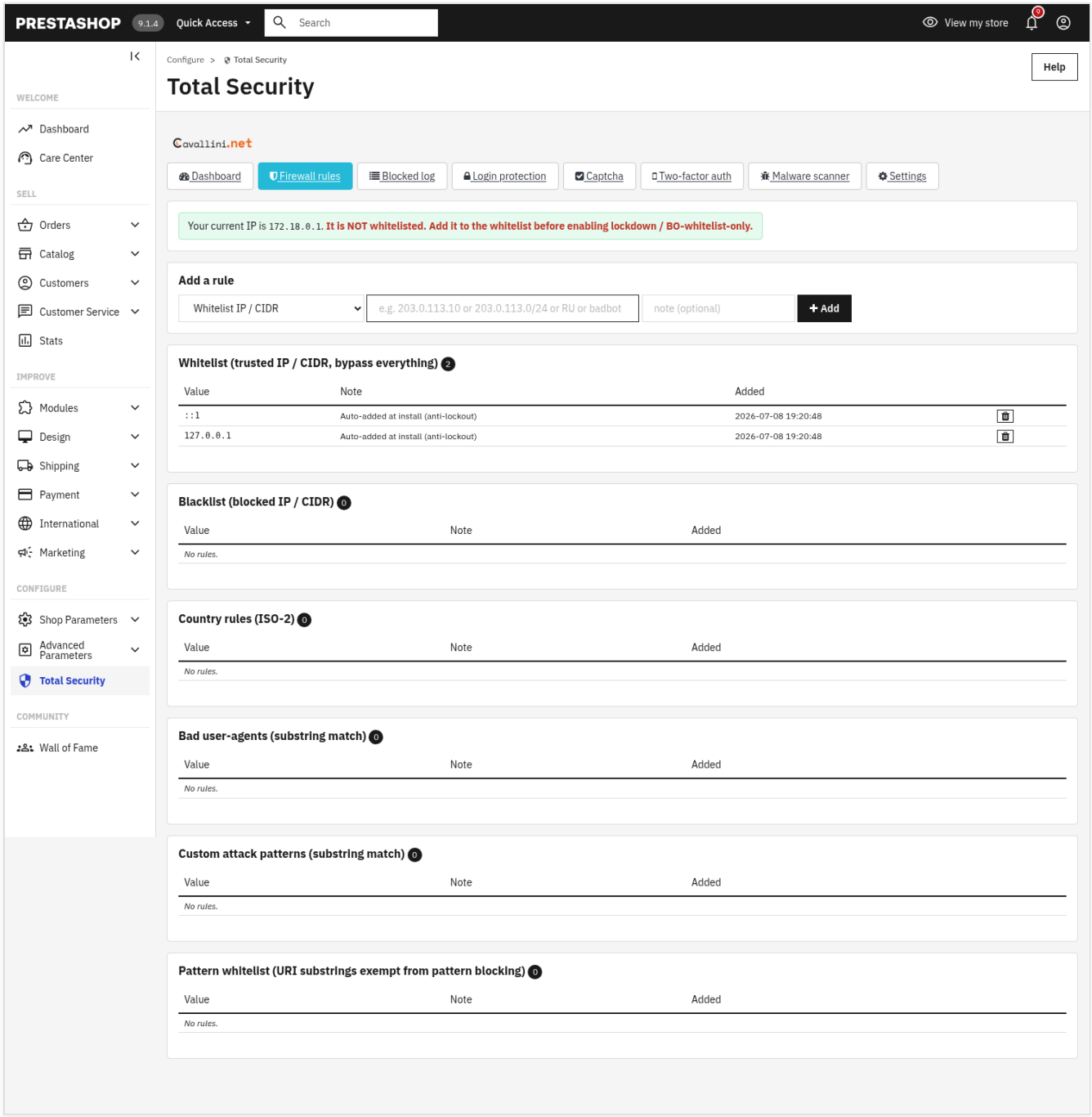
Ein **Sicherheits-Score** in Echtzeit mit einer Buchstabennote (A/B/C/D), berechnet aus den Einstellungen Ihres Shops, den Firewall-/Captcha-/2FA-Ebenen und dem letzten Malware-Scan (nichts verlässt Ihren Server). Darunter finden Sie eine **Checkliste** mit Sicherheitsprüfungen (sichtbare Beispiele: Debug-Modus in der Produktivumgebung deaktiviert, HTTPS überall erzwungen, Web Application Firewall aktiv, Captcha bei Anmeldung/Registrierung, Zwei-Faktor-Authentifizierung im Backoffice, kein Malware/Webshell gefunden, Ordnername des Backoffice nicht erratbar, Sicherheitstoken des Backoffice aktiviert). Punkte, die Aufmerksamkeit benötigen, zeigen eine Verknüpfung **Jetzt beheben**, die direkt zur betreffenden Einstellung springt.



Dashboard — Sicherheits-Score und Checkliste

Firewall-Regeln

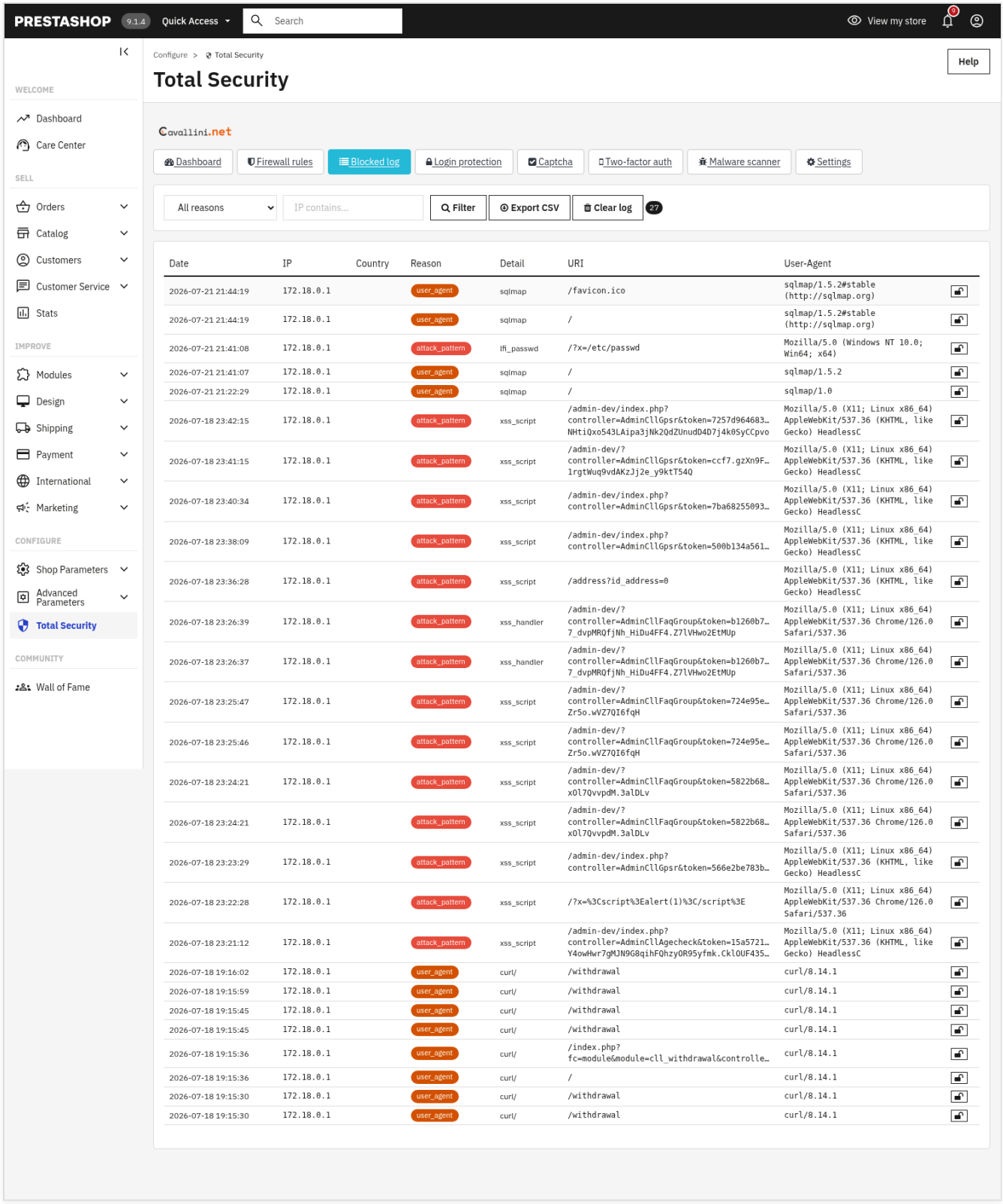
Verwalten Sie die Regellisten über ein einziges Formular **Regel hinzufügen**: **Whitelist IP/CIDR** (vertrauenswürdige Adressen, die alle Prüfungen umgehen), **Blacklist IP/CIDR** (gesperrte Adressen), **Länderregeln** (ISO-2-Codes), **Unerwünschte User-Agents** (Teilstring-Abgleich), **Benutzerdefinierte Angriffsmuster** (Teilstring-Abgleich) und eine **Muster-Whitelist** (URI-Teilstrings, die vom Muster-Blocking ausgenommen sind). Ein Banner zeigt Ihre aktuelle IP an und warnt Sie, diese zur Whitelist hinzuzufügen, bevor Sie den Lockdown-Modus oder die Beschränkung des Backoffice auf Whitelist-IPs aktivieren, damit Sie sich nie selbst aussperren.



Firewall-Regeln — Whitelist, Blacklist, Länder, User-Agents und Muster

Blockierungsprotokoll

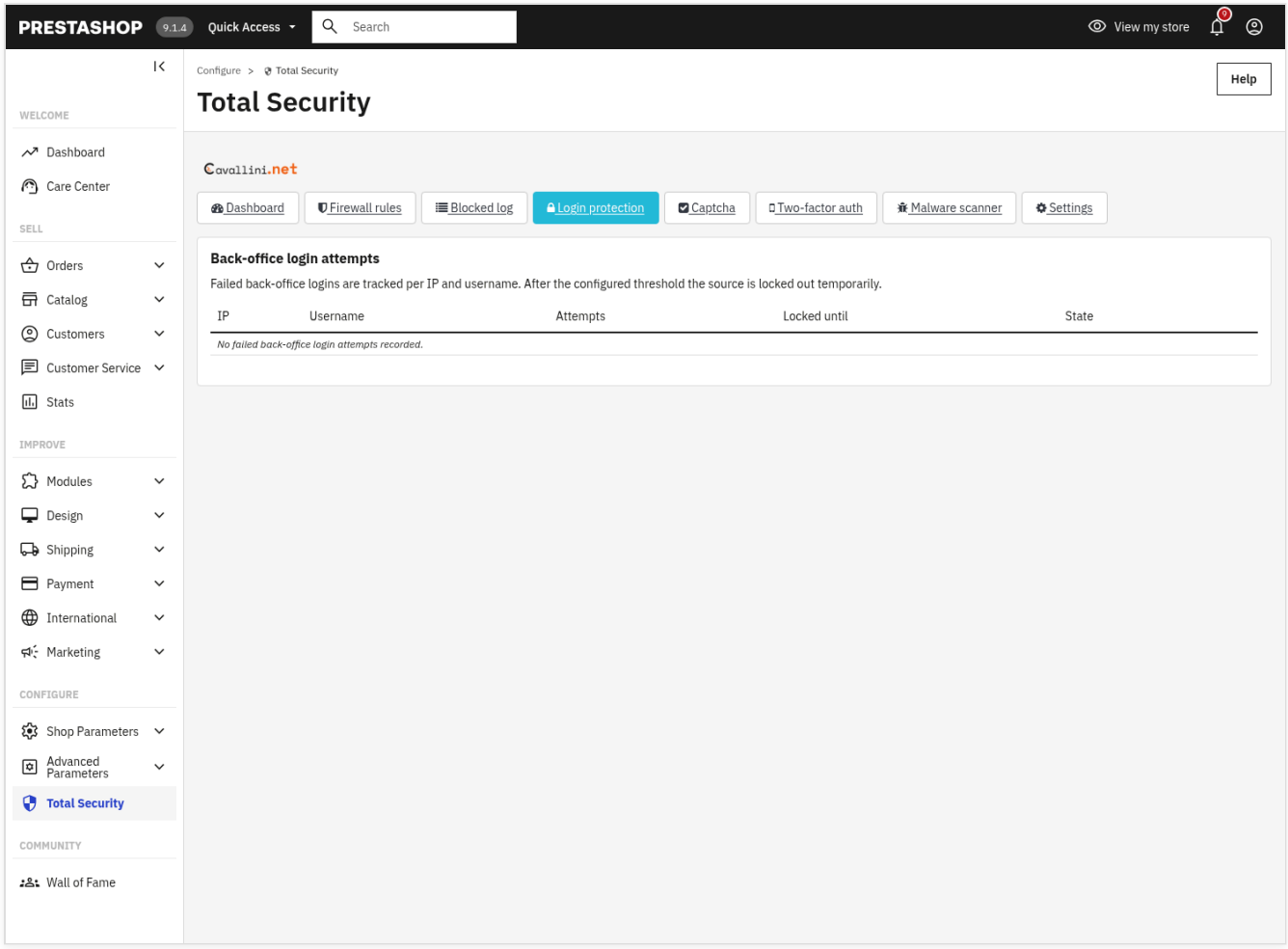
Jede blockierte Anfrage wird mit Datum, IP, Land, Grund (z. B. `user_agent`, `attack_pattern`, `ip`, `rate`, `login`), Detail, angeforderter URI und User-Agent protokolliert. Filtern Sie nach Grund oder IP, nutzen Sie **CSV exportieren**, **Protokoll leeren** oder entsperren Sie eine IP direkt von hier aus.



Blockierungsprotokoll — filtern, exportieren oder eine IP entsperren

Anmeldeschutz

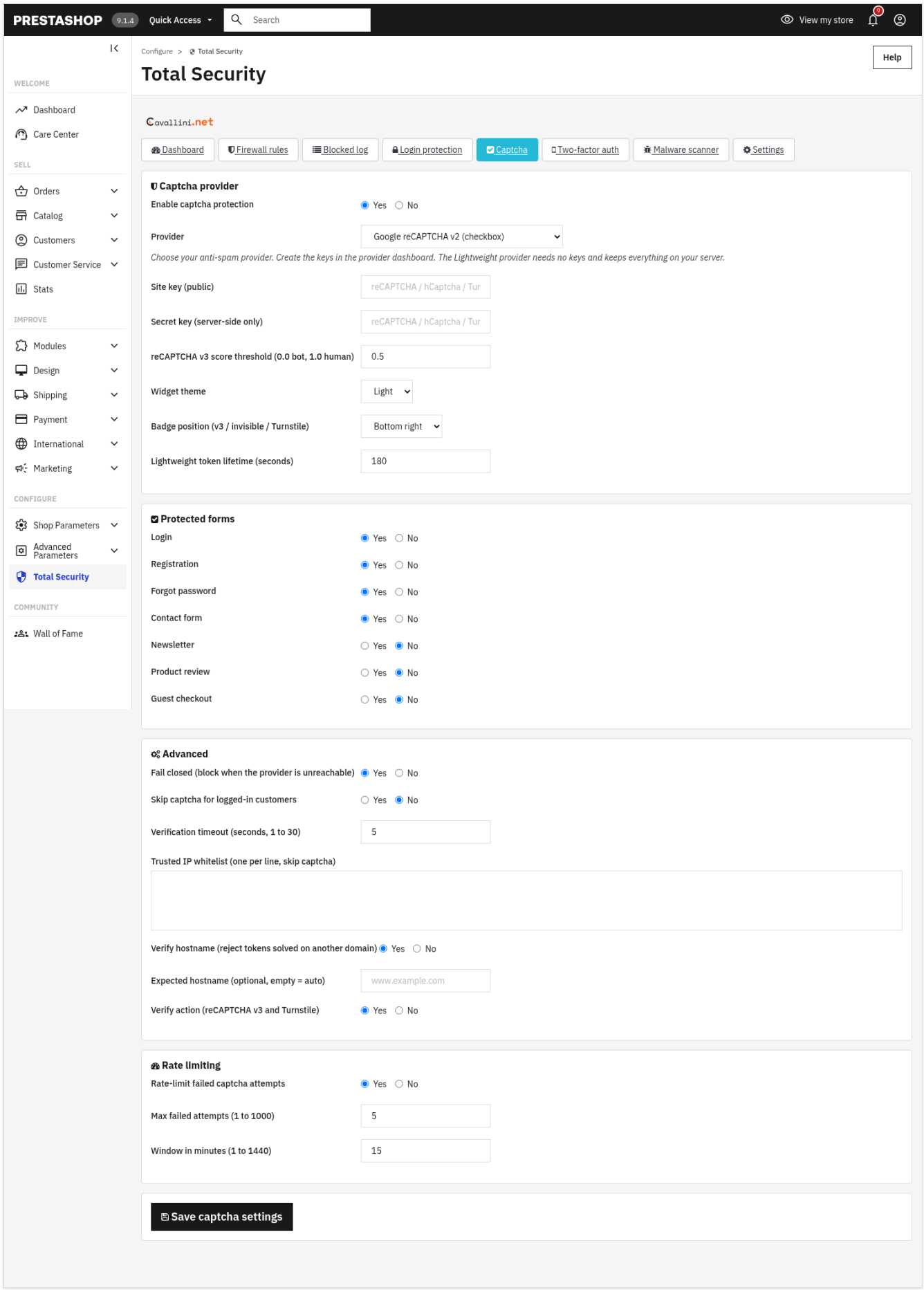
Erfasst Anmeldeversuche im Backoffice und sperrt ein Konto/eine IP nach zu vielen fehlgeschlagenen Versuchen innerhalb eines Zeitfensters; Sie können einen Eintrag manuell entsperren. Die Schwellenwerte konfigurieren Sie in den Einstellungen (Anmeldeschutz für das Backoffice).



Anmeldeschutz — fehlgeschlagene Versuche und aktive Sperren

Captcha

- **Captcha-Anbieter** — wählen Sie Google reCAPTCHA v2 (Kontrollkästchen), reCAPTCHA v3, hCaptcha, Cloudflare Turnstile oder den **Lightweight**-Anbieter, der keine Schlüssel benötigt und vollständig auf Ihrem Server bleibt.
- **Website-Schlüssel / Geheimer Schlüssel** — aus dem Dashboard des gewählten Anbieters, **Score-Schwellenwert für reCAPTCHA v3**, **Widget-Design**, **Badge-Position**, **Gültigkeitsdauer des Lightweight-Tokens**.
- **Geschützte Formulare** — Anmeldung, Registrierung, Passwort vergessen, Kontaktformular, Newsletter, Produktbewertung, Gast-Checkout (jeweils ein-/ausschaltbar).
- **Erweitert** — **Fail closed** (blockieren, wenn der Anbieter nicht erreichbar ist), **Captcha für angemeldete Kunden überspringen**, **Timeout für die Prüfung**, **Whitelist vertrauenswürdiger IPs**, **Hostname-Prüfung**, **Action-Prüfung**.
- **Rate Limiting** — begrenzt fehlgeschlagene Captcha-Versuche mit einem Maximum und einem Zeitfenster.

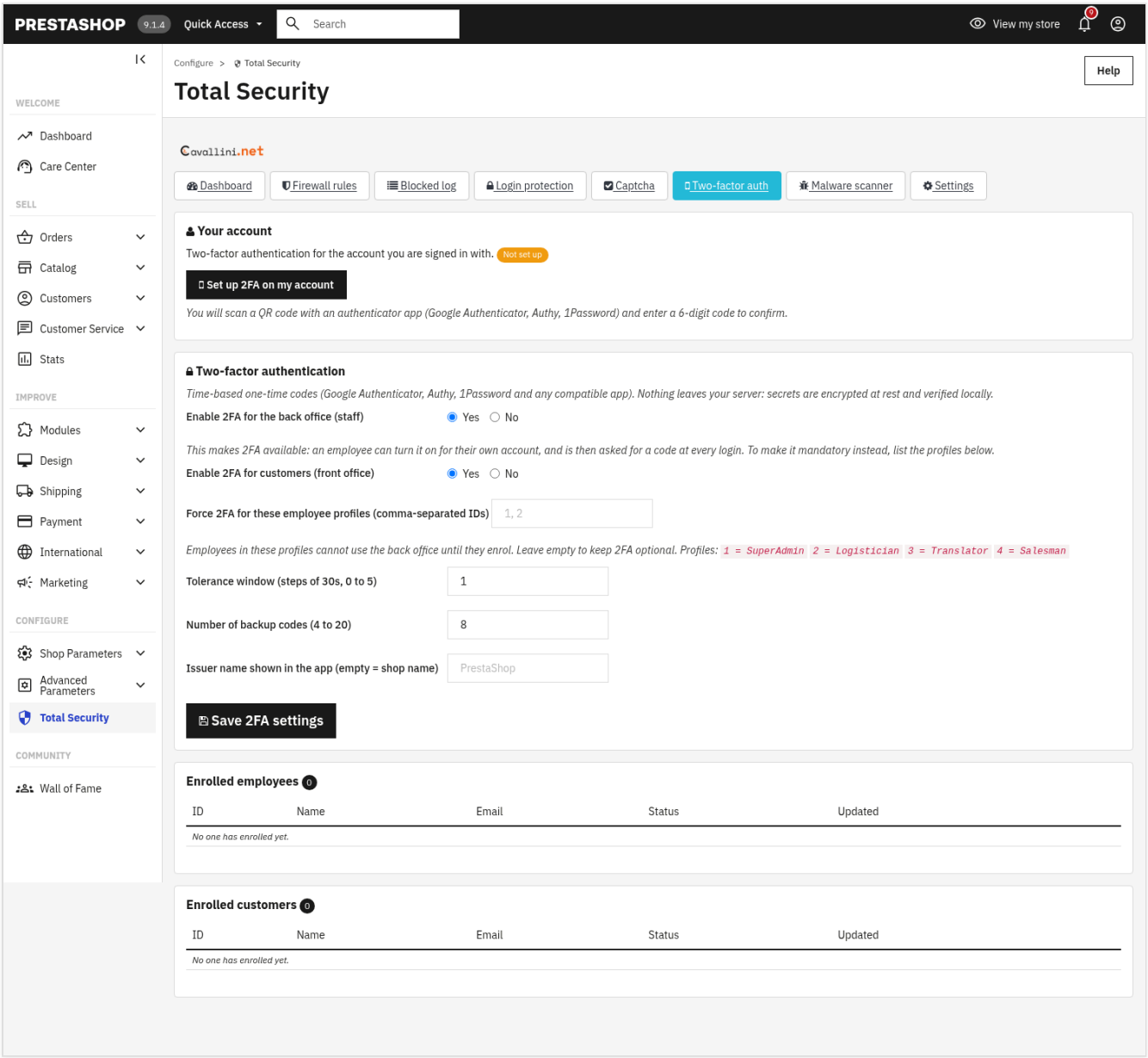


Captcha — Anbieter, geschützte Formulare und Rate Limiting

Zwei-Faktor-Authentifizierung (2FA)

Zeitbasierte Einmalcodes (Google Authenticator, Authy, 1Password und jede kompatible App). Nichts verlässt Ihren Server: Die Secrets werden verschlüsselt gespeichert und lokal verifiziert.

- **Ihr Konto** — richten Sie die 2FA für das Konto ein, mit dem Sie angemeldet sind (QR-Code scannen, 6-stelligen Code eingeben).
- **2FA für das Backoffice aktivieren** (Mitarbeiter) und/oder **für Kunden** (Frontoffice).
- **2FA für bestimmte Mitarbeiterprofile erzwingen**, nach ID (1 = SuperAdmin, 2 = Logistiker, 3 = Übersetzer, 4 = Verkäufer); die aufgeführten Profile können das Backoffice erst nutzen, nachdem sie sich registriert haben.
- **Toleranzfenster**, **Anzahl der Backup-Codes**, **in der App angezeigter Ausstellername**.
- **Registrierte Mitarbeiter** und **registrierte Kunden** werden aufgelistet und können zurückgesetzt werden.

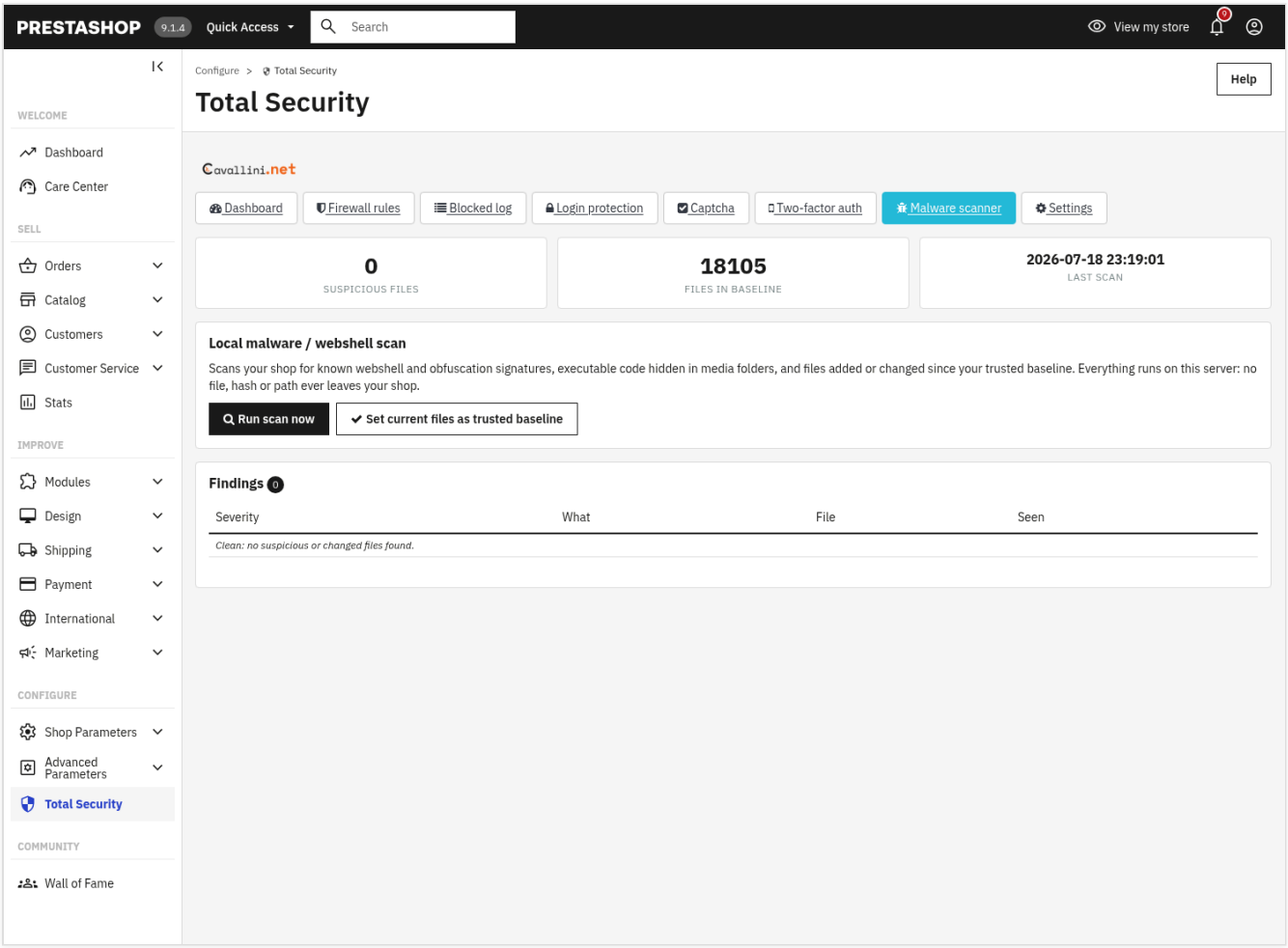


2FA — Registrierung, erzwungene Profile und registrierte Benutzer

Malware-Scanner

Lokaler Malware-/Webshell-Scan: sucht nach bekannten Webshell- und Verschleierungssignaturen, ausführbarem Code, der in Medienordnern versteckt ist, sowie nach Dateien, die seit Ihrer vertrauenswürdigen Baseline hinzugefügt oder geändert wurden. Alles läuft auf dem Server: Keine Datei, kein Hash und kein Pfad verlässt jemals den Shop.

- **Kennzahlen** — verdächtige Dateien, Dateien in der Baseline, letzter Scan.
- **Scan jetzt ausführen** und **Aktuelle Dateien als vertrauenswürdige Baseline festlegen**.
- Die Funde werden mit **Schweregrad**, **Was**, **Datei** und **Wann** aufgelistet.

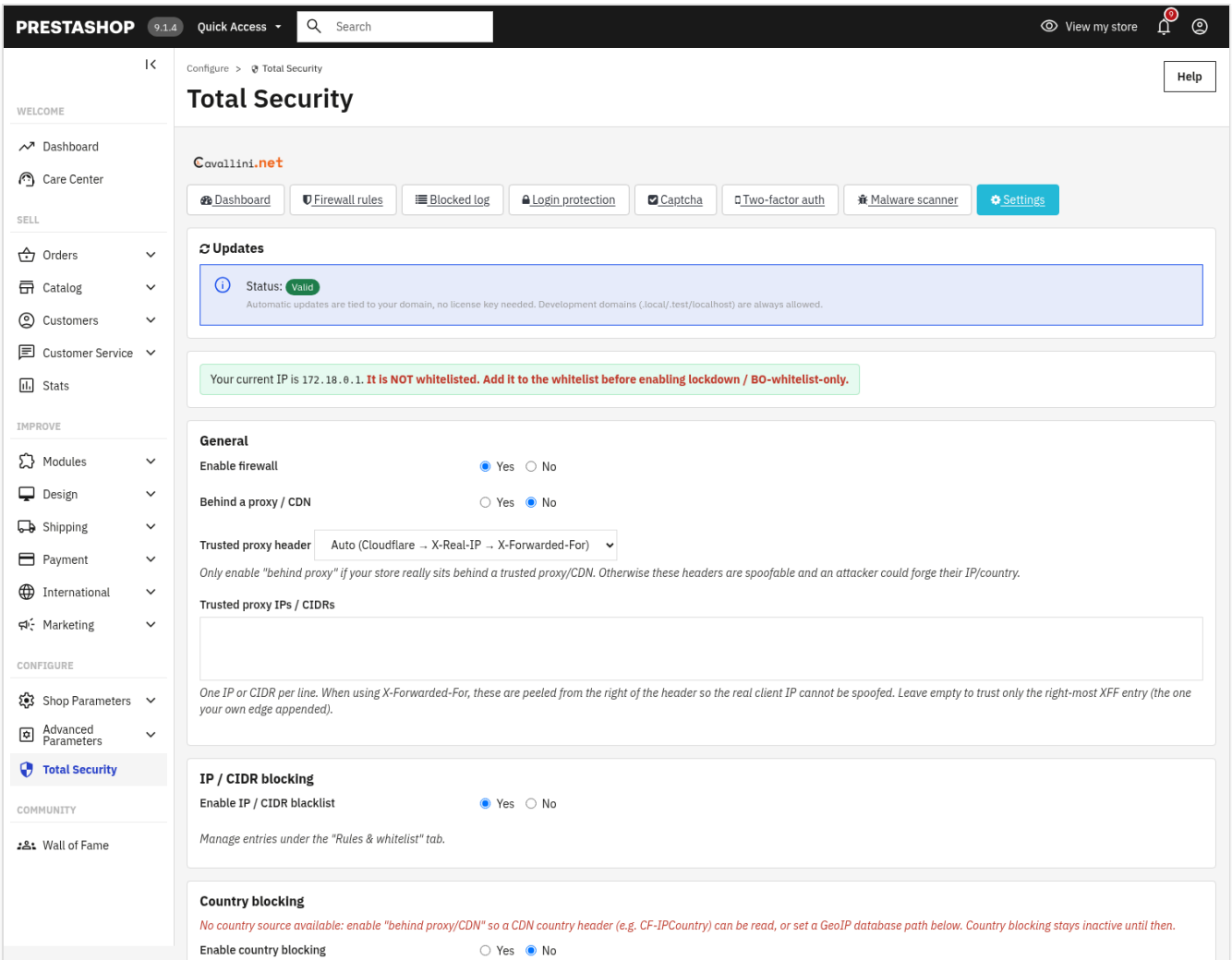


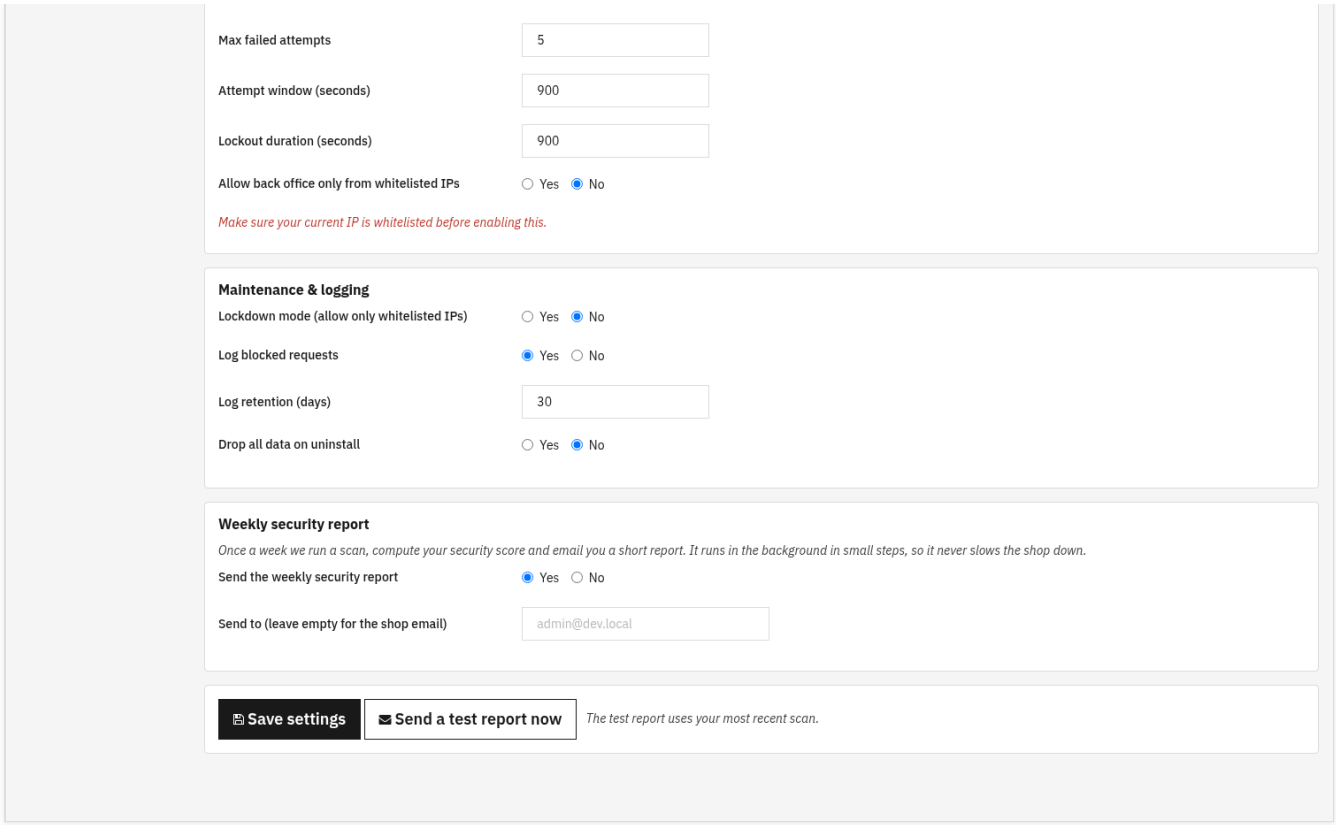
Malware-Scanner — Kennzahlen, Scan und Funde

Einstellungen Firewall-Konfiguration

Die eigentliche Konfiguration der Firewall, nach Abschnitten gruppiert.

- **Allgemein** — Firewall aktivieren; **Hinter einem Proxy/CDN** mit einem vertrauenswürdigen Proxy-Header und vertrauenswürdigen Proxy-IPs/CIDRs — aktivieren Sie dies nur hinter einem tatsächlich vertrauenswürdigen Proxy, sonst lassen sich IP-/Länder-Header fälschen.
- **IP-/CIDR-Blockierung**.
- **Länderblockierung** — Blacklist- oder Whitelist-Modus, ISO-2-Codes, optionaler Pfad zu einer MaxMind-GeoLite2-Datenbank oder ein CDN-Länder-Header — die Datenbank wird aus Lizenzgründen nie mitgeliefert.
- **Bad Bots / User-Agents** — UA-Blocking aktivieren, leere User-Agents blockieren, zusätzliche zu blockierende Teilstrings, die mit einer integrierten Liste zusammengeführt werden.
- **Rate Limiting** — maximale Anfragen pro Zeitfenster, Fenstergröße in Sekunden, Dauer der vorübergehenden Sperre.
- **Angriffsmuster-Blockierung** — SQLi/XSS/LFI/Probing.
- **Anmeldeschutz für das Backoffice** — maximale fehlgeschlagene Versuche, Zeitfenster für Versuche, Dauer der Sperre, Backoffice nur von Whitelist-IPs aus zulassen.
- **Wartung und Protokollierung** — **Lockdown-Modus** (nur Whitelist-IPs zulassen), blockierte Anfragen protokollieren, Aufbewahrungsdauer des Protokolls in Tagen, alle Daten bei der Deinstallation löschen.
- **Wöchentlicher Sicherheitsbericht** — versendet einen kurzen Bericht per E-Mail; läuft in kleinen Schritten im Hintergrund, sodass der Shop nie langsamer wird.

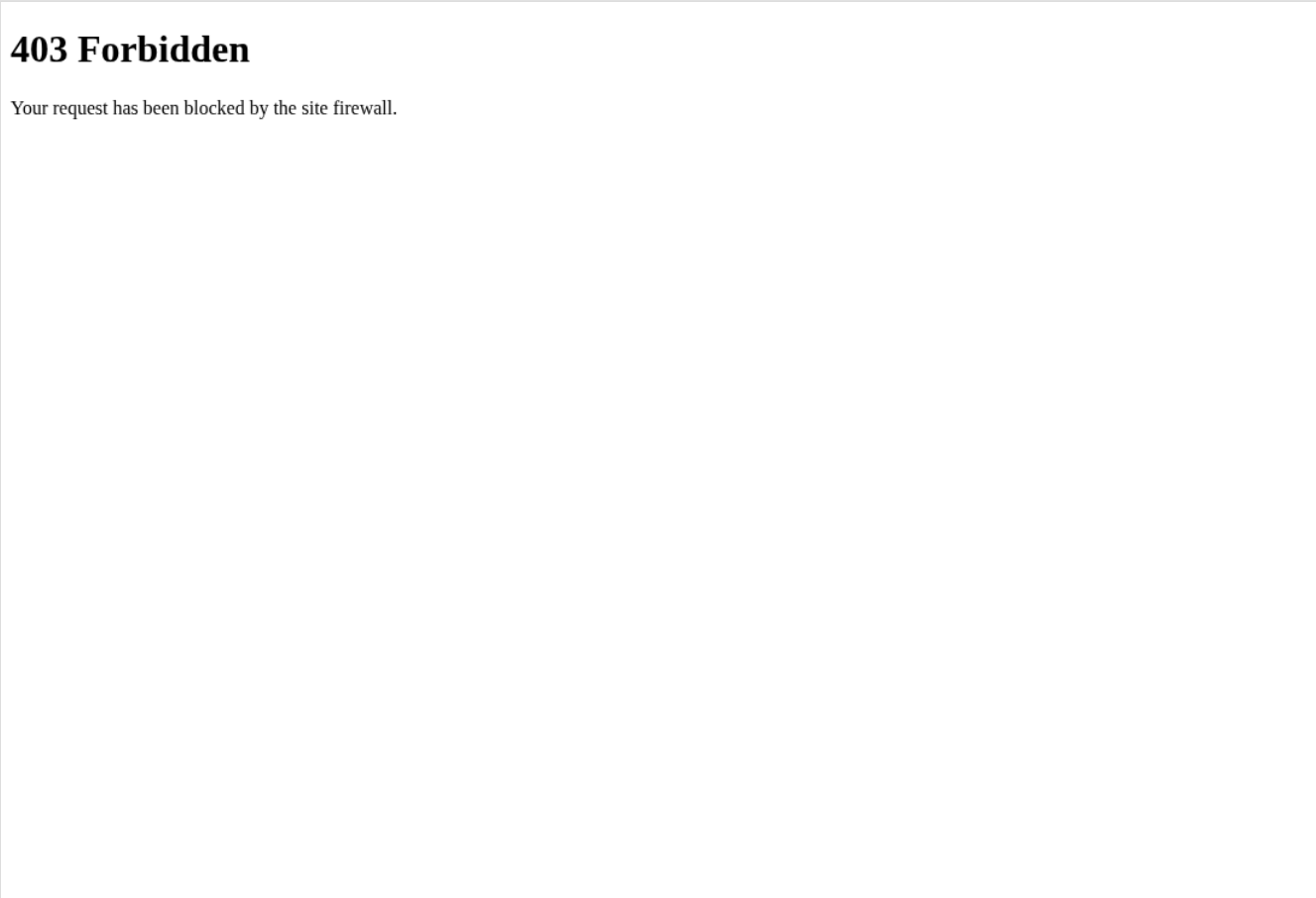

PRESTASHOP
9.1.4
Quick Access
Search
View my store
WELCOME
Dashboard
Care Center
SELL
Orders
Catalog
Customers
Customer Service
Stats
IMPROVE
Modules
Design
Shipping
Payment
International
Marketing
CONFIGURE
Shop Parameters
Advanced Parameters
Total Security
COMMUNITY
Wall of Fame
Configure > Total Security
Total Security
Help
Cavallini.net
Dashboard
Firewall rules
Blocked log
Login protection
Captcha
Two-factor auth
Malware scanner
Settings
Updates
Status: Valid
Automatic updates are tied to your domain, no license key needed. Development domains (.local/.test/localhost) are always allowed.
Your current IP is 172.18.0.1. It is NOT whitelisted. Add it to the whitelist before enabling lockdown / BO-whitelist-only.
General
Enable firewall
Yes
No
Behind a proxy / CDN
Yes
No
Trusted proxy header
Auto (Cloudflare → X-Real-IP → X-Forwarded-For)
Only enable "behind proxy" if your store really sits behind a trusted proxy/CDN. Otherwise these headers are spoofable and an attacker could forge their IP/country.
Trusted proxy IPs / CIDRs
One IP or CIDR per line. When using X-Forwarded-For, these are peeled from the right of the header so the real client IP cannot be spoofed. Leave empty to trust only the right-most XFF entry (the one your own edge appended).
IP / CIDR blocking
Enable IP / CIDR blacklist
Yes
No
Manage entries under the "Rules & whitelist" tab.
Country blocking
No country source available: enable "behind proxy/CDN" so a CDN country header (e.g. CF-IPCountry) can be read, or set a GeoIP database path below. Country blocking stays inactive until then.
Enable country blocking
Yes
No
Mode
Block-list (block listed countries)
Country codes (ISO-2, comma separated)
RU, CN, KP
GeoIP database path (optional MaxMind GeoLite2 .mmdb)
/path/to/GeoLite2-Country.m
We never bundle a GeoIP database (license restrictions). Provide your own .mmdb and the geoip2 library or PECL geoip extension, or rely on the CDN country header.
Bad bots / user-agents
Enable user-agent blocking
Yes
No
Block empty user-agents
Yes
No
Extra blocked user-agent substrings (one per line)
Merged with a sensible built-in list (known scrapers, scanners, empty/suspicious agents).
Rate limiting
Enable rate limiting
Yes
No
Max requests per window
120
Window (seconds)
60
Temporary block duration (seconds)
300
Attack-pattern blocking
Enable attack-pattern blocking (SQLi/XSS/LFI/probing)
Yes
No
Add custom patterns or whitelist legitimate URLs under the "Rules & whitelist" tab.
Back-office login protection
Enable login protection
Yes
No



Einstellungen — Firewall-Konfiguration nach Abschnitt

Im Frontoffice

Wenn die Firewall eine Anfrage blockiert, sieht der Besucher eine einfache 403-Seite „Forbidden — Ihre Anfrage wurde von der Firewall der Website blockiert": Bots und Scanner erreichen Ihren Shop nie.



Im Frontoffice — die 403-Seite, die angezeigt wird, wenn die Firewall eine Anfrage blockiert

3. Prüfen, ob alles funktioniert

- Öffnen Sie das *Dashboard* und lesen Sie Ihren Sicherheits-Score und die Checkliste.
- Senden Sie eine Anfrage mit einem scanner-ähnlichen User-Agent (oder einer Probing-URL) und bestätigen Sie, dass Sie die 403-Blockseite und einen neuen Eintrag im *Blockierungsprotokoll* erhalten.
- Nach mehreren fehlgeschlagenen Backoffice-Anmeldungen wird das Konto/die IP im *Anmeldeschutz* gesperrt.
- Aktivieren Sie das Captcha und bestätigen Sie, dass es im Anmelde-/Registrierungsformular erscheint.
- Richten Sie die 2FA für Ihr Konto ein und melden Sie sich erneut mit einem 6-stelligen Code an.
- Führen Sie den *Malware-Scanner* aus und lesen Sie die Funde.

4. FAQ

Verlangsamt es den Shop?

Nein: Die Firewall läuft zuerst mit günstigen, indexierten Abfragen; der Scanner und der wöchentliche Bericht laufen im Hintergrund.

Sperrt es mich aus?

Setzen Sie zuerst Ihre aktuelle IP auf die Whitelist (die Seite warnt Sie davor, und `127.0.0.1` / `::1` sind bei der Installation bereits auf der Whitelist); aktivieren Sie den Lockdown-Modus oder die Beschränkung des Backoffice auf Whitelist-IPs erst danach.

Verlassen Daten meinen Server?

Nein: Die Firewall, die Lightweight-Captcha-Option, die 2FA-Secrets und der Malware-Scanner laufen alle lokal auf Ihrem Server.

Ersetzt es separate Firewall-/Captcha-/2FA-Module?

Ja: Es ist die einzige, vereinheitlichte Sicherheits-Suite.

Muss ich mein Theme anpassen?

Nein: Es funktioniert über Standard-Hooks und ist mit jedem Theme kompatibel.
