Total Security Guida d'uso

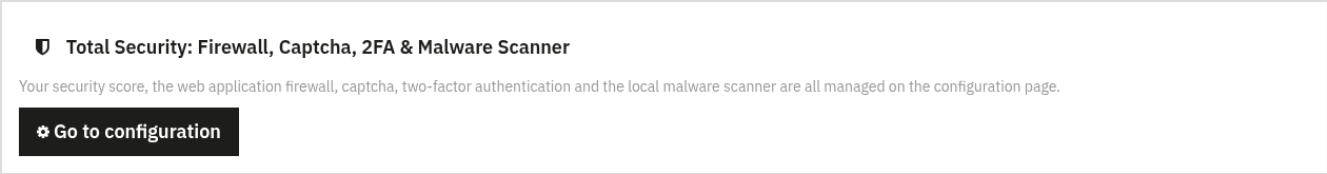
Modulo PrestaShop · Compatibile con PrestaShop 1.7 → 9

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.



Il pannello Configura apre la pagina completa

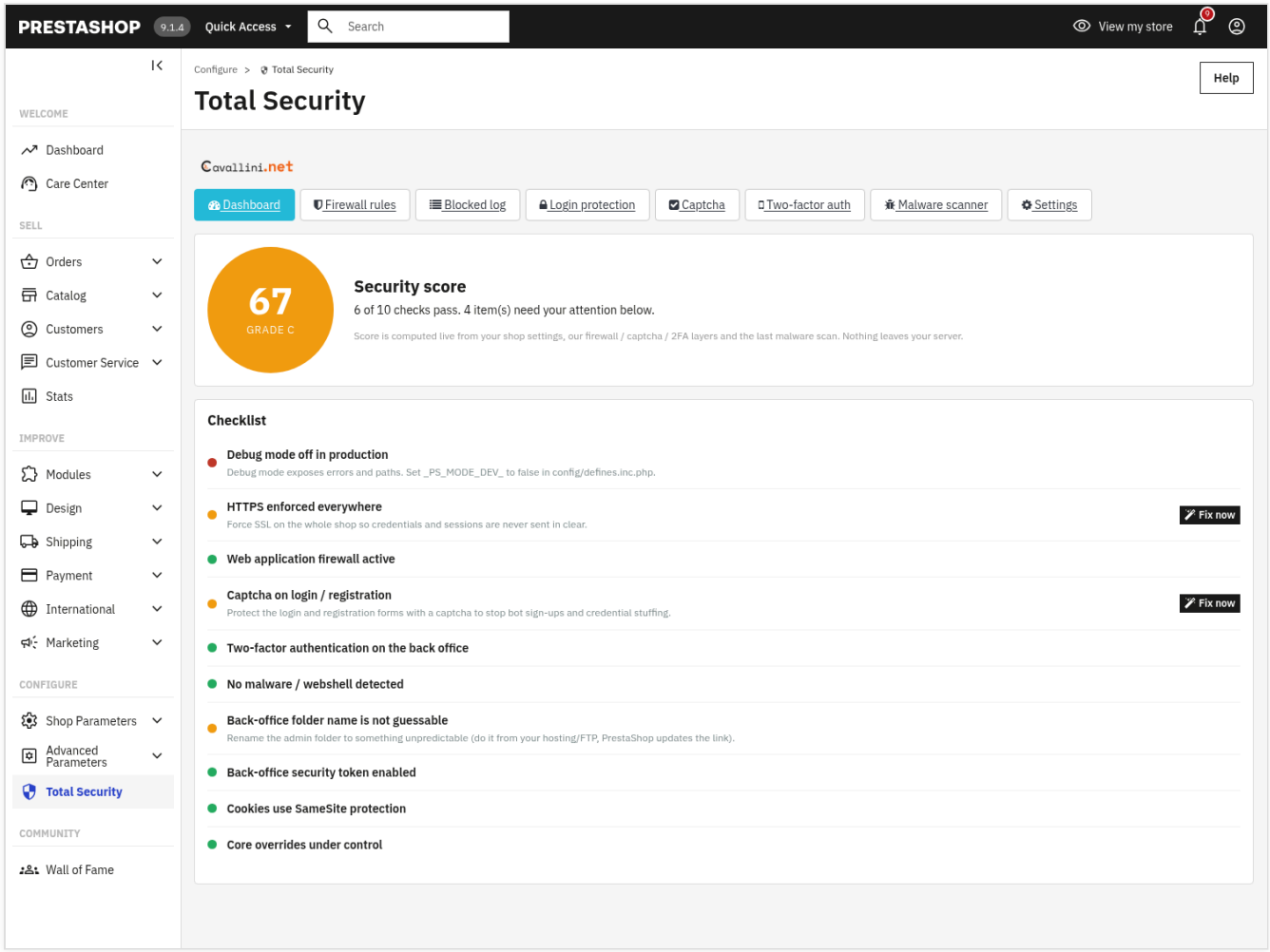
> **Gli aggiornamenti sono automatici.** Gli aggiornamenti sono inclusi. I domini di sviluppo (`.local` , `.test` , `localhost`) sono sempre ammessi. Quando esce una nuova versione viene segnalata dentro al modulo.

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

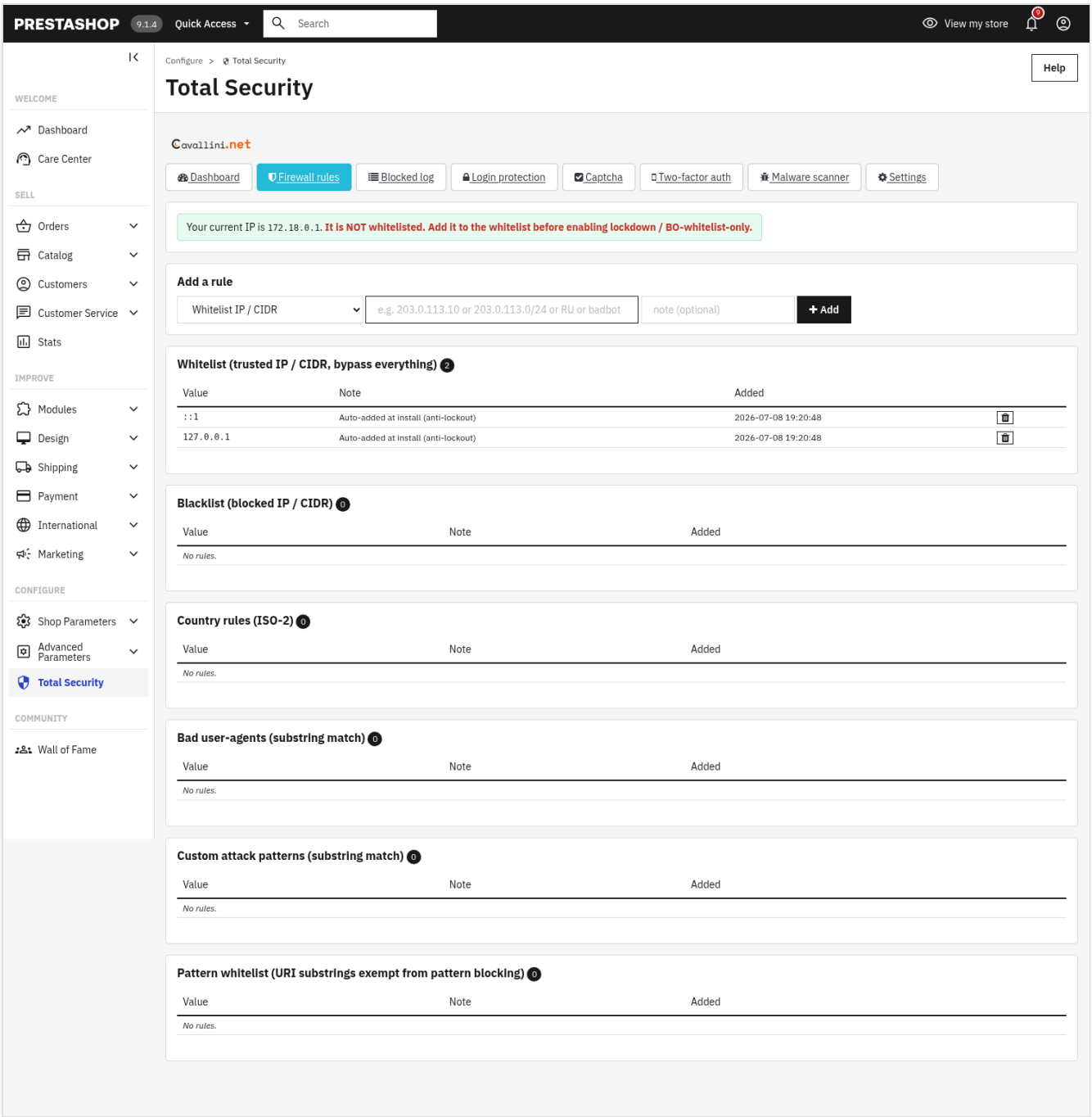
Un **punteggio di sicurezza** aggiornato in tempo reale con un voto in lettere (A/B/C/D), calcolato dalle impostazioni del tuo shop, dai livelli firewall/captcha/2FA e dall'ultima scansione malware (nulla esce dal tuo server). Sotto trovi una **Checklist** dei controlli di sicurezza (tra quelli visibili: 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.



Dashboard — punteggio di sicurezza e checklist

Regole firewall

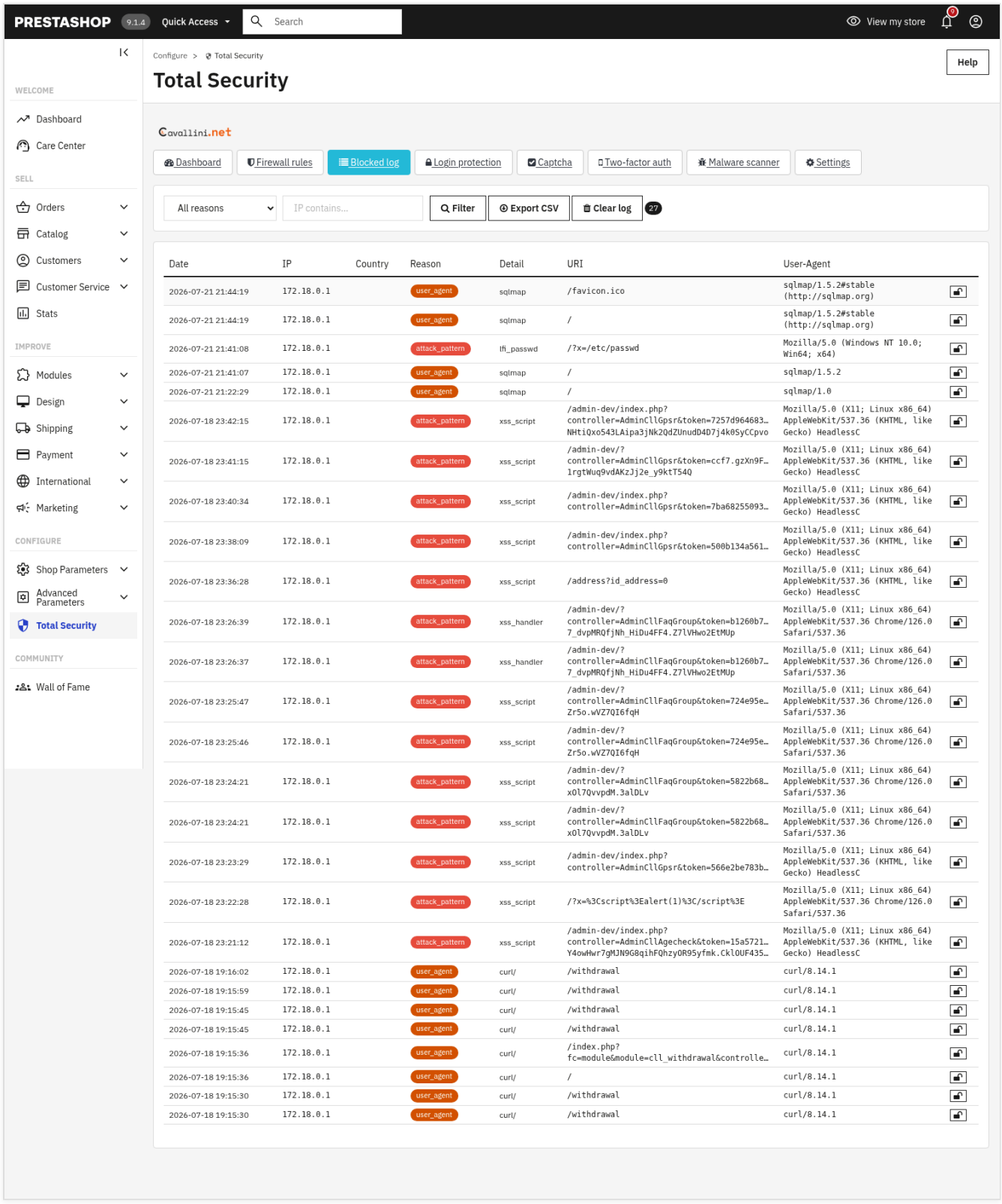
Aggiungi e gestisci le liste di regole con un unico form **Aggiungi una regola**: **Whitelist IP/CIDR** (indirizzi fidati, bypassano tutti i controlli), **Blacklist IP/CIDR** (indirizzi bloccati), **Regole per paese** (codici ISO-2), **User-agent sospetti** (corrispondenza per sottostringa), **Pattern 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.



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

Log dei blocchi

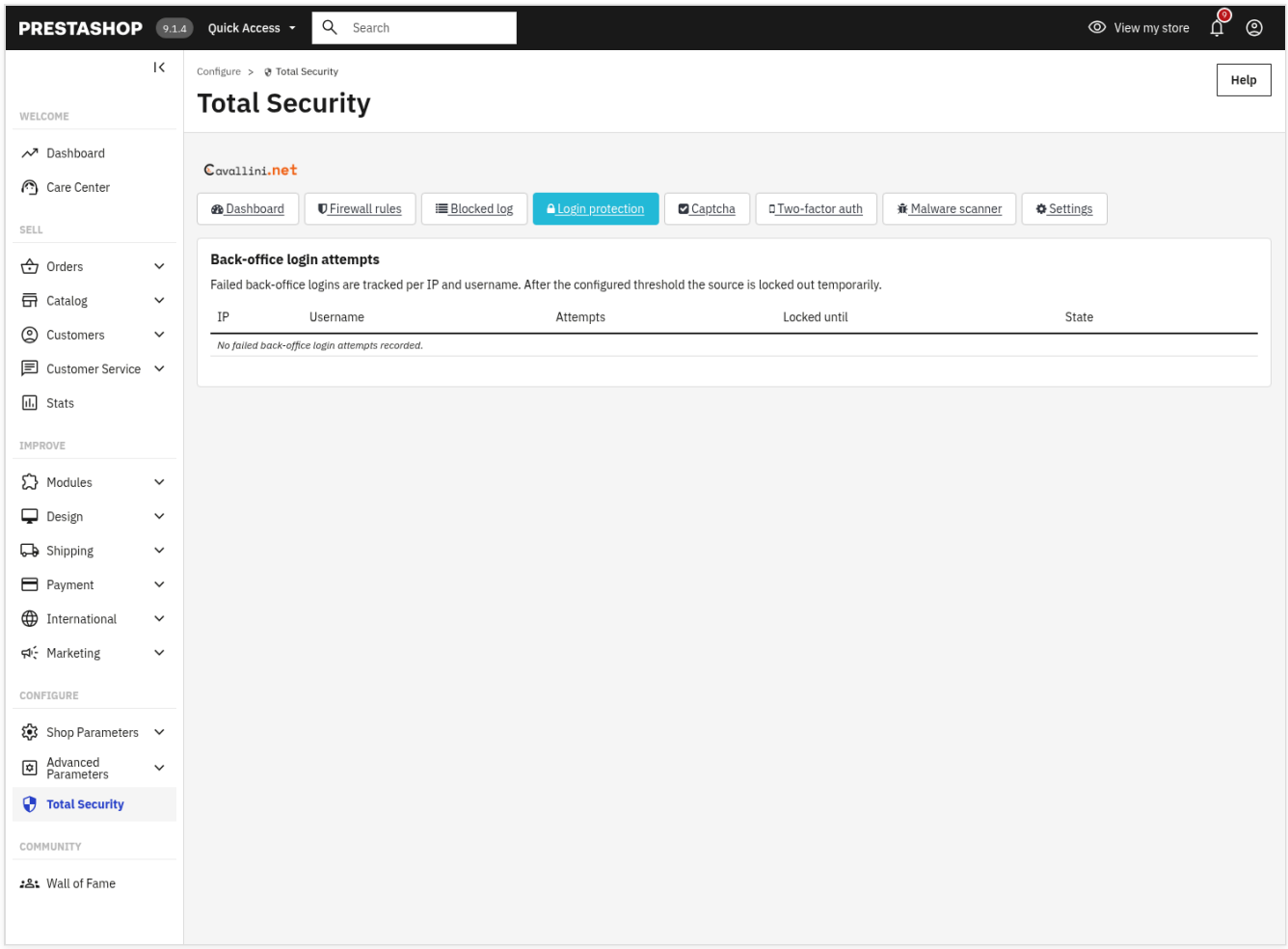
Ogni richiesta bloccata viene registrata con data, IP, paese, motivo (es. `user_agent`, `attack_pattern`, `ip`, `rate`, `login`), dettaglio, URI richiesto e user-agent. Puoi filtrare per motivo o IP, **Esporta CSV**, **Svuota log** oppure sbloccare un IP direttamente da qui.



Log dei blocchi — filtra, esporta o sblocca un IP

Protezione login

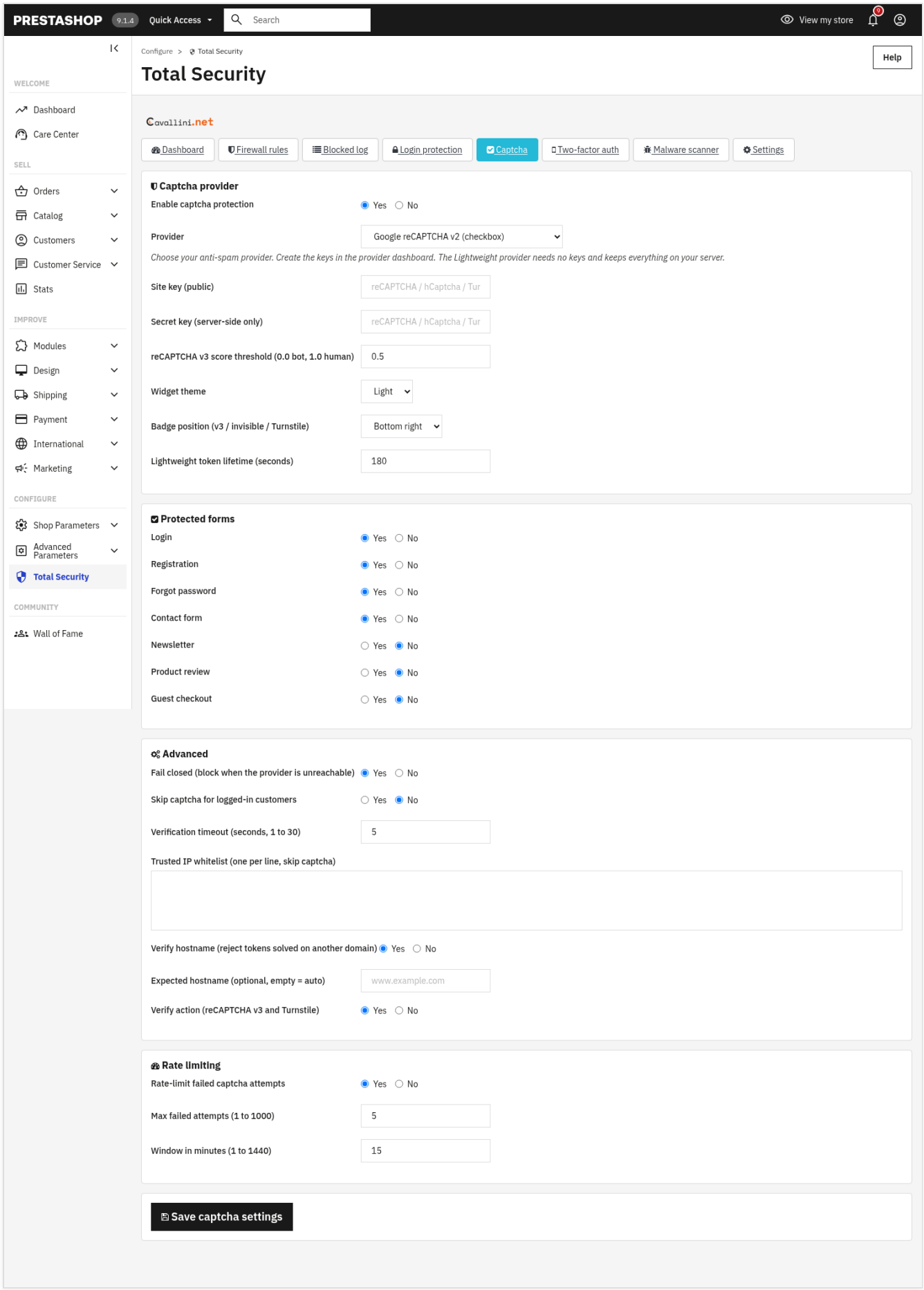
Traccia i tentativi di accesso al back office e blocca account/IP dopo troppi tentativi falliti entro una finestra di tempo; puoi sbloccare manualmente una voce. Le soglie si configurano in Impostazioni (sezione "Protezione login back office").



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.

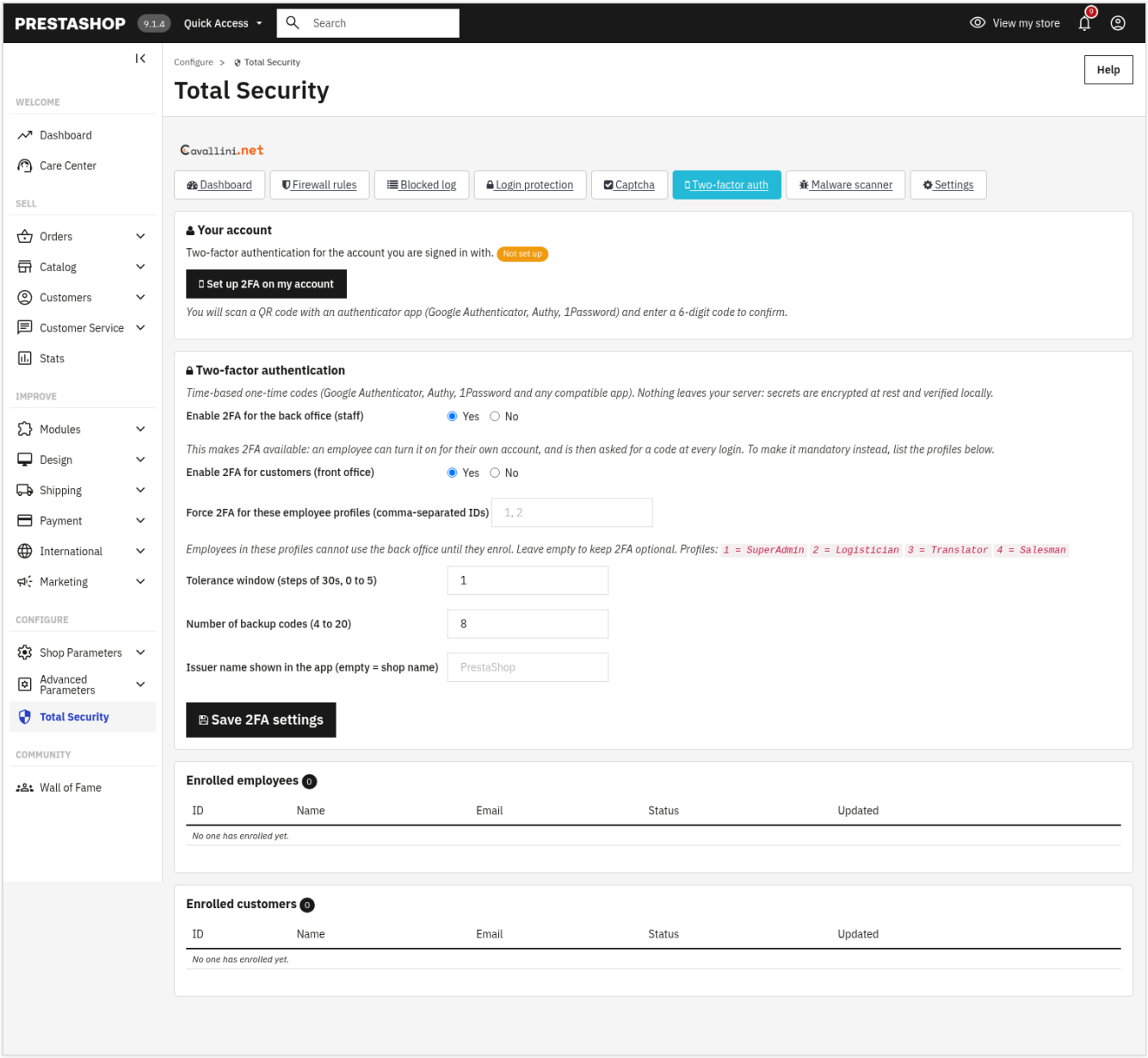


Captcha — provider, form protetti e rate limiting

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.

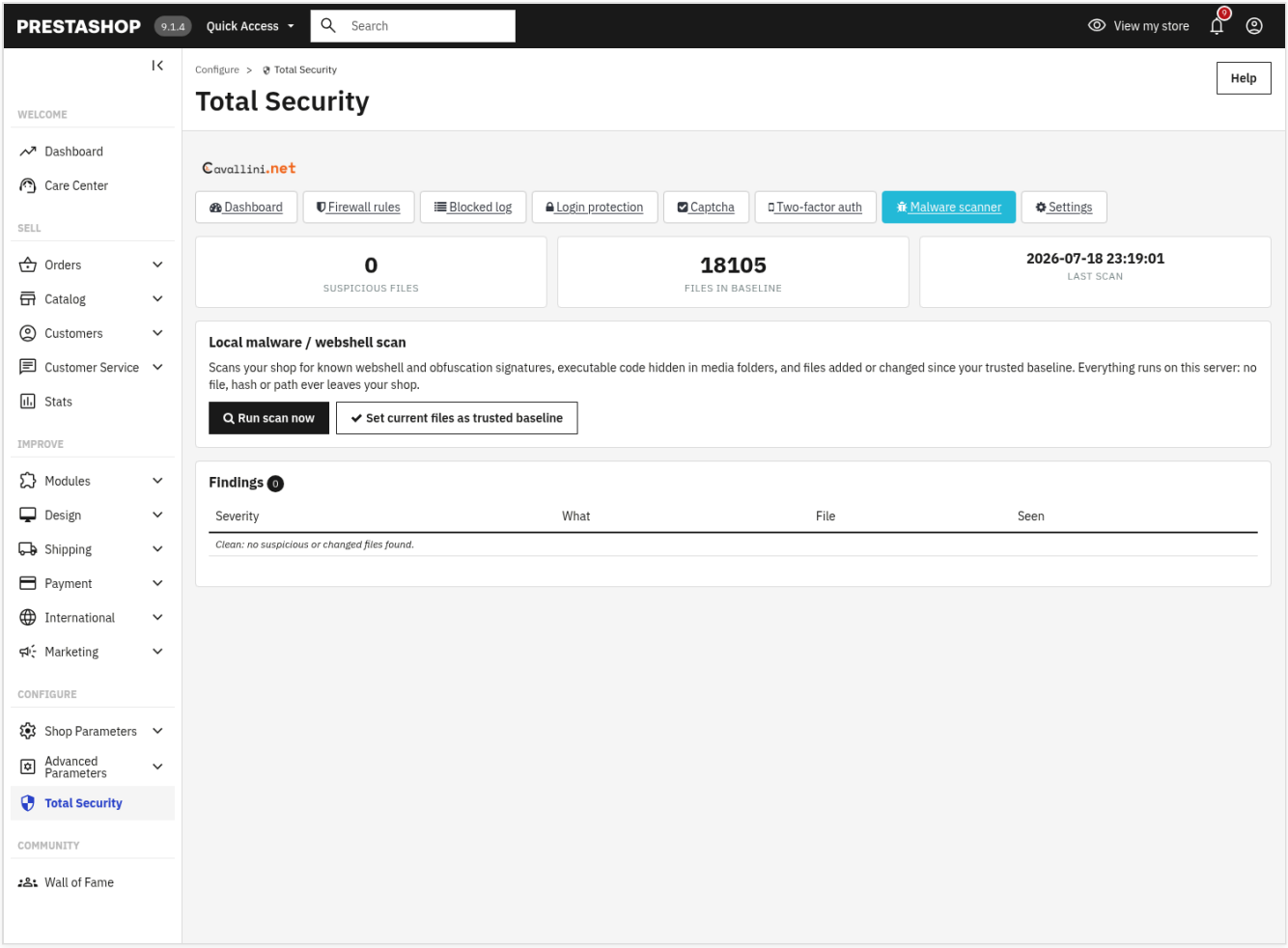


2FA — attivazione, profili forzati e utenti registrati

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**.

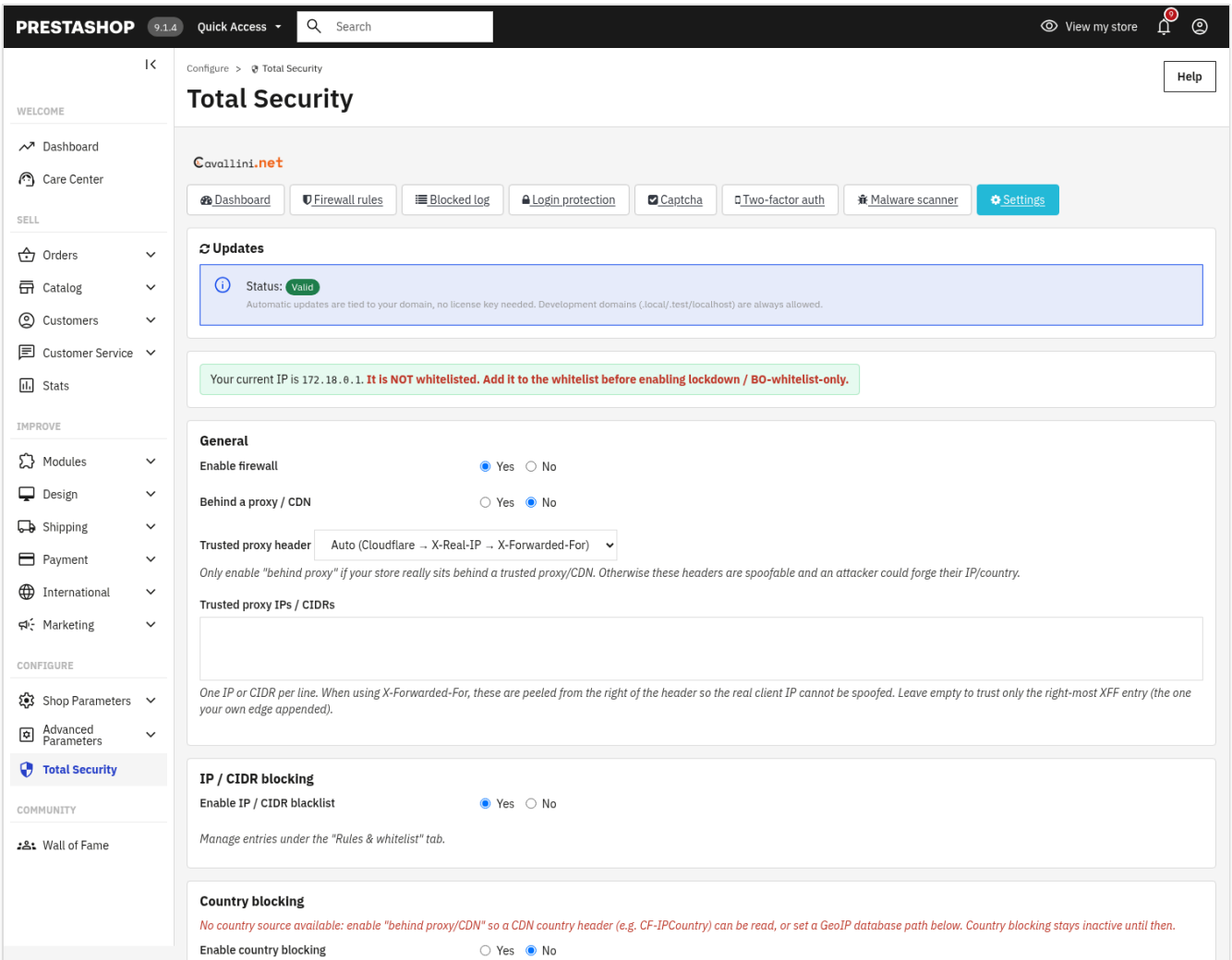


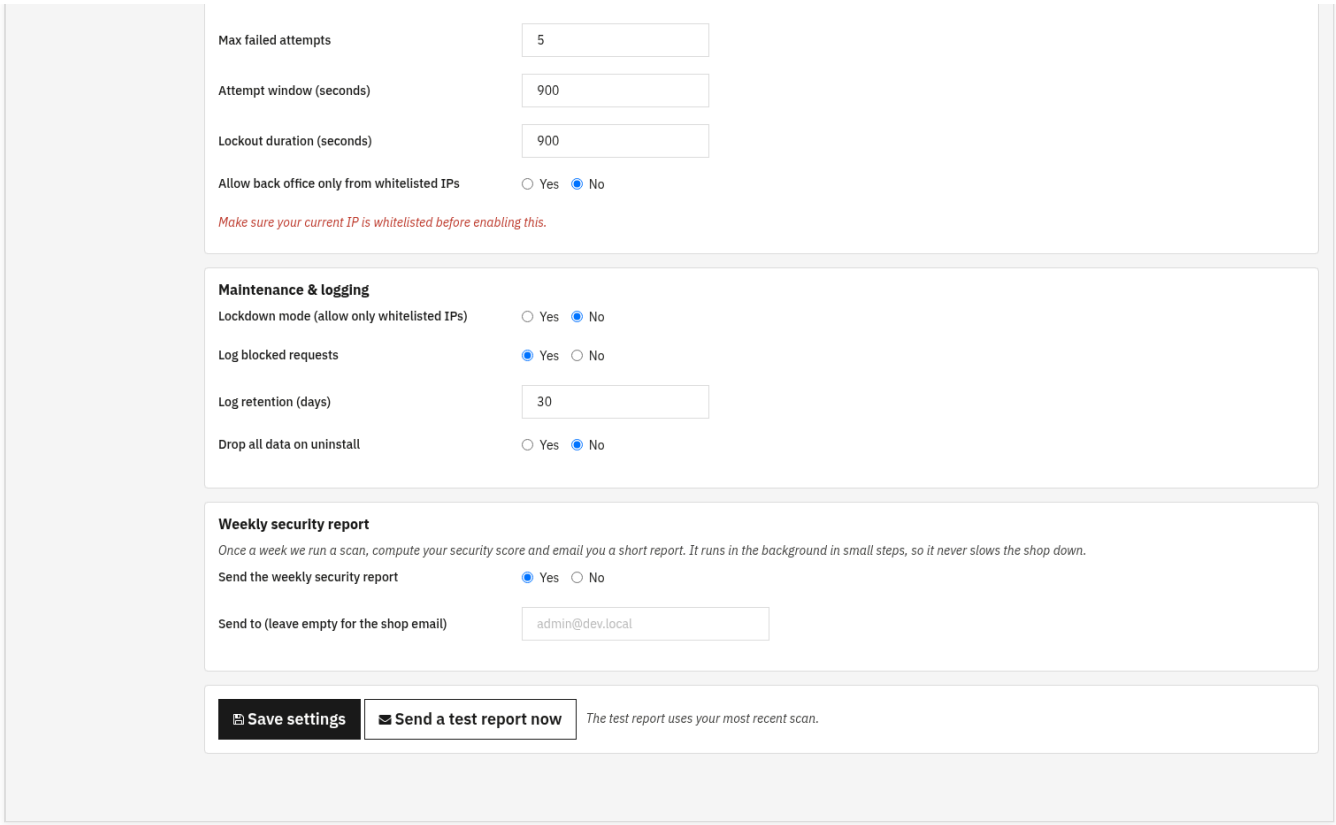
Scanner malware — metriche, scansione e risultati

Impostazioni configurazione firewall

La configurazione vera e propria del firewall, raggruppata 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.

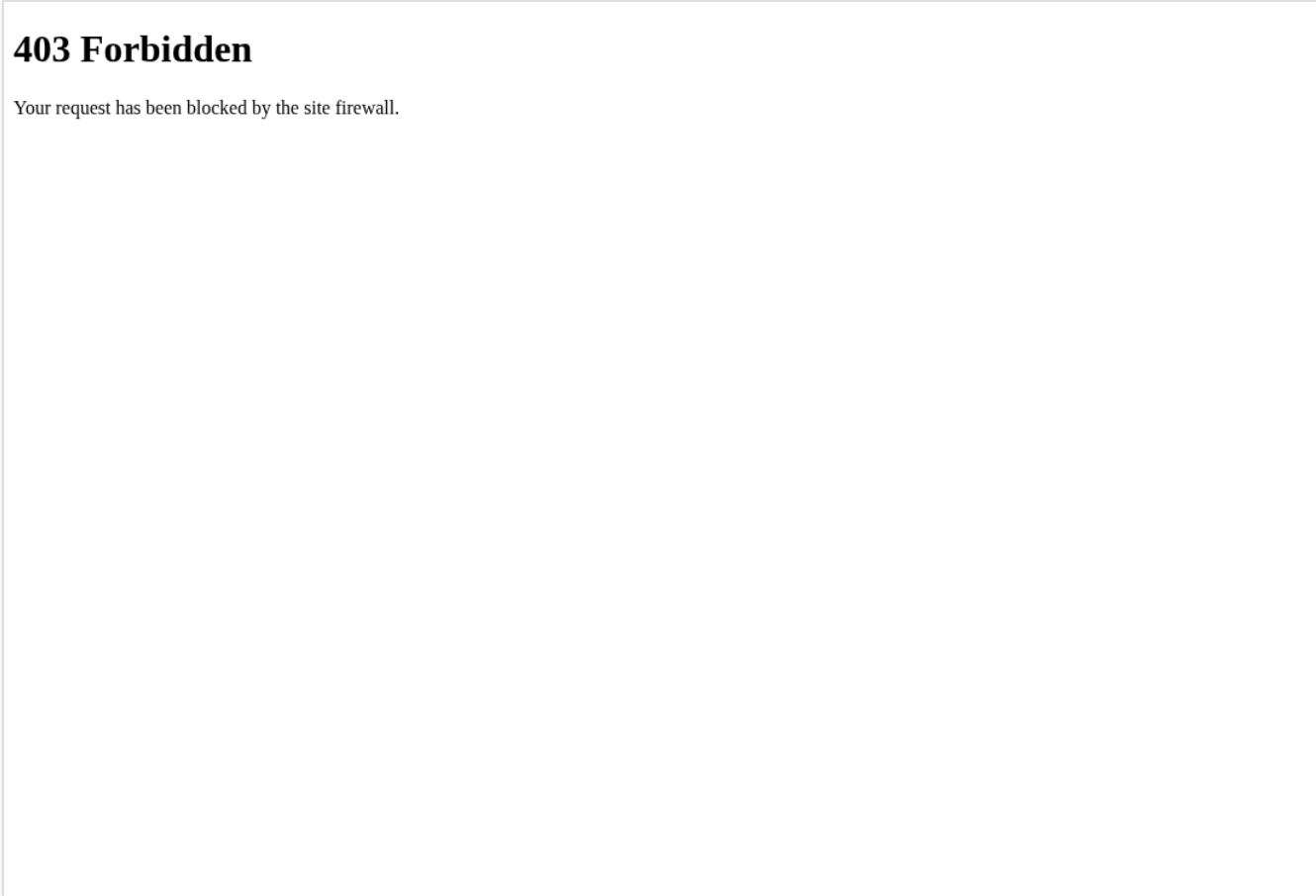

PRESTASHOP
9.1.4
Quick Access
Search
View my store
WELCOME
Dashboard
Care Center
SELL
Orders
Catalog
Customers
Customer Service
Stats
IMPROVE
Modules
Design
Shipping
Payment
International
Marketing
CONFIGURE
Shop Parameters
Advanced Parameters
Total Security
COMMUNITY
Wall of Fame
Configure > Total Security
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



Impostazioni — configurazione del firewall per sezione

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.



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.
