



Understand your protection. Stay in control.

A practical guide from first setup to everyday checks, safe changes and recovery.

Version 1.2.0 · English edition · October 17, 2026

Find the next step

1. [Your first safe walkthrough](#)
2. [Read the overview without guessing](#)
3. [Run a scan and understand its limits](#)
4. [Handle a suspicious file carefully](#)
5. [Move from Monitor to selective blocking](#)
6. [Use bans and trusted addresses deliberately](#)
7. [Protect administrator access](#)
8. [Choose log storage and useful notifications](#)
9. [Choose safeguards that fit your website](#)
10. [Optional Content Protection add-on](#)
11. [A practical maintenance routine](#)
12. [Troubleshooting and support](#)
13. [All 52 included controls](#)

Your first safe walkthrough

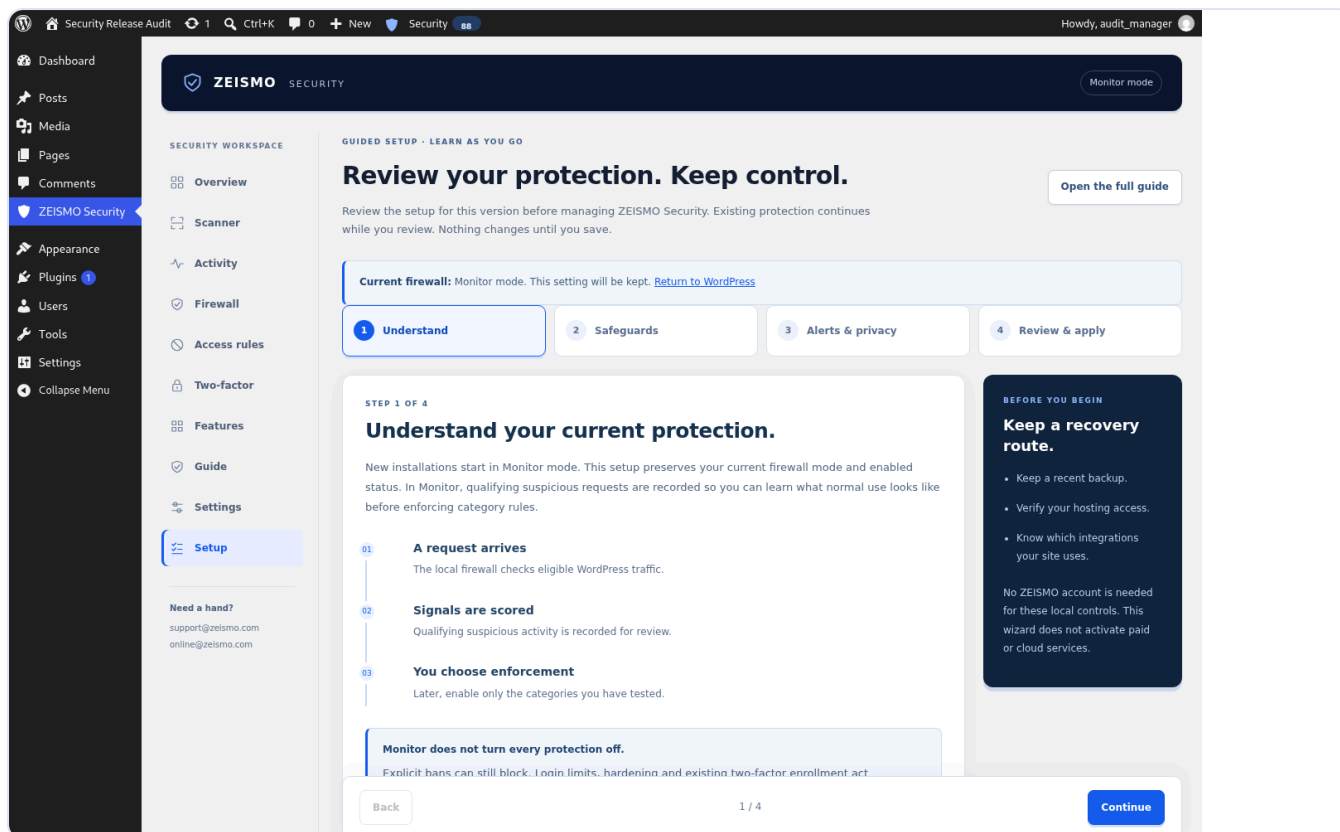
Before changing protection, keep a recent backup and verify that you can reach your hosting control panel. Test changes on a staging copy when possible.

Open Setup. Read the Monitor-mode explanation, choose safeguards, choose alerts and privacy, and review the exact settings before applying. Moving between tutorial steps does not save anything.

Setup review is required when you first open ZEISMO Security after an update. Applying keeps the current firewall enabled status and Monitor or Block mode, access rules, category switches, proxy settings and two-factor enrollment. New installations start with Monitor defaults. Completion opens Overview; help and two-factor recovery remain accessible during review.

The optional first scan inspects eligible local files. A complete first scan creates a local comparison baseline; it does not establish that the files were safe beforehand. Skipping this immediate scan does not disable the daily schedule.

After applying, test a logged-out visit, login, contact form, search, checkout and any app integrations you use. Review Scanner and Activity before switching any firewall category to Block.



The setup review preserves current protection until you apply your choices.

02 / WALKTHROUGH

Read the overview without guessing

Events (24h), Blocked (24h) and Critical (24h) count stored event groups from the previous 24 hours. Similar requests may be grouped; these are not unique attacker or visitor totals.

The timeline offers 24 hours, seven days or 30 days. Its range does not change the labelled 24-hour cards. The current mode tells you whether category enforcement is off, monitoring or blocking selected categories.

The WordPress toolbar score measures eight configuration checks: firewall enabled, login limiter, headers, public REST users, neutral errors, version exposure, disabled editor and absence of an admin username. It is not a safety certificate.

No events can mean no matching traffic, trusted-user testing, caching before WordPress, an inactive firewall or a collection problem. A refresh error means data is unavailable, not zero threats.

Run a scan and understand its limits

Scanner reads wp-admin, wp-includes, plugin folders and theme folders. Eligible extensions are PHP, PHTML, PHP5, JavaScript, HTML, HTM and CSS. Each file must be readable, not a symbolic link and no larger than 2 MB.

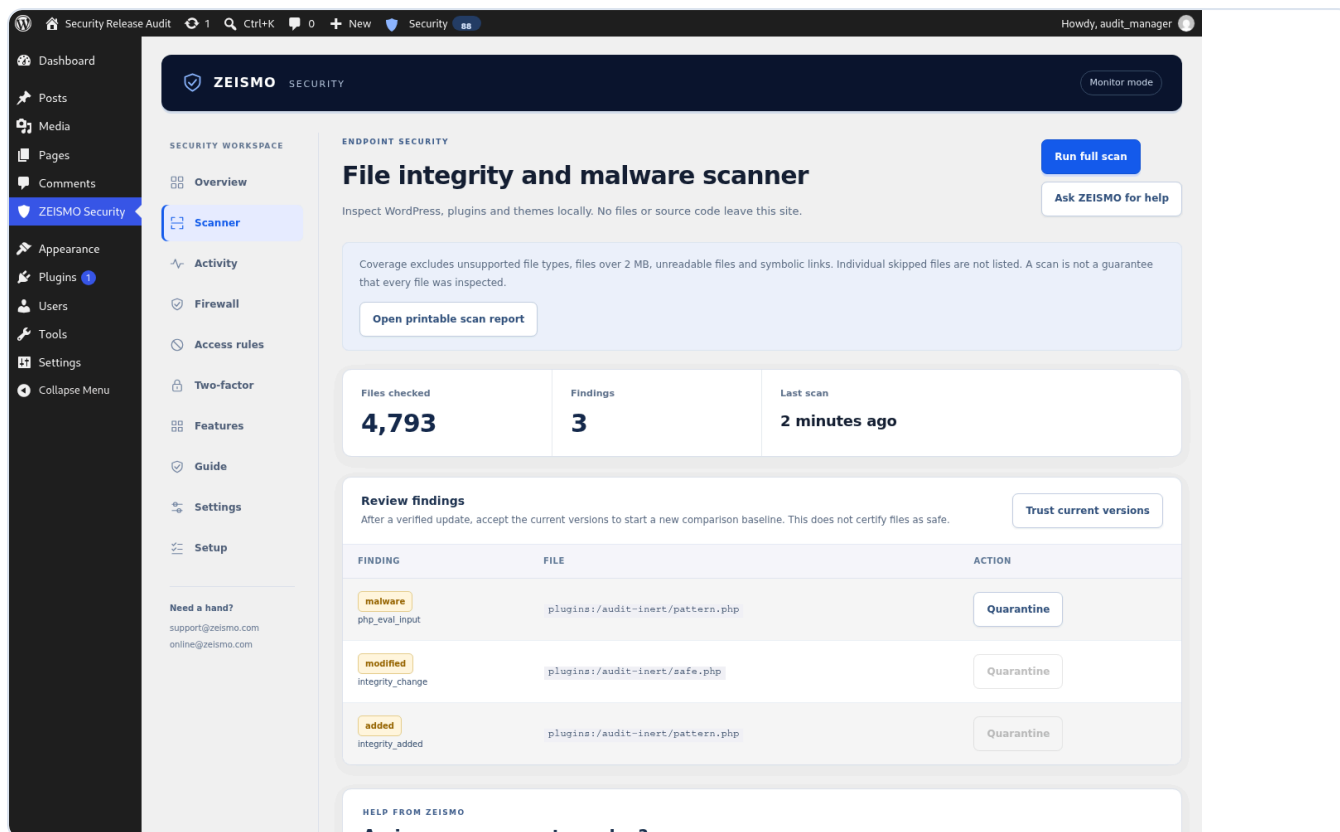
The scan is bounded to 30,000 eligible files. Uploads, the database, root-level WordPress files, unsupported file types and individual skipped files are outside its reported coverage. Up to 500 findings and 100 recent file timestamps are saved.

Added, modified and deleted findings describe differences from your saved local hashes. Malware findings describe packaged pattern matches. Intentional updates and legitimate code can produce findings; never delete blindly.

An incomplete scan keeps the previous baseline. Fix access or execution limits with your host and scan again. Only trust current versions after checking the changes against a known-good source.

Open the printable scan report to print or save a PDF with your browser. It omits absolute server paths and file contents, but relative paths still reveal site structure. Keep the report private.

Daily scanning uses WP-Cron. On a quiet site, ask your host to arrange a dependable cron trigger. Scan completion depends on server resources; a scheduled event is not proof that a scan finished.



The scanner reports observations and coverage; findings require review.

04 / WALKTHROUGH

Handle a suspicious file carefully

Back up first, compare the file with a trusted vendor copy and involve a competent administrator if you cannot determine whether the match is legitimate.

Quarantine requires the host to configure `ZEISMO_SEC_QUARANTINE_DIR` as an existing writable directory outside every public document root. Direct filesystem access is required. The plugin does not create a safe server location automatically.

Only a currently selected malware finding in a plugin or theme can be moved. Core files, symbolic links, missing files and this active Security plugin are rejected. Quarantine can stop part of the website from working.

There is no restore or repair button. If you quarantined a legitimate file, your host or developer must restore it from a trusted source and check the site. Do not automatically accept a new baseline just to hide the incident.

Move from Monitor to selective blocking

Monitor records qualifying suspicious requests without category-based blocking. Block enforces only an enabled top category when the score reaches the configured threshold. The default threshold is 70; allowed values are 20–100.

Categories are SQL injection, cross-site scripting, path traversal/file inclusion, command injection and vulnerability scanners. A scanner signature describes a suspicious client or request pattern, not proof of a successful vulnerability exploit.

Explicit address bans can block in Monitor mode. Trusted addresses and users with the `edit_posts` capability bypass the firewall. Normal admin pages, WP-Cron and command-line requests are excluded. Test public flows while logged out.

The engine runs inside WordPress and allows the request if its processing throws an error. It does not protect traffic served entirely by a cache/CDN, replace server patching or provide DDoS mitigation.

Choose Direct connection unless your host has verified the proxy arrangement. Cloudflare/proxy settings also require trusted proxy ranges configured through `ZEISMO_SEC_TRUSTED_PROXIES`. Never trust arbitrary forwarding headers.

If a legitimate visitor is blocked, note the route and reference, review Activity, then relax the affected category or return to Monitor. If an explicit ban is involved, changing Monitor alone may not help; contact your administrator to review the rule.

Use bans and trusted addresses deliberately

Available new ban types are a single IP address, a CIDR range or a user-agent substring. Choose Log only to observe a match, or Block to enforce it. Duration choices are one hour, one day, one week or permanent.

Trusted addresses accept IP or CIDR and bypass firewall processing, including explicit bans. Use only addresses you control. Prefer temporary entries while testing.

Use Remove ban or Remove trust beside the relevant rule, read the confirmation and confirm. Removing a ban stops that rule from denying matching requests. Removing trust restores firewall checks for matching visitors. Changes are recorded in Recent security changes. Expired rules can also be removed.

Older records may contain country or score match types. This request pipeline does not supply those values to the ban matcher, so those records must not be relied on for protection. New setup does not offer these unsupported rule types.

Recent security changes shows a bounded history of selected administrative events. It is not an external, tamper-proof audit trail. Keep independent backups and server logs for incident investigation.

Protect administrator access

The login limiter tracks failures by client address and username. The default is eight failures in a 15-minute transient window, renewed by failed attempts. A successful login clears that combination. Correct proxy configuration matters.

Two-factor enrollment is optional and applies to your own administrator account on a single-site HTTPS installation. Setup never enables it silently. Open Two-factor, confirm your current password, add the key and confirm a working code.

Save recovery codes immediately. Each is one-use with your password. Replacing codes invalidates the old ones and signs out other sessions; your setup session stays open. Five bad code attempts trigger a five-minute rate window.

Enrolled users cannot authenticate through application passwords or XML-RPC. Standard WordPress login is supported; custom login screens and SSO need separate testing. Check your integrations before enrolling.

If you lose both the authenticator and recovery codes, contact your hosting administrator. Deactivating the plugin stops this protection; changing WordPress authentication salts can require host-assisted re-enrollment. An old database restore may revive used recovery codes.

Choose log storage and useful notifications

Store IP addresses controls address storage in firewall and failed-login records. Turning it off affects future records; it does not immediately erase existing data. Hashed identifiers and other event metadata may still be recorded.

Mask addresses applies to future firewall event addresses only, not failed-login address records. Do not treat masking as complete anonymisation of all logs.

Event retention can be set from seven to 365 days, with 60 as the default. Scheduled maintenance deletes old firewall and failed-login records. Firewall event IP addresses are also cleared after 90 days; failed-login IP addresses follow the chosen retention period. Cron delays can delay deletion.

Critical-event email is optional. A newly logged event scoring at least 80 can produce a notice, with a one-hour duplicate-fingerprint cooldown. It uses the WordPress mail system; transport acceptance does not prove inbox placement.

Administrator/security-change email is a separate optional setting. It covers selected administrator, firewall/login and two-factor changes, with at most ten attempts per clock hour and a five-minute identical-notice cooldown. Failed sends are not retried.

Changing the notification address or disabling change alerts can notify the previous address, subject to sending limits. Do not enter an address you do not control. During setup, mail remains off unless you select the corresponding switches.

Local protection does not require a ZEISMO account. A private scan report is created locally. Email notifications leave through your configured mail service. This release does not activate cloud AI, reputation feeds or paid services.

Choose safeguards that fit your website

Browser headers add nosniff, SAMEORIGIN framing, a strict-origin-when-cross-origin referrer policy and a permissions policy denying camera, microphone and geolocation. Test embeds and device-dependent features before leaving this on.

Public REST user protection hides the standard logged-out user endpoints. Numeric-author protection returns a 404 for logged-out numeric author lookups. Neither hides all public author information.

Neutral login errors reduce information in error messages. Version reduction removes generator output but cannot conceal every version reference.

Disabling the built-in file editor is recommended for sites with controlled deployment. A constant already defined by your host can override the plugin choice; the current request cannot undo a constant it already loaded.

XML-RPC is left off as a blocking choice by default. Enable Disable XML-RPC only if remote publishing, Jetpack or other integrations do not need it. Saved changes may take effect on the next request and cached pages may need purging.

Optional Content Protection add-on

Content Protection is a separate add-on included in existing Security Pro and higher plans, with no separate charge. It is not bundled into the free core. Download it from your Security account when available, install it separately, connect your account and verify Pro access before enabling visitor controls. This release is awaiting publication approval.

The master switch is off by default. Independent controls deter text selection, copy/cut actions, context menus and image dragging on eligible public pages. Only selected controls apply after Save changes.

Buttons, links, form fields, editable content, accessible interactive widgets and normal popups are exempt from interception. Test the real theme, menus, search, checkout and dialogs while logged out before enabling it for visitors.

Administrators, previews, feeds, API responses and recognised WooCommerce cart, checkout and account pages are excluded. You can add page IDs and path-prefix exceptions. A path prefix can exclude multiple URLs; review it carefully.

Changing the labelled sample preview does not save settings or prove compatibility with every theme. Save first, purge full-page/CDN caches and test a fresh logged-out window. Do not serve cached administrator pages to visitors.

This is casual copy deterrence, not DRM. Visitors can still use screenshots, page source, disabled JavaScript or other extraction tools. It does not establish copyright ownership or prevent determined copying.

Paid controls pause when the subscription is past due, unpaid, paused, expired, cancelled or otherwise ineligible. Scheduled cancellation remains valid until the paid period ends. Settings and free security remain intact; verified renewal resumes saved controls. Browser and WordPress checks run about every five minutes, with a maximum fifteen-minute cached lease. Connection failure cannot extend that lease. Purge page caches after changes; modified local code cannot be remotely guaranteed.

A practical maintenance routine

After setup: test public pages and important forms, confirm your own login works and check the first scan result. Add two-factor protection only when you have prepared a recovery method.

Each week: review recent critical events and unfamiliar administrator changes, check Last scan is recent, review temporary access rules and verify your backup can be restored.

After updates: compare changed files with the expected release, test site functions and accept a baseline only after verification. A new update can be legitimate even when many files change.

Before changing enforcement: keep hosting access available, test one category at a time and review any affected customer journey. Do not deliberately attack a live customer site to test a rule.

Troubleshooting and support

Use Contact ZEISMO support on any Security screen, or Ask ZEISMO for help in Scanner, to open a private conversation at app.zeismo.com/portal/security/support. Sign in or create a free account and verify your email. No paid plan is required. Submit your question, read replies while the page is open, or return to the same conversation later. Email notifications are not automatic. No site data, logs, files or credentials are uploaded by the plugin.

No activity appears: check the mode, use a logged-out visit, consider caching and remember that only qualifying suspicious requests are recorded. Normal traffic is not a traffic-analytics feed.

Scan incomplete or stale: check file readability, resource limits and WP-Cron with your host. A missing last-scan time means no saved result, not a clean scan.

Quarantine unavailable: configure private storage through your host. Do not choose a public uploads directory or move files manually without a recovery plan.

Email missing: verify the saved recipient, the alert switch, rate limits and your WordPress mail setup. Check spam and mail logs; a sent or accepted status is not confirmed delivery.

Settings appear unchanged: submit Save, refresh and check the stored switch. For header, version or editor changes, open a new request and purge relevant caches. Host constants can take precedence.

A normal request is blocked: distinguish a category decision from an explicit ban. Monitor affects category enforcement; trusted-address exceptions are broad and should be tightly limited.

Contact support@zeismo.com or online@zeismo.com. Include plugin/WordPress/PHP versions, the affected screen, approximate time and redacted error text. Never send passwords, authenticator keys, recovery codes, private tokens or unredacted security reports in a public support thread.

The screenshot displays the Zeismo Security Support chat interface. On the left is a sidebar with a 'YOUR PRODUCTS' section containing links for Overview, Security support (selected), ZEISMO Security, ZEISMO SEO, WhatsApp bot, CRM, Refer & earn, and Rewards. Below this is a 'BOT' section with links for Builder, Inbox, Contacts, Campaigns, Templates, Flows, Integrations, and Billing. At the bottom is an 'AGENCY' section with links for Services, Requests, and Documents, followed by a 'Collapse' button. The main chat area has a header with 'Portal / 48f2690f bd4f 4de9 9a20 3236528a09b1', a search bar, and language/translation icons. A 'Back to your conversations' link is at the top. The chat title is 'ZEISMO / SECURITY SUPPORT' with a subtitle 'TEST ONLY: Setup and protection review'. A status message reads: 'Replies are saved in this conversation. You can leave and return later. Waiting for support · Checking for replies...'. The conversation history shows a customer message from 2026-10-17 17:45:46 UTC: 'TEST ONLY: I updated Security. Will reviewing setup keep my existing firewall rules?'. A support response from 2026-10-17 17:45:47 UTC follows: 'TEST ONLY: Yes. Setup review keeps your current firewall mode and access rules. Review your choices, apply, and continue to Overview.' Below the messages is a 'Your reply' text input field. At the bottom, a disclaimer states: 'Do not send passwords or private access credentials. Support is available in English. Email notifications are not sent from this conversation; return here to check later replies.' and a 'Send reply' button is present.

Demonstration conversation with test data. Replies are saved for later visits.

Every control, explained

Included does not mean enabled. Some entries describe different uses of the same scanner or firewall. These local core controls need no paid plan.

01 / 52

WordPress core integrity scanner

Compares eligible WordPress core files with a locally saved baseline.

How to use it

Run Scanner on a known-good site. After later scans, investigate added, modified or deleted files before trusting a new baseline.

Limits to understand

Covers wp-admin and wp-includes. It does not download official WordPress checksums, inspect root-level files or prove the first baseline is clean.

Manage in: Scanner

02 / 52

Plugin integrity monitoring

Shows changes to eligible files inside installed plugin folders.

How to use it

Scan before and after a planned plugin update. Compare unexpected changes with a trusted copy of that plugin.

Limits to understand

Runs during scans, not continuously. An intentional update can produce legitimate findings.

Manage in: Scanner

Theme integrity monitoring

Compares eligible theme files against the saved local baseline.

How to use it

Scan after a theme update or an unexpected appearance change. Confirm intentional edits before accepting the current versions.

Limits to understand

Does not inspect database-stored templates or certify a theme as malware-free.

Manage in: Scanner

Basic malware scanner

Looks for packaged suspicious-code patterns in eligible local files.

How to use it

Run Scanner, read each rule and file path, then ask a trusted developer to investigate uncertain matches.

Limits to understand

Pattern matches are clues, not a diagnosis. Both false positives and missed threats are possible.

Manage in: Scanner

Malicious PHP pattern detection

Flags selected PHP execution patterns involving request input or encoded code.

How to use it

Review a flagged PHP file against its original vendor version before changing it.

Limits to understand

Uses a fixed set of expressions; it does not execute the file or understand every PHP program.

Manage in: Scanner

Base64/encoded malware detection

Finds selected long encoded strings and decoding-plus-execution patterns.

How to use it

Check why a plugin or theme contains the flagged encoding and whether the file matches its trusted source.

Limits to understand

Encoding alone is not malicious. Other encodings and obfuscation can be missed.

Manage in: Scanner

Backdoor detection

Flags selected patterns often associated with remote command execution.

How to use it

If an unexpected file matches, restrict access through your host and investigate the site with a security specialist.

Limits to understand

Shares the local malware rules; it is not an exhaustive backdoor inventory.

Manage in: Scanner

Suspicious file scanner

Brings signature findings and baseline changes into one review list.

How to use it

Start with unfamiliar files and changes outside your maintenance window. Keep a backup before remediation.

Limits to understand

Only eligible files in the configured scan roots are examined. Empty results are not a clean-site certificate.

Manage in: Scanner

Recently modified file report

Records modification times for recently changed eligible files during a scan.

How to use it

Use the baseline findings in Scanner to review changes; the saved scan also keeps up to 100 recent file timestamps for technical investigation.

Limits to understand

The current screen has no separate recent-files viewer. Timestamps cover the previous seven days and can be changed; they do not establish when an intrusion occurred.

Manage in: Scanner

Admin-user monitoring

Records administrator creation and administrator-role grants in the local audit history.

How to use it

Open Access rules and review Recent security changes for accounts you do not recognise.

Limits to understand

This is event recording, not continuous account-behaviour analysis or automatic account suspension.

Manage in: Access rules

Failed-login monitoring

Records failed login attempts and supports the local login limiter.

How to use it

Keep login limiting on in Settings. Ask your site administrator to inspect local login records when investigating repeated failures.

Limits to understand

Failed-login records are stored separately; the Activity screen is the firewall event log, not a complete failed-login viewer.

Manage in: Settings

Login attempt limiting

Temporarily rejects repeated failed logins for an address-and-username combination.

How to use it

Enable Limit repeated login attempts. The default threshold is eight failures; wait 15 minutes after the last failed attempt before trying again.

Limits to understand

Depends on correct client-address detection. It is not a global distributed-attack defence and can affect users sharing an address and username.

Manage in: Settings

Brute-force protection

Uses the local login-attempt limiter to slow repeated password guesses.

How to use it

Enable the login limiter and add two-factor authentication to your own administrator account.

Limits to understand

This entry describes the same limiter, not an additional independent protection engine.

Manage in: Settings

Username enumeration protection

Blocks unauthenticated numeric author lookups that can reveal a username.

How to use it

Enable Block numeric author username discovery in Settings; test public author links afterwards.

Limits to understand

Does not hide public display names, existing author pages or usernames disclosed by another plugin.

Manage in: Settings

Disable XML-RPC option

Disables XML-RPC methods and removes the pingback response header.

How to use it

Turn on Disable XML-RPC only after checking whether mobile publishing, Jetpack or another integration needs it.

Limits to understand

Can break integrations. It is off by default and is separate from firewall Monitor mode.

Manage in: Settings

XML-RPC brute-force protection

Removes the XML-RPC method surface when XML-RPC is disabled.

How to use it

Use the Disable XML-RPC switch if none of your integrations depends on this endpoint.

Limits to understand

This is the XML-RPC disable control, not a separate rate limiter for applications that keep XML-RPC enabled.

Manage in: Settings

Disable WordPress file editor

Removes the built-in plugin and theme code editors from the dashboard.

How to use it

Keep this enabled when you deploy edits through a controlled development process. Reload the next request after changing it.

Limits to understand

Does not prevent filesystem, hosting or deployment access. A host-level `DISALLOW_FILE_EDIT` setting can keep the editor disabled even when this switch is off.

Manage in: Settings

WordPress version exposure reduction

Removes WordPress generator output that advertises the version.

How to use it

Keep Reduce WordPress version exposure enabled and continue installing security updates.

Limits to understand

Other assets or endpoints may still reveal a version. Concealing it is not a substitute for updates.

Manage in: Settings

Basic security headers

Adds browser headers for content sniffing, framing, referrers and device permissions.

How to use it

Enable Send safe browser security headers, then test embedded pages and any feature using a camera, microphone or location.

Limits to understand

SAMEORIGIN restricts cross-site framing. Camera, microphone and geolocation are denied by this header set. Server/CDN rules can override responses.

Manage in: Settings

REST API user enumeration protection

Removes public WordPress user-list and user-detail REST routes for logged-out visitors.

How to use it

Enable Stop public REST API user enumeration. Check any public author directory or front-end app that uses these endpoints.

Limits to understand

Logged-in access and other plugins may still expose account information.

Manage in: Settings

Login error obfuscation

Uses one neutral error message when WordPress rejects a login.

How to use it

Enable Use neutral login error messages to avoid explaining which part of a login was wrong.

Limits to understand

Changes the message, not password strength or the outcome of authentication.

Manage in: Settings

Default admin username warning

Flags an account using the predictable username admin.

How to use it

Review the Overview warning and manage administrator accounts through WordPress Users. Ensure another verified administrator works before changing access.

Limits to understand

The warning does not rename or delete an account automatically.

Manage in: Overview

Inactive administrator detection

Highlights administrator accounts without a recorded recent login.

How to use it

Review the Overview warning with the account owner before deciding whether access is still needed.

Limits to understand

Uses a 90-day threshold and locally recorded logins or registration age. Missing pre-installation history is not proof the person never logged in.

Manage in: Overview

Basic security dashboard

Summarises recorded firewall events, critical events and current mode.

How to use it

Open Overview, check whether the firewall is Off, Monitoring or Blocking, and review Activity before changing enforcement.

Limits to understand

Counts describe stored event groups, not unique attackers, visitors or every request to your server.

Manage in: Overview

Security configuration score

Shows how many of eight configuration checks currently pass.

How to use it

Hover or open the Security item in the WordPress toolbar, then review the relevant settings.

Limits to understand

A score of 100 is not proof a site is secure. It is a configuration checklist, not a penetration test or malware result.

Manage in: Overview

Manual security scan

Lets an administrator start a local file scan on demand.

How to use it

Open Scanner and choose Run full scan. Wait for the request to finish, then review coverage, findings and last-scan time.

Limits to understand

Large sites can hit file or server execution limits. An incomplete scan should never be treated as full coverage.

Manage in: Scanner

Basic email security alerts

Can notify a selected address about newly recorded critical firewall events.

How to use it

Enable critical-event emails in Settings and choose an inbox you monitor. Review the corresponding Activity entry when a notice arrives.

Limits to understand

Uses the site mail system. Repeated notices for the same event fingerprint are suppressed for one hour; delivery to an inbox is not guaranteed.

Manage in: Settings

Security activity summary

Shows time-bounded patterns in the recorded firewall activity.

How to use it

Use Overview for totals, categories, targeted routes and the activity timeline; use Activity for event details.

Limits to understand

The timeline range does not change the four labelled 24-hour summary cards. Repeated event records may be grouped.

Manage in: Overview

Scheduled malware scanning

Registers a daily local scan through WordPress scheduling.

How to use it

After activation, check that Last scan advances. Ask your host to check WP-Cron if a low-traffic site stops running scheduled work.

Limits to understand

WP-Cron depends on requests or a configured system trigger. A daily schedule is not an exact delivery time or real-time monitoring.

Manage in: Scanner

Advanced malware signatures

Applies the additional packaged patterns used by the same local scanner.

How to use it

Review the named rule for each finding and compare suspicious code with a trusted vendor copy.

Limits to understand

This build has eight fixed pattern rules, not a cloud intelligence feed or continuously updated signature subscription.

Manage in: Scanner

Heuristic malware detection

Uses suspicious-code patterns as practical investigation clues.

How to use it

Review the context of a finding instead of deleting a file just because a pattern matched.

Limits to understand

The heuristics are fixed rules, not AI reasoning, sandbox execution or guaranteed malicious-behaviour detection.

Manage in: Scanner

JavaScript malware detection

Inspects eligible JavaScript files with the packaged pattern rules.

How to use it

Investigate unexpected redirect code and compare it with the intended behaviour of the site.

Limits to understand

Does not run JavaScript or inspect every script delivered dynamically, remotely or from the database.

Manage in: Scanner

SEO spam detection

Looks for a small set of spam-related words near link markup in eligible files.

How to use it

Check a flagged file and compare rendered content with the content you intentionally published.

Limits to understand

Database content is not scanned. Legitimate writing may match, and many spam techniques fall outside these patterns.

Manage in: Scanner

Redirect malware detection

Flags selected JavaScript assignments that redirect to an external URL.

How to use it

Verify the destination and why the redirect exists before deciding whether to remove it.

Limits to understand

A normal payment, login or navigation redirect can match. Server, database and other redirect mechanisms may be missed.

Manage in: Scanner

Malicious iframe detection

Flags selected external iframes that appear hidden in eligible source files.

How to use it

Review the iframe destination and compare the file with a trusted version.

Limits to understand

Hidden iframes can be legitimate. Visible, dynamically created or differently hidden frames may not match.

Manage in: Scanner

Webshell detection

Looks for selected upload-and-command-execution patterns.

How to use it

Treat an unfamiliar matching file as an investigation priority and involve your hosting administrator.

Limits to understand

A fixed pattern match does not confirm a webshell, and absence of a match does not rule one out.

Manage in: Scanner

One-click infected-file quarantine

Moves a selected reported suspicious plugin or theme file into private server storage.

How to use it

Ask the host to configure private quarantine storage first. Back up the site, verify the finding and choose Quarantine for an eligible malware finding.

Limits to understand

Can break the affected plugin or theme. Core files and this active Security plugin cannot be moved by this action. There is no automatic repair or restore button.

Manage in: Scanner

Two-factor authentication using TOTP

Adds authenticator codes to your own administrator login after explicit enrollment.

How to use it

Use Two-factor over HTTPS, confirm your password, add the setup key to an authenticator and verify a fresh code. Save the recovery codes immediately.

Limits to understand

Single-site standard WordPress login only. Existing application passwords and XML-RPC authentication are blocked for enrolled users; custom login and SSO need compatibility testing.

Manage in: Two-factor

Backup authentication recovery codes

Provides one-use alternatives when your authenticator is unavailable.

How to use it

Keep the codes in your password manager or offline. Sign in with your password and one unused recovery code.

Limits to understand

Each code works once. Replacing the codes invalidates the old set and signs out other sessions. Restoring an old database backup may restore previously used codes.

Manage in: Two-factor

Temporary IP bans

Blocks or logs matching addresses or ranges until a chosen expiry.

How to use it

In Access rules, choose IP address or CIDR, enter a value you have verified, and select one hour, one day or one week.

Limits to understand

A block rule can act even in Monitor mode. Addresses can be shared or change; broad ranges can affect legitimate visitors.

Manage in: Access rules

Permanent IP blocklist

Keeps an explicit address restriction active without an expiry.

How to use it

Use a permanent rule only when the target and impact are understood. Review the rule and its hit count regularly.

Limits to understand

Remove ban stops enforcement by that rule after confirmation. The removed rule remains visible for review; other protections still apply.

Manage in: Access rules

IP allowlist

Lets a trusted address or CIDR bypass this plugin's firewall evaluation.

How to use it

Add only verified addresses you control in Trusted addresses, preferably with a short expiry.

Limits to understand

The exception also bypasses explicit firewall bans. Remove trust restores normal firewall checks. Logged-in administrators and editors keep their built-in exemption; WordPress authentication and the separate login limiter remain unchanged.

Manage in: Access rules

Detailed security audit log

Keeps a bounded local history of selected account and security actions.

How to use it

Review Recent security changes under Access rules after a scan, baseline acceptance, quarantine or administrator change.

Limits to understand

The view shows recent records, not a complete forensic history of all WordPress actions or a tamper-proof external archive.

Manage in: Access rules

Application-level WordPress firewall

Examines selected requests after they reach WordPress and records suspicious signals.

How to use it

Start in Monitor, test normal visitor journeys, then enable Block mode for the categories you have reviewed.

Limits to understand

Not an edge firewall or DDoS service. Trusted users/addresses, normal admin requests, cron and CLI are excluded; an internal firewall error allows the request through.

Manage in: Firewall

SQL injection protection

Scores selected request patterns associated with SQL injection.

How to use it

Review SQL injection events, then enable its category in Block mode if the observed traffic warrants it.

Limits to understand

Blocking also requires the risk threshold. Pattern inspection does not fix vulnerable application code.

Manage in: Firewall

Cross-site scripting attack protection

Scores selected suspicious script and markup patterns in request input.

How to use it

Test forms and content-submission tools before enabling the XSS category in Block mode.

Limits to understand

Legitimate HTML can resemble an attack. It does not scan stored database content or guarantee protection against every XSS technique.

Manage in: Firewall

Remote code execution exploit filtering

Checks selected request patterns that can indicate an attempt to execute commands or code.

How to use it

Review the event context before enabling Command injection in Firewall.

Limits to understand

Shares the command-injection request rules. It is not a patch for a vulnerable plugin or an operating-system sandbox.

Manage in: Firewall

Local file inclusion protection

Checks selected path and wrapper patterns associated with local file inclusion.

How to use it

Review related events and enable Path traversal & file inclusion only after testing normal site requests.

Limits to understand

Shares the traversal category and does not change filesystem permissions or repair vulnerable code.

Manage in: Firewall

Remote file inclusion protection

Looks for selected suspicious file-wrapper and inclusion patterns in requests.

How to use it

Use the Path traversal & file inclusion category and keep WordPress, plugins and themes updated.

Limits to understand

Shares the traversal rules; not every external URL or remote inclusion technique is detected.

Manage in: Firewall

Path traversal attack filtering

Scores attempts to reach unintended paths using selected traversal patterns.

How to use it

Inspect the affected route and test legitimate download or file-selection flows before enforcing the category.

Limits to understand

Patterns and normalisation are bounded. A matching request is evidence to review, not proof a file was accessed.

Manage in: Firewall

Command-injection filtering

Scores selected shell-command patterns in incoming request input.

How to use it

Enable the Command injection category only after reviewing its Monitor-mode findings.

Limits to understand

Shares rules with the remote-code-execution label. Detection is not operating-system process monitoring.

Manage in: Firewall

Request anomaly detection

Combines weighted request signals into a risk score from 0 to 100.

How to use it

Review event categories and scores. In Block mode, an enabled top category and a score at or above the threshold are required for category enforcement.

Limits to understand

This is deterministic rule scoring, not behavioural AI or a probability that an attacker succeeded. Signals below 20 are not recorded as firewall events.

Manage in: Firewall

Need help with an unresolved issue?

Tell us what happened, the affected screen and plugin version. Never send passwords, recovery codes or private credentials.

support@zeismo.com · online@zeismo.com