Total Security User Guide

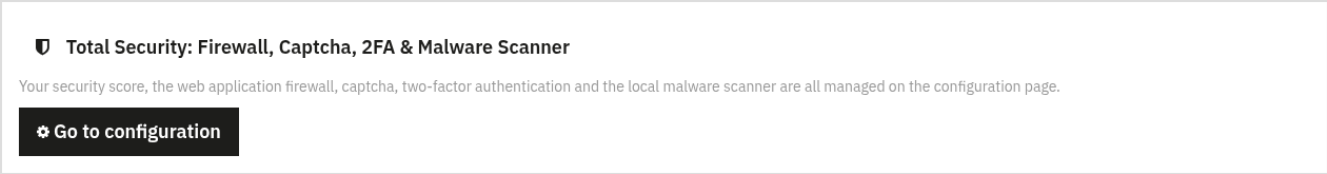
PrestaShop module · Compatible with PrestaShop 1.7 → 9

Firewall, captcha, 2FA and malware scanner, in one module

Total Security bundles into one module a web application firewall, a captcha for the store forms, two-factor authentication (2FA) for the back office and customers, a local malware/webshell scanner, and a live security score that tells you what to improve. Everything runs on your own server: nothing leaves your shop. No coding, no theme edits.

1. Installation

1. In the back office go to **Modules → Module Manager → Upload a module** and select the module ZIP.
2. Once installed, click **Configure**. A short panel opens with a **Go to configuration** button that takes you to the full page.



The Configure panel opens the full configuration page

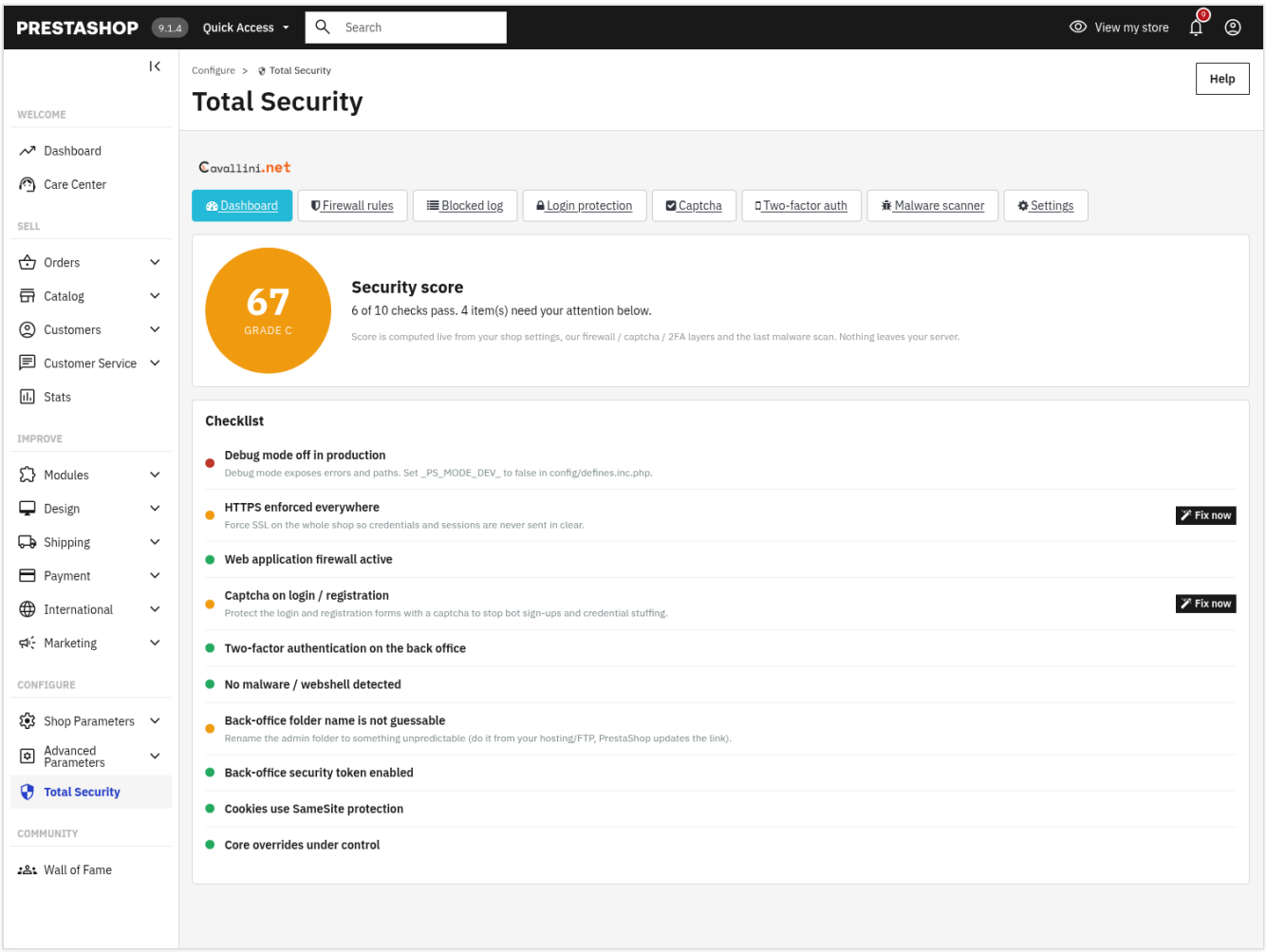
> **Updates are automatic.** Updates are included. Development domains (`.local` , `.test` , `localhost`) are always allowed. When a new version is available it is shown right inside the module.

2. Configuration — the tabs

The module page is organised in tabs across the top: **Dashboard**, **Firewall rules**, **Blocked log**, **Login protection**, **Captcha**, **Two-factor auth**, **Malware scanner** and **Settings**.

Dashboard security score

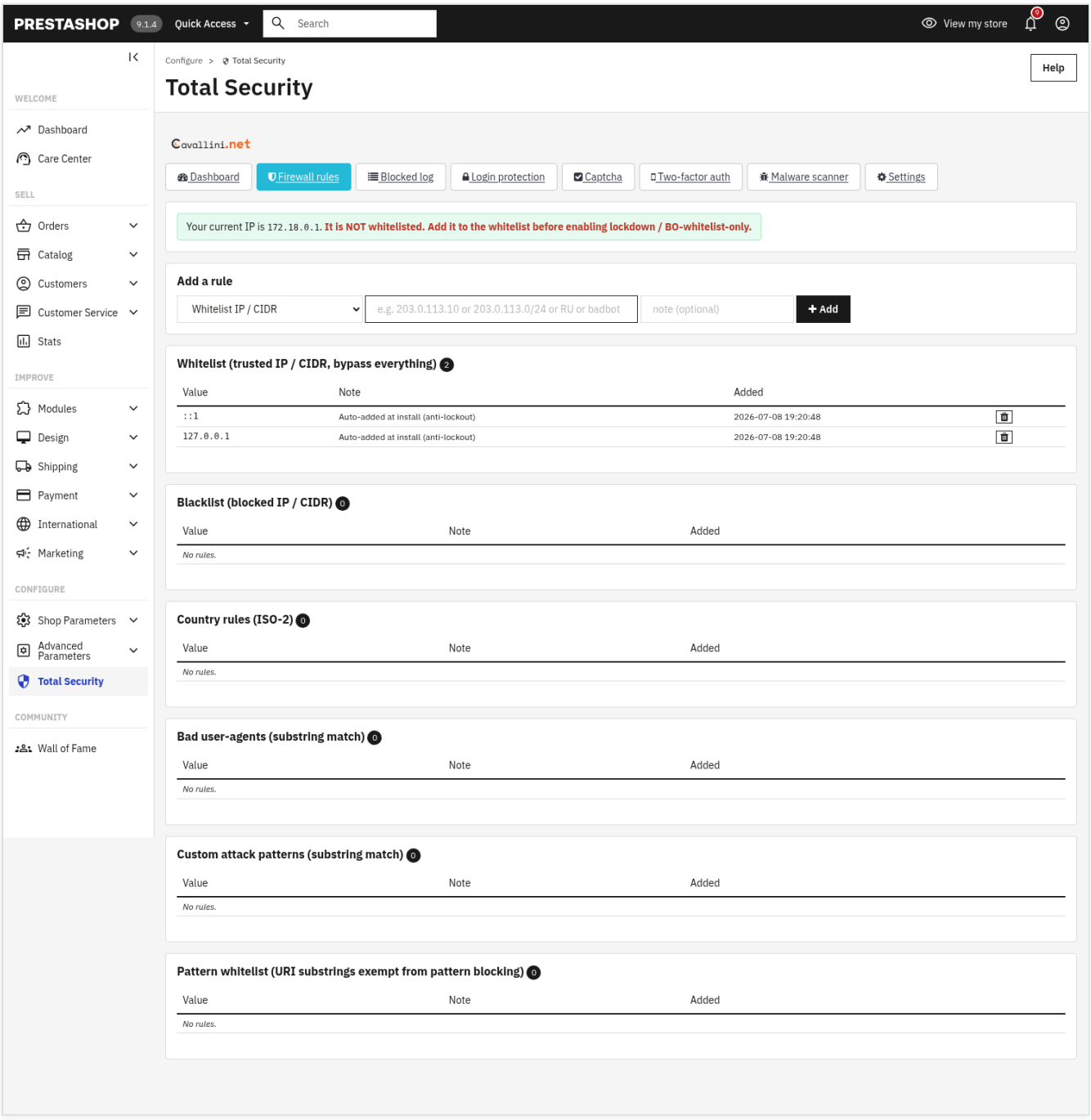
A live **Security score** with a letter grade (A/B/C/D), computed from your shop settings, the firewall/captcha/2FA layers and the last malware scan (nothing leaves your server). Below it a **Checklist** of security checks (examples visible: debug mode off in production, HTTPS enforced everywhere, web application firewall active, captcha on login/registration, two-factor authentication on the back office, no malware/webshell detected, back-office folder name not guessable, back-office security token enabled). Items that need attention show a **Fix now** shortcut that jumps straight to the relevant setting.



Dashboard — security score and checklist

Firewall rules

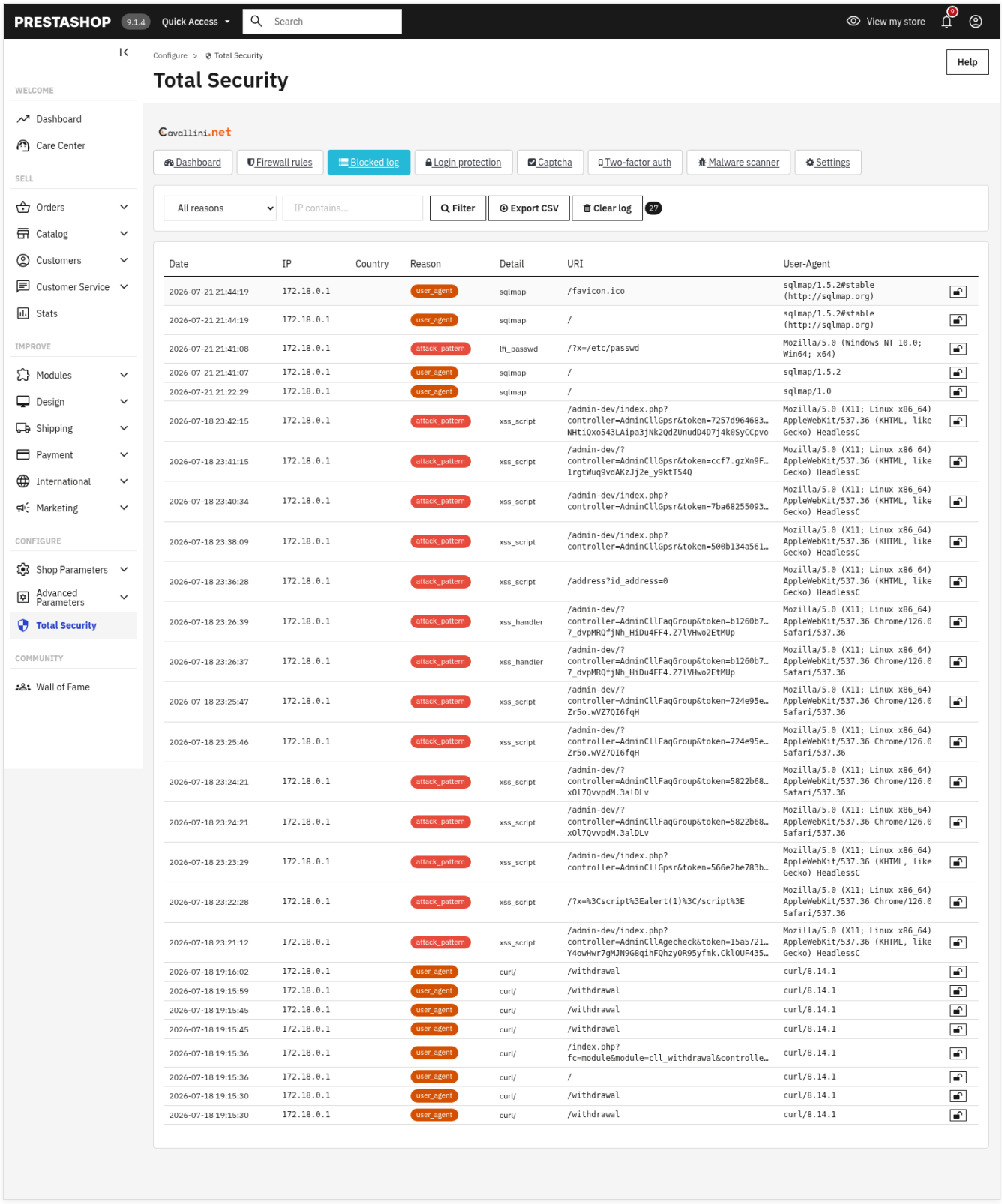
Add and manage the rule lists with one **Add a rule** form: **Whitelist IP/CIDR** (trusted, bypasses everything), **Blacklist IP/CIDR** (blocked), **Country rules** (ISO-2 codes), **Bad user-agents** (substring match), **Custom attack patterns** (substring match), and a **Pattern whitelist** (URI substrings exempt from pattern blocking). A banner shows your current IP and warns you to whitelist it before enabling lockdown mode or back-office-whitelist-only, so you never lock yourself out.



Firewall rules — whitelist, blacklist, countries, user-agents and patterns

Blocked log

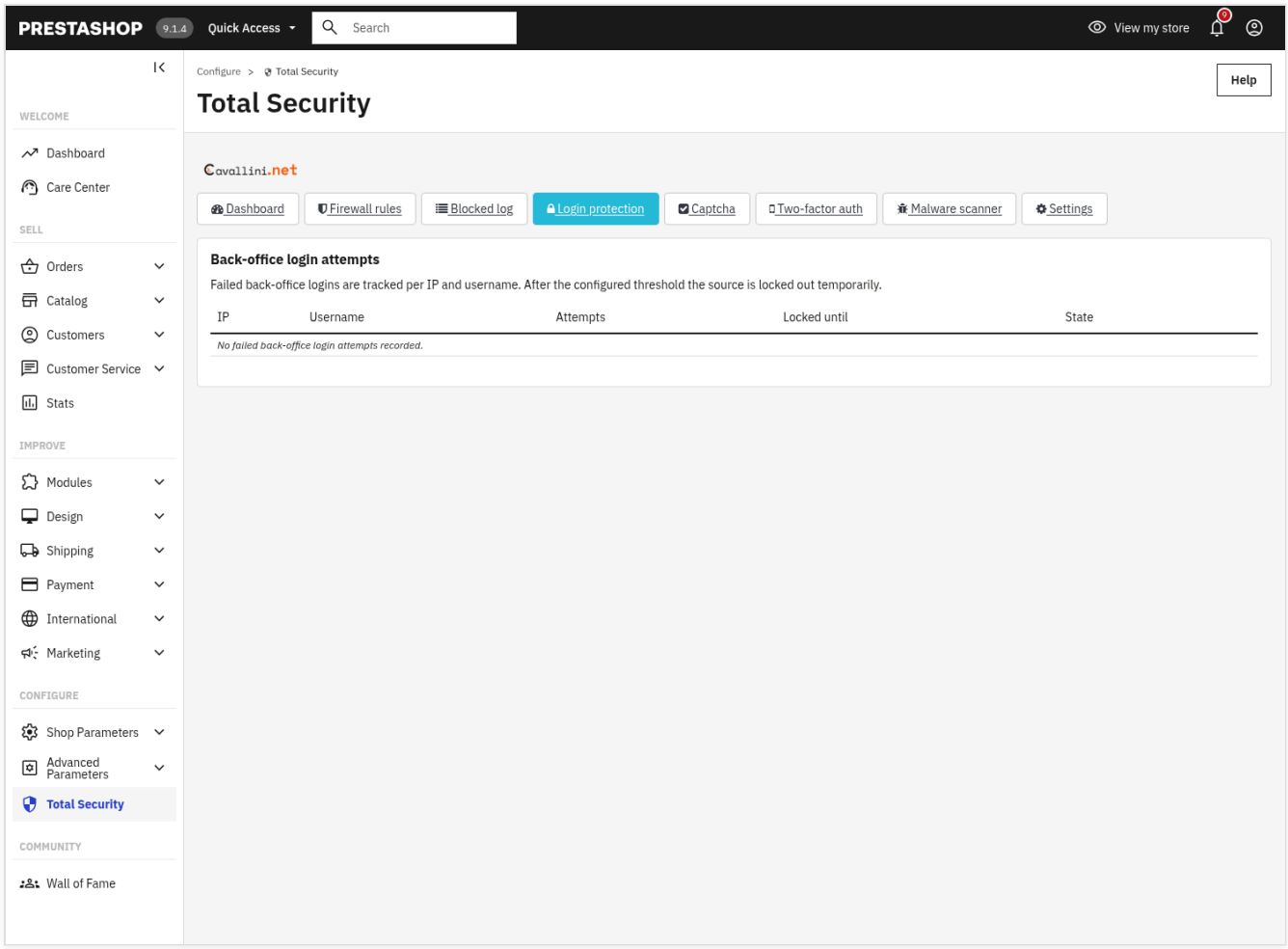
Every blocked request is logged with date, IP, country, reason (e.g. `user_agent`, `attack_pattern`, `ip`, `rate`, `login`), detail, the requested URI and the user-agent. Filter by reason or IP, **Export CSV**, **Clear log**, or unblock an IP right from here.



Blocked log — filter, export or unblock an IP

Login protection

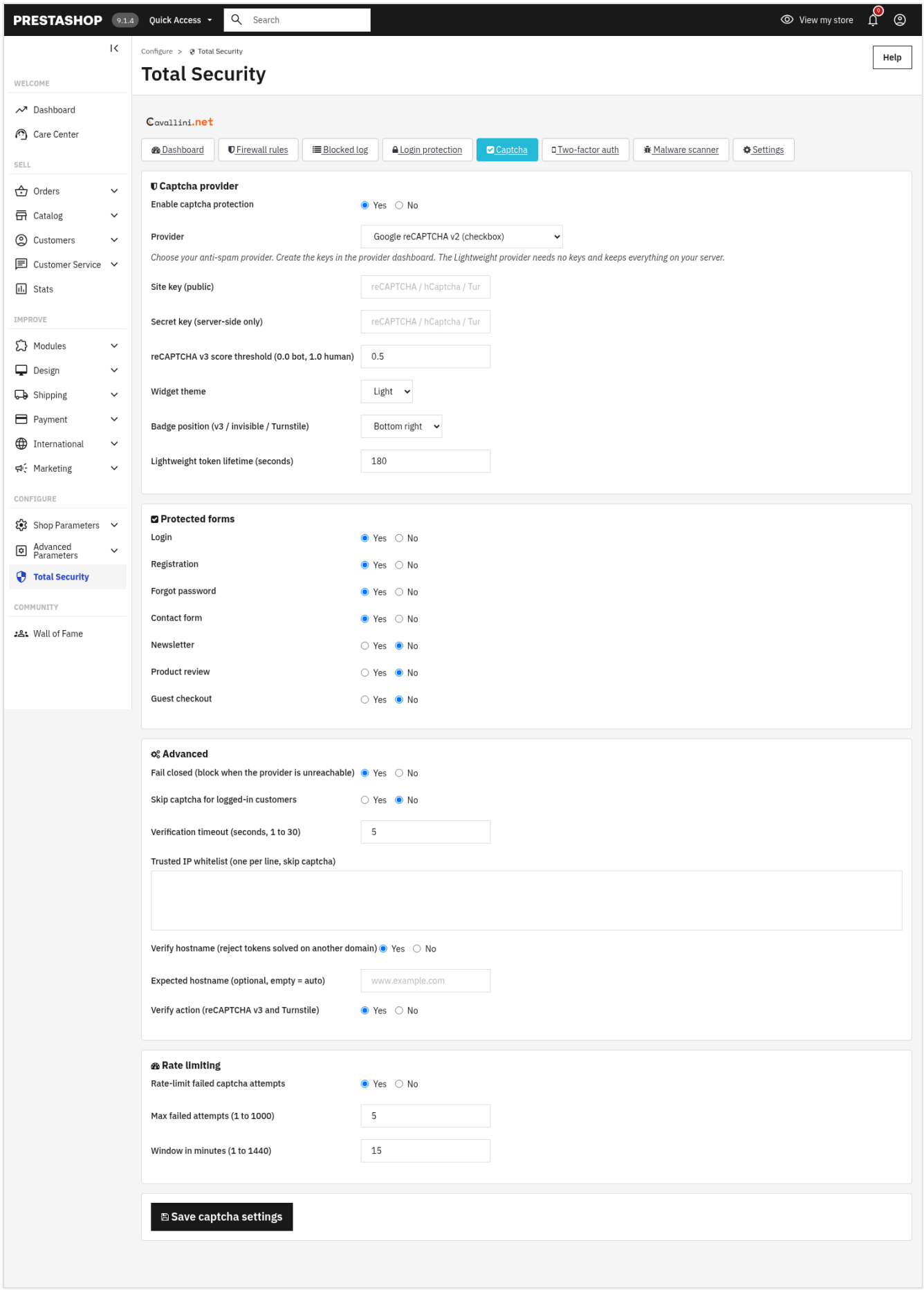
Tracks back-office login attempts and locks an account/IP after too many failed attempts within a time window; you can unlock an entry manually. Configure the thresholds in Settings (Back-office login protection).



Login protection — failed attempts and active locks

Captcha

- **Captcha provider** — choose Google reCAPTCHA v2 (checkbox), reCAPTCHA v3, hCaptcha, Cloudflare Turnstile, or the **Lightweight** provider that needs no keys and keeps everything on your server.
- **Site key** / **Secret key** — from the chosen provider's dashboard, **reCAPTCHA v3 score threshold**, **widget theme**, **badge position**, **lightweight token lifetime**.
- **Protected forms** — Login, Registration, Forgot password, Contact form, Newsletter, Product review, Guest checkout (each on/off).
- **Advanced** — **Fail closed** (block when the provider is unreachable), **Skip captcha for logged-in customers**, **Verification timeout**, **Trusted IP whitelist**, **verify hostname**, **verify action**.
- **Rate limiting** — rate-limit failed captcha attempts with a max and a window.

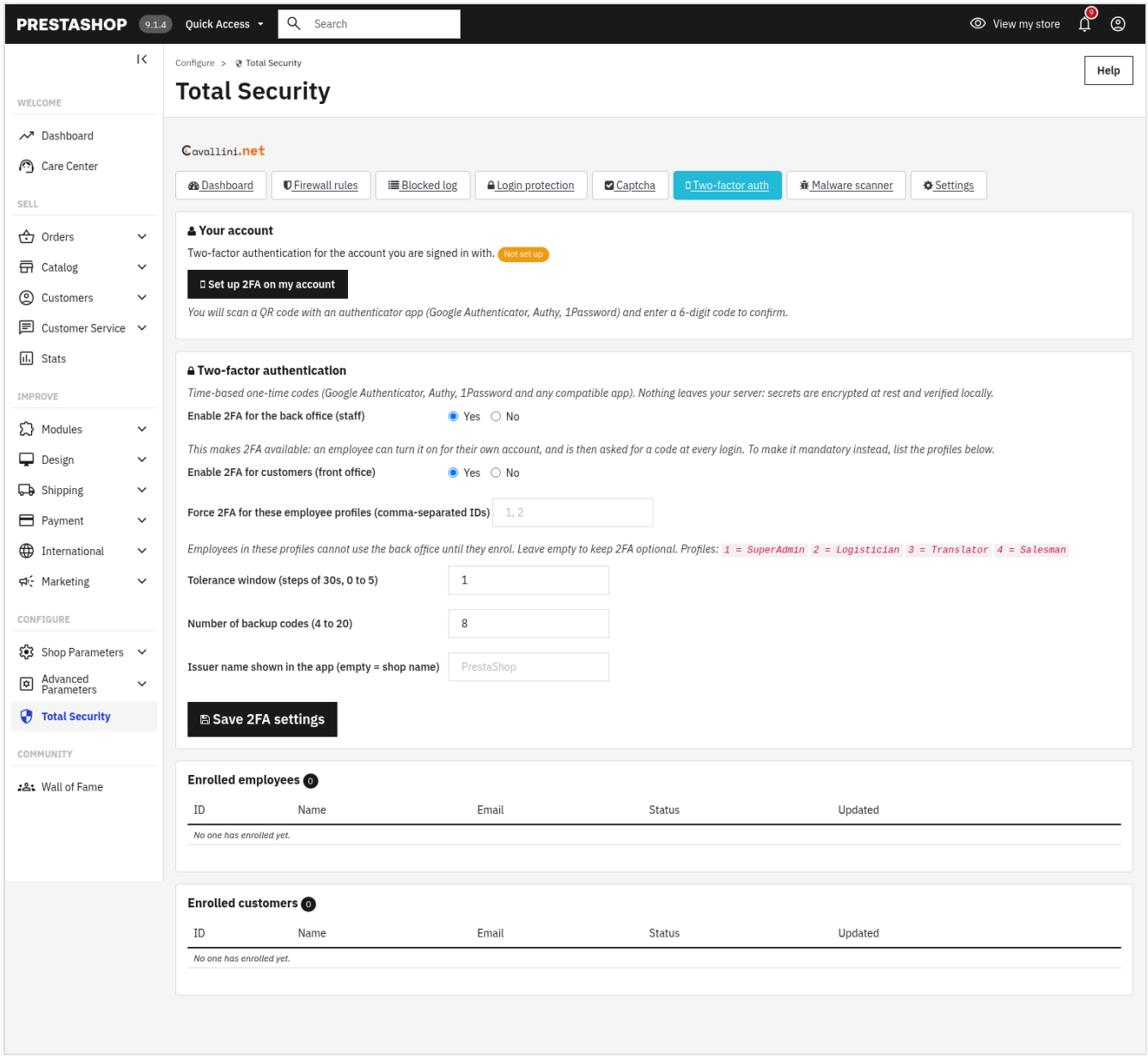


Captcha — provider, protected forms and rate limiting

Two-factor auth (2FA)

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.

- **Your account** — set up 2FA for the account you are signed in with (scan a QR code, enter a 6-digit code).
- **Enable 2FA for the back office** (staff) and/or **for customers** (front office).
- **Force 2FA for specific employee profiles**, by ID (1 = SuperAdmin, 2 = Logistician, 3 = Translator, 4 = Salesman); listed profiles cannot use the back office until they enrol.
- **Tolerance window**, **number of backup codes**, **issuer name** shown in the app.
- **Enrolled employees** and **enrolled customers** are listed and can be reset.

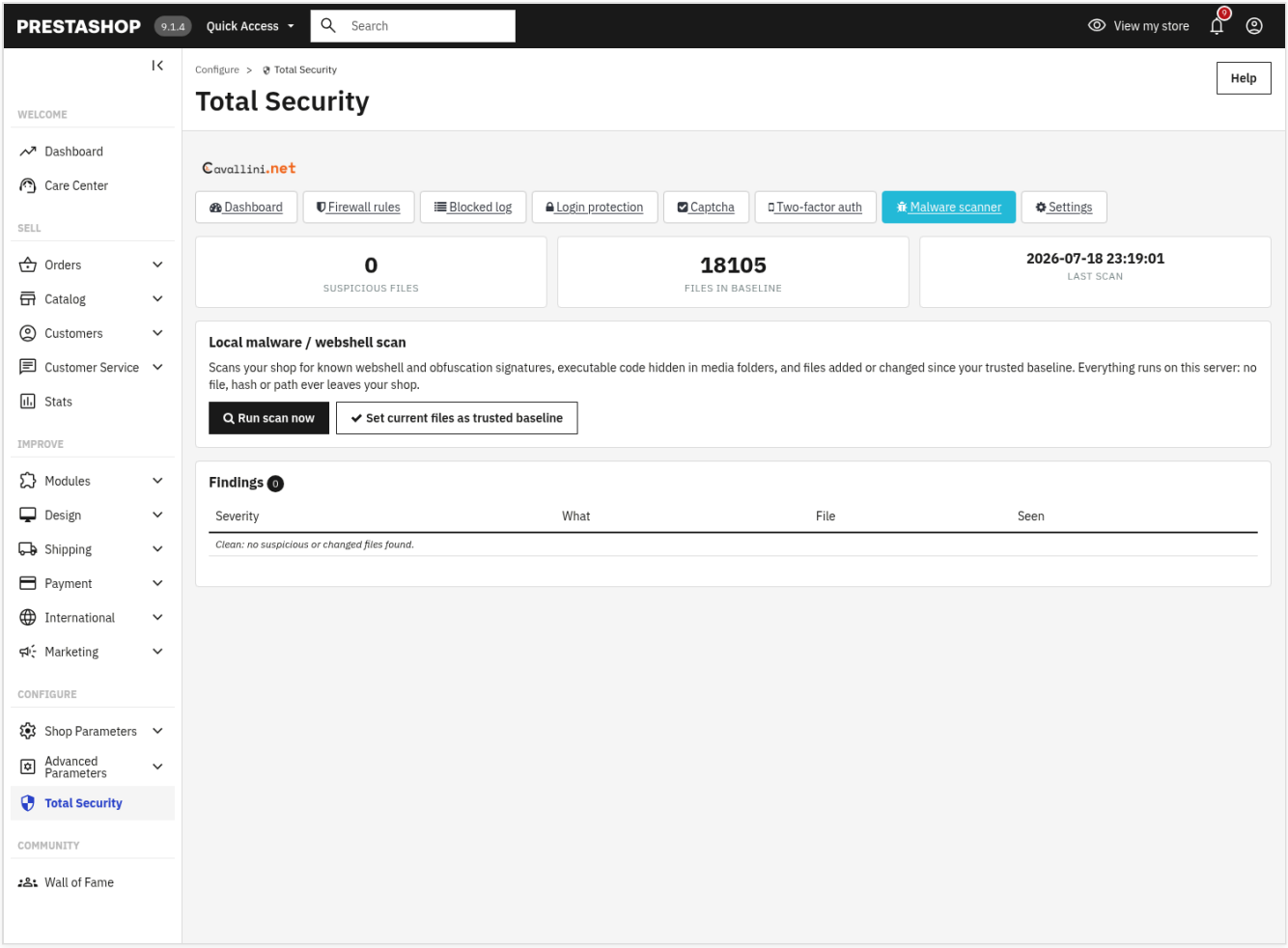


2FA — enrolment, forced profiles and enrolled users

Malware scanner

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

- **Metrics** — suspicious files, files in baseline, last scan.
- **Run scan now** and **Set current files as trusted baseline**.
- Findings are listed with **severity**, **what**, **file** and **when**.

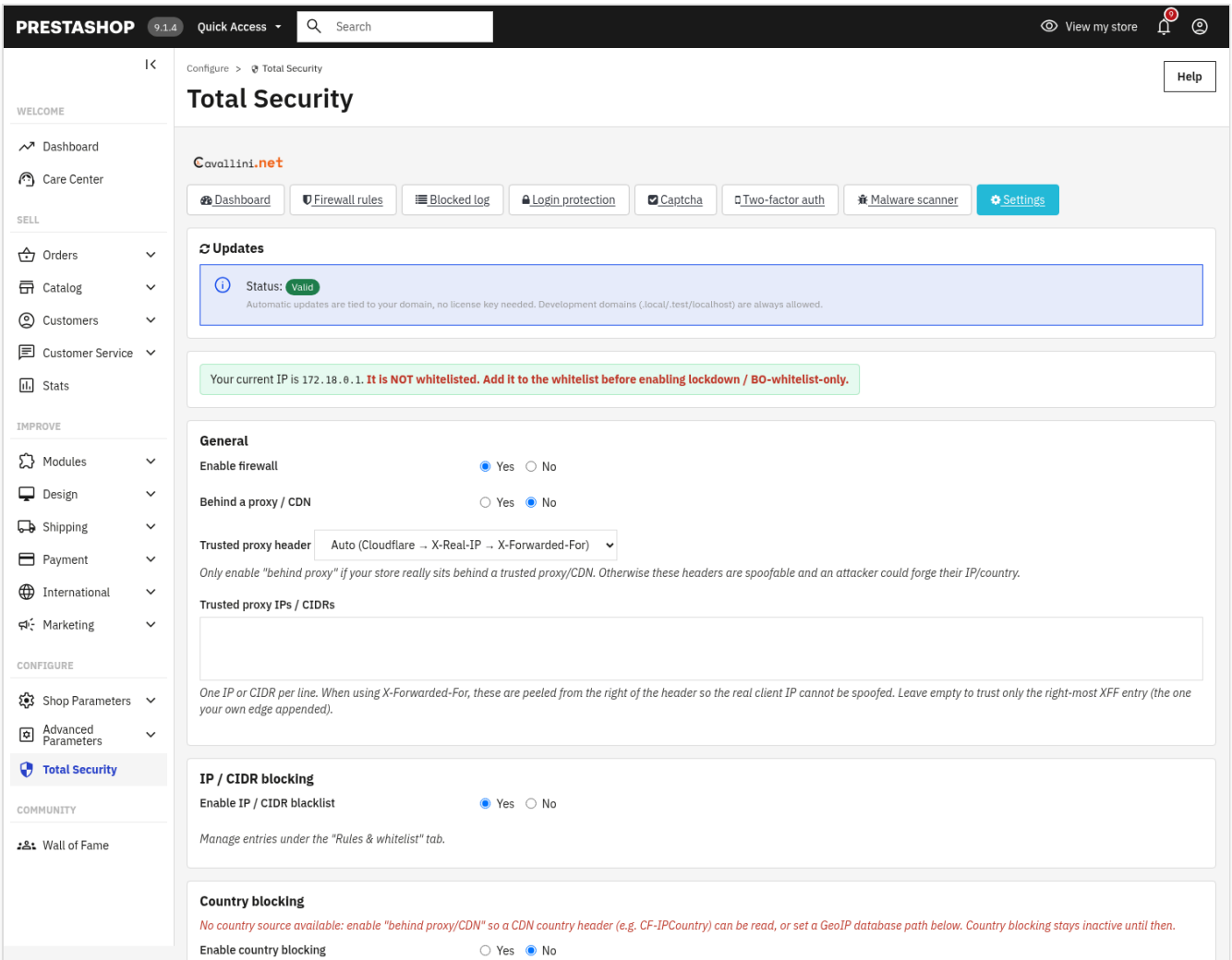


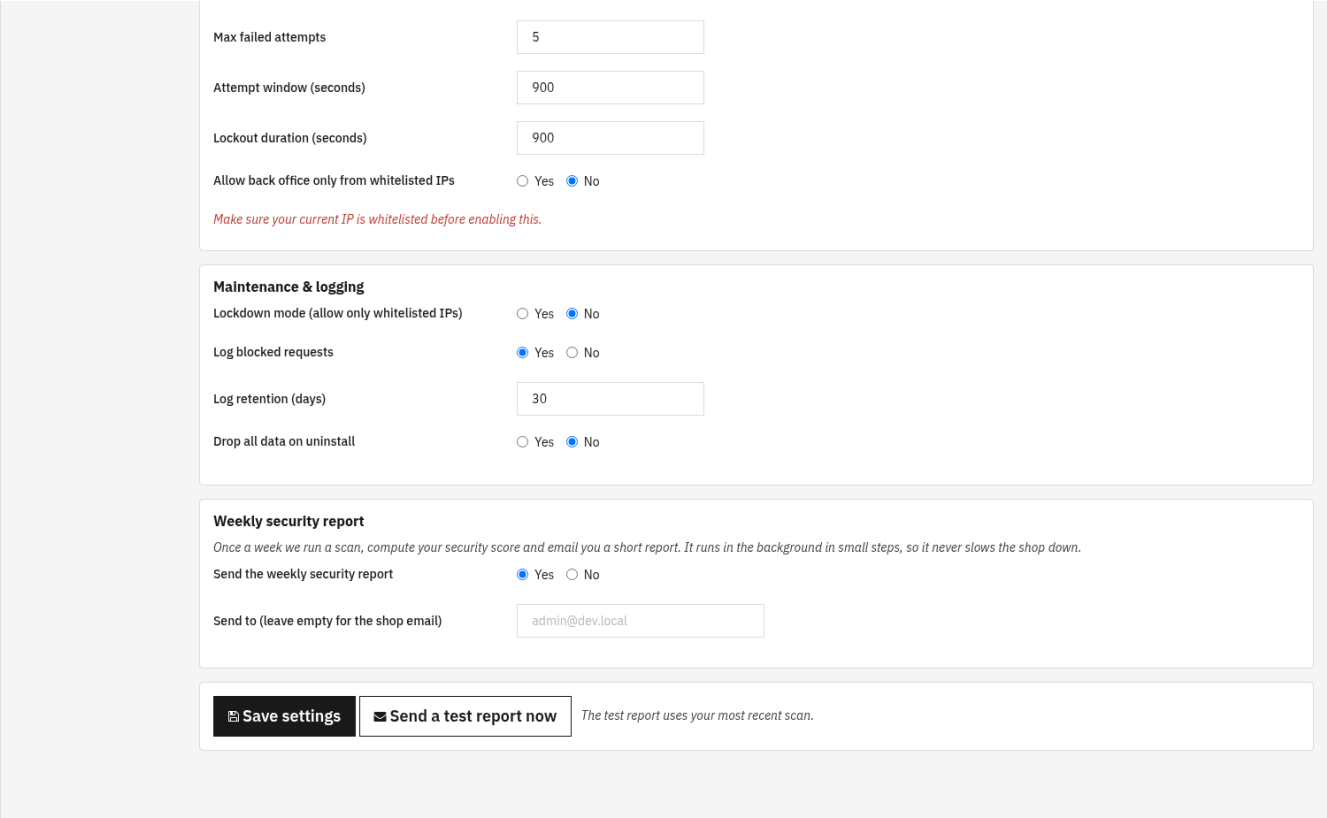
Malware scanner — metrics, scan and findings

Settings firewall configuration

The firewall's own configuration, grouped by section.

- **General** — Enable firewall; **Behind a proxy/CDN** with a trusted proxy header and trusted proxy IPs/CIDRs — only enable this behind a real trusted proxy, otherwise IP/country headers are spoofable.
- **IP/CIDR blocking**.
- **Country blocking** — block-list or allow-list mode, ISO-2 codes, an optional MaxMind GeoLite2 database path or a CDN country header — the database is never bundled, for licensing reasons.
- **Bad bots / user-agents** — enable UA blocking, block empty UA, extra blocked substrings merged with a built-in list.
- **Rate limiting** — max requests per window, window seconds, temporary block duration.
- **Attack-pattern blocking** — SQLi/XSS/LFI/probing.
- **Back-office login protection** — max failed attempts, attempt window, lockout duration, allow back office only from whitelisted IPs.
- **Maintenance & logging** — **Lockdown mode** (allow only whitelisted IPs), log blocked requests, log retention days, drop all data on uninstall.
- **Weekly security report** — emails a short report; runs in the background in small steps so it never slows the shop.

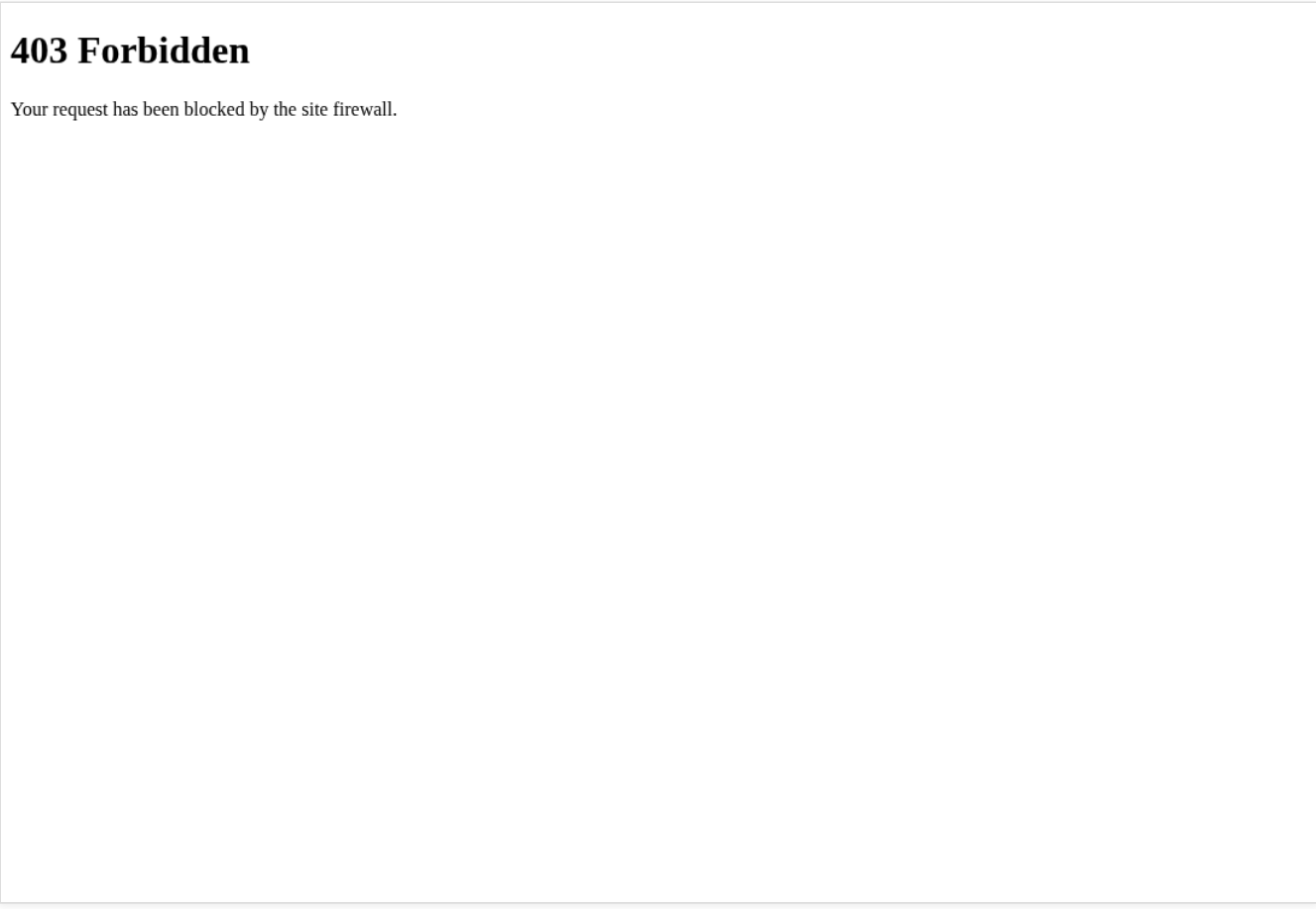

PRESTASHOP
9.1.4
Quick Access
Search
View my store
WELCOME
Dashboard
Care Center
SELL
Orders
Catalog
Customers
Customer Service
Stats
IMPROVE
Modules
Design
Shipping
Payment
International
Marketing
CONFIGURE
Shop Parameters
Advanced Parameters
Total Security
COMMUNITY
Wall of Fame
Configure > Total Security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



Settings — firewall configuration by section

In the front office

When the firewall blocks a request, the visitor gets a plain 403 "Forbidden — your request has been blocked by the site firewall" page: bots and scanners never reach your shop.



In the front office — the 403 page shown when the firewall blocks a request

3. Check that it works

- Open the *Dashboard* and read your security score and checklist.
- Send a request with a scanner-like user-agent (or a probing URL) and confirm you get the 403 block page and a new row in the *Blocked log*.
- After several failed back-office logins, the account/IP is locked in *Login protection*.
- Enable captcha and confirm it appears on the login/registration form.
- Set up 2FA on your account and log in again with a 6-digit code.
- Run the *Malware scanner* and read the findings.

4. FAQ

Does it slow down the shop?

No: the firewall runs first with cheap, indexed lookups; the scanner and the weekly report run in the background.

Will it lock me out?

Whitelist your current IP first (the page warns you, and `127.0.0.1` / `::1` are whitelisted at install); enable lockdown mode or back-office-whitelist-only only after that.

Does any data leave my server?

No: the firewall, the Lightweight captcha option, the 2FA secrets and the malware scanner all run locally on your server.

Does it replace separate firewall / captcha / 2FA modules?

Yes: it is the single, unified security suite.

Do I need to edit my theme?

No: it works through standard hooks and is compatible with any theme.
