



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.

Total Security: Firewall, Captcha, 2FA & Malware Scanner

Your security score, the web application firewall, captcha, two-factor authentication and the local malware scanner are all managed on the configuration page.

 [Go to configuration](#)

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 Moduleseite 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.

PRESTASHOP 9.1.4 Quick Access

Configure > Total Security Help

Total Security

Cavallini.net

[Dashboard](#) [Firewall rules](#) [Blocked log](#) [Login protection](#) [Captcha](#) [Two-factor auth](#) [Malware scanner](#) [Settings](#)

67
GRADE C

Security score
6 of 10 checks pass. 4 item(s) need your attention below.
Score is computed live from your shop settings, our firewall / captcha / 2FA layers and the last malware scan. Nothing leaves your server.

Checklist

- **Debug mode off in production**
Debug mode exposes errors and paths. Set `_PS_MODE_DEV_` to false in `config/defines.inc.php`.
- **HTTPS enforced everywhere**
Force SSL on the whole shop so credentials and sessions are never sent in clear. [Fix now](#)
- **Web application firewall active**
- **Captcha on login / registration**
Protect the login and registration forms with a captcha to stop bot sign-ups and credential stuffing. [Fix now](#)
- **Two-factor authentication on the back office**
- **No malware / webshell detected**
- **Back-office folder name is not guessable**
Rename the admin folder to something unpredictable (do it from your hosting/FTP, PrestaShop updates the link).
- **Back-office security token enabled**
- **Cookies use SameSite protection**
- **Core overrides under control**

Firewall-Regeln

Verwalten Sie die Regellisten über ein einziges Formular **Regel hinzufügen: Whitelist IP/CIDR** (vertrauenswürdige Adressen, die alle Prüfungen umgehen), **Blacklist IP/CIDR** (gespernte 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.

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

Help

Total Security

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

Your current IP is 172.18.0.1. It is NOT whitelisted. Add it to the whitelist before enabling lockdown / BO-whitelist-only.

Add a rule

Whitelist IP / CIDR

e.g. 203.0.113.10 or 203.0.113.0/24 or RU or badbot

note (optional)

+ Add

Whitelist (trusted IP / CIDR, bypass everything) 2

Value	Note	Added
::1	Auto-added at install (anti-lockout)	2026-07-08 19:20:48
127.0.0.1	Auto-added at install (anti-lockout)	2026-07-08 19:20:48

Blacklist (blocked IP / CIDR) 0

Value	Note	Added
No rules.		

Country rules (ISO-2) 0

Value	Note	Added
No rules.		

Bad user-agents (substring match) 0

Value	Note	Added
No rules.		

Custom attack patterns (substring match) 0

Value	Note	Added
No rules.		

Pattern whitelist (URI substrings exempt from pattern blocking) 0

Value	Note	Added
No rules.		

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.

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

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

All reasons

IP contains...

Q Filter

Export CSV

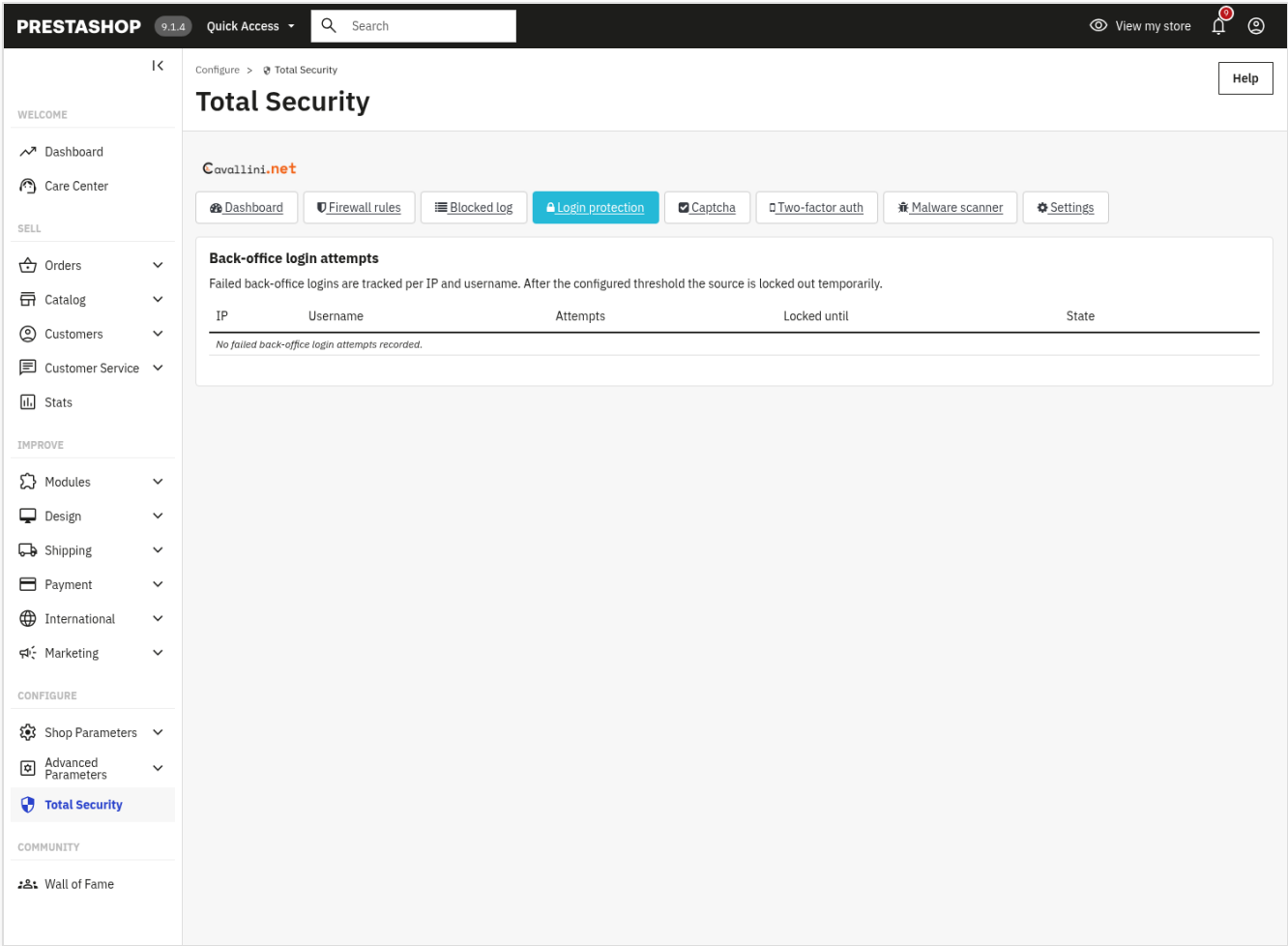
Clear log 27

Date	IP	Country	Reason	Detail	URI	User-Agent	
2026-07-21 21:44:19	172.18.0.1		user_agent	sqlmap	/favicon.ico	sqlmap/1.5.2wstable (http://sqlmap.org)	
2026-07-21 21:44:19	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.5.2wstable (http://sqlmap.org)	
2026-07-21 21:41:08	172.18.0.1		attack_pattern	ifn_passwd	/?x=/etc/passwd	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	
2026-07-21 21:41:07	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.5.2	
2026-07-21 21:22:29	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.0	
2026-07-18 23:42:15	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=7257d964683..Nht1Qxo543LAipa3jNk2QdZUnudD4D7j4k05yCCpvo	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:41:15	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=ccf7.gzXn9F..lrgtWuq9vdAKzJj2e_y9ktT54Q	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:40:34	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=7ba68255093..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:38:09	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=500b134a561..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:36:28	172.18.0.1		attack_pattern	xss_script	/address?id_address=0	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:26:39	172.18.0.1		attack_pattern	xss_handler	/admin-dev/?controller=AdminController&token=b1260b7..7_dvpMRQfjNh_HiDu4FF4.Z7lVHwo2EtMUp	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:26:37	172.18.0.1		attack_pattern	xss_handler	/admin-dev/?controller=AdminController&token=b1260b7..7_dvpMRQfjNh_HiDu4FF4.Z7lVHwo2EtMUp	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:25:47	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=724e95e..Zr5o.wVZ7Q16fGh	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:25:46	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=724e95e..Zr5o.wVZ7Q16fGh	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:24:21	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=5822b68..x0L7QvvpdM.3a1DLv	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:24:21	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=5822b68..x0L7QvvpdM.3a1DLv	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:23:29	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=566e2be783b..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 23:22:28	172.18.0.1		attack_pattern	xss_script	/?x=%3Cscript%3Ealert(1)%3C/script%3E	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36	
2026-07-18 23:21:12	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=15a5721..Y4owHwr7gHJN9G8qihFQhzyOR95yfmk.Ck1OUF435..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC	
2026-07-18 19:16:02	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:59	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:45	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:45	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:36	172.18.0.1		user_agent	curl/	/index.php?fc=modules&module=cli_withdrawal&controlle..	curl/8.14.1	
2026-07-18 19:15:36	172.18.0.1		user_agent	curl/	/	curl/8.14.1	
2026-07-18 19:15:30	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	
2026-07-18 19:15:30	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1	

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.

PRESTASHOP 9.1.4

Quick Access

Search

View my store

Configure > Total Security

Help

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

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

Captcha provider

Enable captcha protection

Provider

Choose your anti-spam provider. Create the keys in the provider dashboard. The Lightweight provider needs no keys and keeps everything on your server.

Site key (public)

Secret key (server-side only)

reCAPTCHA v3 score threshold (0.0 bot, 1.0 human)

Widget theme

Badge position (v3 / invisible / Turnstile)

Lightweight token lifetime (seconds)

Protected forms

Login

Registration

Forgot password

Contact form

Newsletter

Product review

Guest checkout

Advanced

Fail closed (block when the provider is unreachable)

Skip captcha for logged-in customers

Verification timeout (seconds, 1 to 30)

Trusted IP whitelist (one per line, skip captcha)

Verify hostname (reject tokens solved on another domain)

Expected hostname (optional, empty = auto)

Verify action (reCAPTCHA v3 and Turnstile)

Rate limiting

Rate-limit failed captcha attempts

Max failed attempts (1 to 1000)

Window in minutes (1 to 1440)

Save captcha settings

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.

The screenshot shows the PrestaShop 9.1.4 interface with the 'Total Security' configuration page. The left sidebar contains navigation menus for 'WELCOME', 'SELL', 'IMPROVE', 'CONFIGURE', and 'COMMUNITY'. The main content area is titled 'Total Security' and includes a top navigation bar with links like 'Dashboard', 'Firewall rules', 'Blocked log', 'Login protection', 'Captcha', 'Two-factor auth' (highlighted), 'Malware scanner', and 'Settings'. Below this, the 'Your account' section shows a 'Set up 2FA on my account' button. The 'Two-factor authentication' section contains settings for enabling 2FA for staff and customers, forcing 2FA for specific employee profiles (1, 2), and setting a tolerance window (1 step), number of backup codes (8), and issuer name (PrestaShop). At the bottom, there are two tables: 'Enrolled employees' and 'Enrolled customers', both showing columns for ID, Name, Email, Status, and Updated, with a note that no one is currently enrolled.

PRESTASHOP 9.1.4 Quick Access Search

Configure > Total Security

Total Security

Cavallini.net

Dashboard Firewall rules Blocked log Login protection Captcha **Two-factor auth** Malware scanner Settings

Your account

Two-factor authentication for the account you are signed in with. Not set up

[Set up 2FA on my account](#)

You will scan a QR code with an authenticator app (Google Authenticator, Authy, 1Password) and enter a 6-digit code to confirm.

Two-factor authentication

Time-based one-time codes (Google Authenticator, Authy, 1Password and any compatible app). Nothing leaves your server: secrets are encrypted at rest and verified locally.

Enable 2FA for the back office (staff) ☒ Yes ☐ No

This makes 2FA available: an employee can turn it on for their own account, and is then asked for a code at every login. To make it mandatory instead, list the profiles below.

Enable 2FA for customers (front office) ☒ Yes ☐ No

Force 2FA for these employee profiles (comma-separated IDs)

Employees in these profiles cannot use the back office until they enrol. Leave empty to keep 2FA optional. Profiles: 1 = SuperAdmin 2 = Logistician 3 = Translator 4 = Salesman

Tolerance window (steps of 30s, 0 to 5)

Number of backup codes (4 to 20)

Issuer name shown in the app (empty = shop name)

[Save 2FA settings](#)

Enrolled employees 0

ID	Name	Email	Status	Updated
No one has enrolled yet.				

Enrolled customers 0

ID	Name	Email	Status	Updated
No one has enrolled yet.				

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.

The screenshot displays the PrestaShop Total Security dashboard. The interface includes a top navigation bar with the PrestaShop logo, version 9.1.4, and a search bar. A left sidebar contains various menu items categorized into 'WELCOME', 'SELL', 'IMPROVE', 'CONFIGURE', and 'COMMUNITY'. The main content area is titled 'Total Security' and features a 'Cavallini.net' logo. Below the logo are several tabs: 'Dashboard', 'Firewall rules', 'Blocked log', 'Login protection', 'Captcha', 'Two-factor auth', 'Malware scanner' (which is active), and 'Settings'. Three summary cards are shown: '0 SUSPICIOUS FILES', '18105 FILES IN BASELINE', and '2026-07-18 23:19:01 LAST SCAN'. A section titled 'Local malware / webshell scan' provides a description of the scan process and includes two buttons: 'Run scan now' and 'Set current files as trusted baseline'. Below this is a 'Findings' table with columns for 'Severity', 'What', 'File', and 'Seen'. The table currently shows a single entry: 'Clean: no suspicious or changed files found.'

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.

Max failed attempts	5
Attempt window (seconds)	900
Lockout duration (seconds)	900
Allow back office only from whitelisted IPs	☐ Yes ☒ No

Make sure your current IP is whitelisted before enabling this.

Maintenance & logging

Lockdown mode (allow only whitelisted IPs)	☐ Yes ☒ No
Log blocked requests	☒ Yes ☐ No
Log retention (days)	30
Drop all data on uninstall	☐ Yes ☒ No

Weekly security report

Once a week we run a scan, compute your security score and email you a short report. It runs in the background in small steps, so it never slows the shop down.

Send the weekly security report	☒ Yes ☐ No
Send to (leave empty for the shop email)	admin@dev.local

Save settings	Send a test report now	<i>The test report uses your most recent scan.</i>
--	---	--

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.

403 Forbidden

Your request has been blocked by the site firewall.

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.