



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.

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](#)

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.

PRESTASHOP 9.1.4 Quick Access View my store

Configure > Total Security Help

Total Security

Covallini.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**

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.

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

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 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.

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/1.5.2#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..lrgtWuq9vDkAzj2e_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.3aLDLv	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.3aLDLv	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..Y4owHw7gMJN9G8qihFQhyOR95yfmk.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&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	

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).

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

Help

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.				

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.

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

Yes

No

Provider

Google reCAPTCHA v2 (checkbox)

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)

reCAPTCHA / hCaptcha / Tur

Secret key (server-side only)

reCAPTCHA / hCaptcha / Tur

reCAPTCHA v3 score threshold (0.0 bot, 1.0 human)

0.5

Widget theme

Light

Badge position (v3 / invisible / Turnstile)

Bottom right

Lightweight token lifetime (seconds)

180

Protected forms

Login

Yes

No

Registration

Yes

No

Forgot password

Yes

No

Contact form

Yes

No

Newsletter

Yes

No

Product review

Yes

No

Guest checkout

Yes

No

Advanced

Fail closed (block when the provider is unreachable)

Yes

No

Skip captcha for logged-in customers

Yes

No

Verification timeout (seconds, 1 to 30)

5

Trusted IP whitelist (one per line, skip captcha)

Verify hostname (reject tokens solved on another domain)

Yes

No

Expected hostname (optional, empty = auto)

www.example.com

Verify action (reCAPTCHA v3 and Turnstile)

Yes

No

Rate limiting

Rate-limit failed captcha attempts

Yes

No

Max failed attempts (1 to 1000)

5

Window in minutes (1 to 1440)

15

Save captcha settings

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.

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 — 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**.

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

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.			

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.

Max failed attempts	5
Attempt window (seconds)	900
Lockout duration (seconds)	900
Allow back office only from whitelisted IPs	☐ Yes ☒ No
<i>Make sure your current IP is whitelisted before enabling this.</i>	

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)

 Save settings

 Send a test report now

The test report uses your most recent scan.

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.

403 Forbidden

Your request has been blocked by the site firewall.

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.