



Total Security Guida d'uso

Modulo PrestaShop · Compatibile con PrestaShop 1.7 → 9

Firewall, captcha, 2FA e scanner malware, in un unico modulo

Total Security riunisce in un solo modulo un firewall applicativo, un captcha per i form del negozio, l'autenticazione a due fattori (2FA) per back office e clienti, uno scanner locale di malware/webshell e un punteggio di sicurezza sempre aggiornato che ti dice cosa migliorare. Tutto gira sul tuo server: nulla esce dal tuo shop. Nessun codice, nessuna modifica al tema.

1. Installazione

1. Nel back office vai su **Moduli → Gestione moduli → Carica un modulo** e seleziona lo ZIP del modulo.
2. A installazione completata, clicca **Configura**. Si apre un breve pannello con un pulsante **Vai alla configurazione** che porta alla pagina completa.

 **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**

Il pannello Configura apre la pagina completa

Gli aggiornamenti sono automatici. Gli aggiornamenti sono inclusi. I domini di sviluppo (`.local` , `.test` , `localhost`) sono sempre ammessi. Quando esce una nuova versione viene segnalata dentro al modulo.

2. Configurazione — le schede

La pagina del modulo è organizzata in schede in alto: **Dashboard**, **Regole firewall**, **Log dei blocchi**, **Protezione login**, **Captcha**, **Autenticazione a due fattori**, **Scanner malware** e **Impostazioni**.

Dashboard punteggio di sicurezza

Un **punteggio di sicurezza** aggiornato in tempo reale con un voto in lettere (A/B/C/D), calcolato dalle impostazioni del tuo shop, dai livelli firewall/captcha/2FA e dall'ultima scansione malware (nulla esce dal tuo server). Sotto trovi una **Checklist** dei controlli di sicurezza (tra quelli visibili: modalità debug spenta in produzione, HTTPS forzato ovunque, firewall applicativo attivo, captcha su login/registrazione, autenticazione a due fattori sul back office, nessun malware/webshell rilevato, nome cartella back office non prevedibile, token di sicurezza del back office abilitato). Le voci che richiedono attenzione mostrano una scorciatoia **Correggi ora** che porta direttamente all'impostazione interessata.

The screenshot displays the PrestaShop 9.1.4 interface, specifically 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 features a 'Covallini.net' logo. Below the logo is a row of tabs: 'Dashboard' (selected), 'Firewall rules', 'Blocked log', 'Login protection', 'Captcha', 'Two-factor auth', 'Malware scanner', and 'Settings'. The 'Dashboard' tab shows a 'Security score' of 67 (GRADE C) with a note that 6 of 10 checks pass and 4 items need attention. Below this is a 'Checklist' of 10 items, each with a status indicator (red, orange, or green dot) and a 'Fix now' button. The items are: 'Debug mode off in production' (red), 'HTTPS enforced everywhere' (orange), 'Web application firewall active' (green), 'Captcha on login / registration' (orange), 'Two-factor authentication on the back office' (green), 'No malware / webshell detected' (green), 'Back-office folder name is not guessable' (orange), 'Back-office security token enabled' (green), 'Cookies use SameSite protection' (green), and 'Core overrides under control' (green).

Item	Status	Action
Debug mode off in production	Red	Fix now
HTTPS enforced everywhere	Orange	Fix now
Web application firewall active	Green	
Captcha on login / registration	Orange	Fix now
Two-factor authentication on the back office	Green	
No malware / webshell detected	Green	
Back-office folder name is not guessable	Orange	
Back-office security token enabled	Green	
Cookies use SameSite protection	Green	
Core overrides under control	Green	

Dashboard — punteggio di sicurezza e checklist

Regole firewall

Aggiungi e gestisci le liste di regole con un unico form **Aggiungi una regola: Whitelist IP/CIDR** (indirizzi fidati, bypassano tutti i controlli), **Blacklist IP/CIDR** (indirizzi bloccati), **Regole per paese** (codici ISO-2), **User-agent sospetti** (corrispondenza per sottostringa), **Pattern di attacco personalizzati** (corrispondenza per sottostringa) e una **Whitelist di pattern** (sottostringhe di URI esentate dal blocco per pattern). Un banner mostra il tuo IP attuale e ti avvisa di metterlo in whitelist prima di attivare la modalità lockdown o il back office riservato agli IP in whitelist, così non resti mai chiuso fuori.

PRESTASHOP 9.1.4Quick AccessSearch

View my store

WELCOME

DashboardCare Center

SELL

OrdersCatalogCustomersCustomer ServiceStats

IMPROVE

ModulesDesignShippingPaymentInternationalMarketing

CONFIGURE

Shop ParametersAdvanced ParametersTotal Security

COMMUNITY

Wall of Fame

Configure > Total Security

Total Security

Help

Cavallini.net

DashboardFirewall rulesBlocked logLogin protectionCaptchaTwo-factor authMalware scannerSettings

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.		

Regole firewall — whitelist, blacklist, paesi, user-agent e pattern

Log dei blocchi

Ogni richiesta bloccata viene registrata con data, IP, paese, motivo (es. `user_agent` , `attack_pattern` , `ip` , `rate` , `login`), dettaglio, URI richiesto e user-agent. Puoi filtrare per motivo o IP, **Esporta CSV**, **Svuota log** oppure sbloccare un IP direttamente da qui.

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...

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/1.5.2#stable (http://sqlmap.org)	
2026-07-21 21:44:19	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.5.2#stable (http://sqlmap.org)	
2026-07-21 21:41:08	172.18.0.1		attack_pattern	lf_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_NHtiQxo543LAipa3jNk2qdZUnudD4D7j4k05yCCpvo	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_y9ktTS4Q	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_Y4owHw7gMJN9G8qihFQhzyOR95yfmk.cklOUF435_	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=module&module=cli_withdrawal&controle_	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	

Log dei blocchi — filtra, esporta o sblocca un IP

Protezione login

Traccia i tentativi di accesso al back office e blocca account/IP dopo troppi tentativi falliti entro una finestra di tempo; puoi sbloccare manualmente una voce. Le soglie si configurano in Impostazioni (sezione "Protezione login back office").

PRESTASHOP 9.1.4Quick AccessSearch

View my store

WELCOME

DashboardCare Center

SELLOrdersCatalogCustomersCustomer ServiceStats

IMPROVEModulesDesignShippingPaymentInternationalMarketing

CONFIGUREShop ParametersAdvanced ParametersTotal Security

COMMUNITYWall of Fame

Configure > Total Security

Total Security

Cavallini.net

DashboardFirewall rulesBlocked logLogin protectionCaptchaTwo-factor authMalware scannerSettings

Back-office login attempts

Failed back-office logins are tracked per IP and username. After the configured threshold the source is locked out temporarily.

IP	Username	Attempts	Locked until	State
No failed back-office login attempts recorded.				

Protezione login — tentativi falliti e blocchi attivi

Captcha

- **Provider captcha** — scegli tra Google reCAPTCHA v2 (checkbox), reCAPTCHA v3, hCaptcha, Cloudflare Turnstile, oppure il provider **Lightweight** che non richiede alcuna chiave e resta interamente sul tuo server.
- **Site key / Secret key** — dalla dashboard del provider scelto, **soglia punteggio reCAPTCHA v3, tema del widget, posizione del badge, durata del token** per il provider Lightweight.
- **Form protetti** — Login, Registrazione, Password dimenticata, Form di contatto, Newsletter, Recensione prodotto, Checkout ospite (ognuno on/off).
- **Avanzate** — **Fail closed** (blocca quando il provider non è raggiungibile), **Salta il captcha per i clienti già autenticati, Timeout di verifica, Whitelist IP fidati, verifica hostname, verifica action.**
- **Rate limiting** — limita i tentativi di captcha falliti con un massimo e una finestra di tempo.

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 — provider, form protetti e rate limiting

Autenticazione a due fattori (2FA)

Codici monouso basati sul tempo (Google Authenticator, Authy, 1Password e qualsiasi app compatibile). Nulla esce dal tuo server: i segreti sono cifrati a riposo e verificati in locale.

- **Il tuo account** — attiva la 2FA per l'account con cui hai effettuato l'accesso (scansiona un QR code, inserisci un codice a 6 cifre).
- **Abilita la 2FA per il back office** (staff) e/o **per i clienti** (front office).
- **Forza la 2FA per profili impiegato specifici**, per ID (1 = SuperAdmin, 2 = Logistico, 3 = Traduttore, 4 = Addetto vendite); i profili elencati non possono usare il back office finché non si registrano.
- **Finestra di tolleranza, numero di codici di backup, nome emittente** mostrato nell'app.
- **Impiegati registrati e clienti registrati** sono elencati e possono essere azzerati.

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 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.				

2FA — attivazione, profili forzati e utenti registrati

Scanner malware

Scansione locale di malware/webshell: cerca firme note di webshell e codice offuscato, codice eseguibile nascosto nelle cartelle media, e file aggiunti o modificati rispetto alla tua baseline fidata. Tutto gira sul server: nessun file, hash o percorso esce mai dallo shop.

- **Metriche** — file sospetti, file in baseline, ultima scansione.
- **Esegui scansione ora e Imposta i file attuali come baseline fidata.**
- I risultati sono elencati con **gravità, cosa, file e quando**.

The screenshot displays the PrestaShop Total Security dashboard. The top navigation bar includes the PrestaShop logo, version 9.1.4, a Quick Access menu, a search bar, and links to 'View my store', a notification bell, and a user profile icon. The left sidebar contains a 'WELCOME' section with a 'Dashboard' link, a 'Care Center' link, and a 'SELL' section with links for Orders, Catalog, Customers, Customer Service, and Stats. Below these are 'IMPROVE' and 'CONFIGURE' sections with various settings links. The main content area is titled 'Total Security' and features a 'Cavallini.net' logo. It includes a row of tabs: Dashboard, Firewall rules, Blocked log, Login protection, Captcha, Two-factor auth, Malware scanner (active), and Settings. Three summary cards show '0 SUSPICIOUS FILES', '18105 FILES IN BASELINE', and the '2026-07-18 23:19:01' LAST SCAN. A 'Local malware / webshell scan' section explains the scan process and provides buttons for 'Run scan now' and 'Set current files as trusted baseline'. A 'Findings' table is shown with columns for Severity, What, File, and Seen, containing a single row stating 'Clean: no suspicious or changed files found.'

PRESTASHOP 9.1.4 Quick Access Search

View my store

Configure > Total Security

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

0
SUSPICIOUS FILES

18105
FILES IN BASELINE

2026-07-18 23:19:01
LAST SCAN

Local malware / webshell scan

Scans your shop for known webshell and obfuscation signatures, executable code hidden in media folders, and files added or changed since your trusted baseline. Everything runs on this server: no file, hash or path ever leaves your shop.

Run scan now Set current files as trusted baseline

Findings

Severity	What	File	Seen
Clean: no suspicious or changed files found.			

Scanner malware — metriche, scansione e risultati

Impostazioni **configurazione firewall**

La configurazione vera e propria del firewall, raggrupata per sezione.

- **Generale** — Abilita firewall; **Dietro un proxy/CDN** con un header del proxy fidato e gli IP/CIDR del proxy fidato — attivalo solo dietro un proxy realmente fidato, altrimenti gli header IP/paese sono falsificabili.
- **Blocco IP/CIDR.**
- **Blocco per paese** — modalità blacklist o whitelist, codici ISO-2, percorso opzionale al database MaxMind GeoLite2 oppure un header CDN con il paese — il database non è mai incluso nel modulo, per motivi di licenza.
- **Bot / user-agent sospetti** — abilita il blocco per user-agent, blocca gli user-agent vuoti, sottostringhe extra da bloccare unite a un elenco integrato.
- **Rate limiting** — richieste massime per finestra, secondi della finestra, durata del blocco temporaneo.
- **Blocco pattern di attacco** — SQLi/XSS/LFI/probing.
- **Protezione login back office** — tentativi falliti massimi, finestra di tentativo, durata del blocco, back office accessibile solo da IP in whitelist.
- **Manutenzione e log** — **Modalità lockdown** (consenti solo IP in whitelist), registra le richieste bloccate, giorni di conservazione del log, elimina tutti i dati alla disinstallazione.
- **Report settimanale di sicurezza** — invia via email un breve report; gira in background a piccoli passi così non rallenta mai il negozio.

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

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.n

We never bundle a GeoIP database (license restrictions). Provide your own .mmdb and the geoup2 library or PECL geoup 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

Max failed attempts

Attempt window (seconds)

Lockout duration (seconds)

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)

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)

The test report uses your most recent scan.

Nel front office

Quando il firewall blocca una richiesta, il visitatore riceve una semplice pagina 403 "Forbidden — la tua richiesta è stata bloccata dal firewall del sito": bot e scanner non raggiungono mai il tuo shop.

403 Forbidden

Your request has been blocked by the site firewall.

Nel front office — la pagina 403 mostrata quando il firewall blocca una richiesta

3. Verifica che funzioni

- Apri la *Dashboard* e leggi il tuo punteggio di sicurezza e la checklist.
- Invia una richiesta con uno user-agent simile a quello di uno scanner (o un URL di probing) e verifica di ricevere la pagina di blocco 403 e una nuova riga nel *Log dei blocchi*.
- Dopo diversi accessi falliti al back office, l'account/IP risulta bloccato in *Protezione login*.
- Attiva il captcha e verifica che compaia sul form di login/registrazione.
- Attiva la 2FA sul tuo account ed effettua di nuovo l'accesso con un codice a 6 cifre.
- Esegui lo *Scanner malware* e leggi i risultati.

4. Domande frequenti

Rallenta il negozio?

No: il firewall gira per primo con controlli leggeri su indici; lo scanner e il report settimanale girano in background.

Rischio di restare chiuso fuori?

Metti prima in whitelist il tuo IP attuale (la pagina te lo ricorda e `127.0.0.1 / ::1` sono in whitelist fin dall'installazione); attiva la modalità lockdown o il back office riservato agli IP in whitelist solo dopo.

Qualche dato esce dal mio server?

No: il firewall, il provider captcha Lightweight, i segreti 2FA e lo scanner malware girano tutti in locale sul tuo server.

Sostituisce moduli separati di firewall / captcha / 2FA?

Sì: è l'unica suite di sicurezza integrata.

Devo modificare il tema?

No: funziona tramite hook standard ed è compatibile con qualsiasi tema.