Dashboard
Analytik
Beiträge
Medien
Seiten
Kommentare
Spectra
Rank Math SEO
Elementor
Templates
Hello
Design
Plugins
Benutzer
Werkzeuge
Einstellungen
Copy & Delete Posts
WP Mail SMTP
Folders Settings
WP Armour
UpdraftPlus
Wordfence
Dashboard
Firewall
Scan
Tools
Audit Log
Login Security
All Options
Help
Upgrade to Premium
Menü einklappen

Search All Options

RESTORE DEFAULTS | CANCEL CHANGES | SAVE CHANGES

All Options

EXPAND ALL

These options are also available throughout the plugin pages, in the relevant sections. This page is provided for easier setup for experienced Wordfence users.

Wordfence Global Options

Wordfence License

View Customization

- [x] Display "All Options" menu item
- [ ] Display "Blocking" menu item
- [ ] Display "Live Traffic" menu item
- [x] Display "Audit Log" menu item

General Wordfence Options

- [x] Update Wordfence automatically when a new version is released?
  Automatically updates Wordfence to the newest version within 24 hours of a new release.

Where to email alerts: admin@anitaschwarz.com

How does Wordfence get IPs

- (•) Let Wordfence use the most secure method to get visitor IP addresses. Prevents spoofing and works with most sites. **(Recommended)**
- ( ) Use PHP's built in REMOTE_ADDR and don't use anything else. Very secure if this is compatible with your site.
- ( ) Use the X-Forwarded-For HTTP header. Only use if you have a front-end proxy or spoofing may result.
- ( ) Use the X-Real-IP HTTP header. Only use if you have a front-end proxy or spoofing may result.
- ( ) Use the Cloudflare "CF-Connecting-IP" HTTP header to get a visitor IP. Only use if you're using Cloudflare.

Detected IP(s): **79.117.95.43**
Your IP with this setting: 79.117.95.43
+ Edit trusted proxies

- [ ] Look up visitor IP locations via Wordfence servers
  If this option is disabled, Wordfence can look up countries for visitor IP addresses using a local database, but cannot look up regions or cities
- [ ] Hide WordPress version
- [x] Disable Code Execution for Uploads directory
- [x] Pause live updates when window loses focus

Update interval in seconds: 15
Setting higher will reduce browser traffic but slow scan starts, live traffic & status updates.

- [ ] Bypass the LiteSpeed "noabort" check
- [ ] Delete Wordfence tables and data on deactivation
  Note: This does not include Login Security settings and tables. An option to delete those must be selected separately on the Login Security settings page.

Dashboard Notification Options

- [x] Updates Needed (Plugin, Theme, or Core)
- [x] Scan Status

Dashboard notifications will also be displayed for Security Alerts, Promotions, Blog Highlights, and Product Updates. These notifications can be disabled by upgrading to a premium license.

UPGRADE TO PREMIUM | LEARN MORE

Email Alert Preferences

- [ ] Email me when Wordfence is automatically updated
  If you have automatic updates enabled (see above), you'll get an email when an update occurs.
- [x] Email me if Wordfence is deactivated
- [x] Email me if the Wordfence Web Application Firewall is turned off
- [x] Alert me with scan results of this severity level or greater: High
- [x] Alert when an IP address is blocked
- [x] Alert when someone is locked out from login
- [x] Alert when someone is blocked from logging in for using a password found in a breach
- [x] Alert when the "lost password" form is used for a valid user
- [x] Alert me when someone with administrator access signs in
  - [x] Only alert me when that administrator signs in from a new device
- [x] Alert me when a non-admin user signs in
  - [ ] Only alert me when that user signs in from a new device
- [x] Alert me when there's a large increase in attacks detected on my site

Maximum email alerts to send per hour
0 means unlimited alerts will be sent.
0

Activity Report

- [x] Enable email summary — Once a week

List of directories to exclude from recently modified file list
wp-content/cache
wp-content/wflogs

- [x] Enable activity report widget on the WordPress dashboard

Firewall Options

Basic Firewall Options

Web Application Firewall Status

Learning Mode: When you first install the Wordfence Web Application Firewall, it will be in learning mode. This allows Wordfence to learn about your site so that we can understand how to protect it and how to allow normal visitors through the firewall. We recommend you let Wordfence learn for a week before you enable the firewall. Learn More

Learning Mode

- [x] Automatically enable on 2025-05-22

Protection Level

Extended Protection: All PHP requests will be processed by the firewall prior to running.

If you're moving to a new host or a new installation location, you may need to temporarily disable extended protection to avoid any file not found errors. Use this action to remove the configuration changes that enable extended protection mode or you can remove them manually.

REMOVE EXTENDED PROTECTION

Real-Time IP Blocklist

Premium Feature: This feature blocks all traffic from IPs with a high volume of recent malicious activity using Wordfence's real-time blocklist.

UPGRADE TO PREMIUM LEARN MORE

Advanced Firewall Options

- [ ] Delay IP and Country blocking until after WordPress and plugins have loaded (only process firewall rules early)

Allowlisted IP addresses that bypass all rules

Allowlisted IPs must be separated by commas or placed on separate lines. You can specify ranges using the following formats: 127.0.0.1/24, 127.0.0.[1-100], or 127.0.0.1-127.0.1.100 Wordfence automatically allowlists private networks because these are not routable on the public Internet.

Allowlisted services

- [x] Sucuri
- [x] Facebook
- [x] Uptime Robot
- [x] StatusCake
- [ ] ManageWP
- [x] Seznam Search Engine

Immediately block IPs that access these URLs

Separate multiple URLs with commas or place them on separate lines. Asterisks are wildcards, but use with care. If you see an attacker repeatedly probing your site for a known vulnerability you can use this to immediately block them. All URLs must start with a "/" without quotes and must be relative. e.g. /badURLone/, /bannedPage.html, /dont-access/this/URL/, /starts/with-*

Ignored IP addresses for Wordfence Web Application Firewall alerting

Ignored IPs must be separated by commas or placed on separate lines. These addresses will be ignored from any alerts about increased attacks and can be used to ignore things like standalone website security scanners.

Rules

	Category	Description
ON	whitelist	Whitelisted URL
ON	lfi	Slider Revolution <= 4.1.4 - Directory Traversal
ON	sqli	SQL Injection
ON	xss	XSS: Cross Site Scripting
ON	file_upload	Malicious File Upload
ON	traversal	Directory Traversal
ON	lfi	LFI: Local File Inclusion
ON	xxe	XXE: External Entity Expansion
ON	xss	DZS Video Gallery <= 8.60 - Reflected Cross-Site Scripting

SHOW ALL RULES

MANUALLY REFRESH RULES *Next Update Check: 22.5.2025, 11:18:33*

Brute Force Protection

Enable brute force protection
This option enables all "Brute Force Protection" options, including strong password enforcement and invalid login throttling. You can modify individual options below. OFF ON

Lock out after how many login failures: 5

Lock out after how many forgot password attempts: 3

Count failures over what time period: 4 hours

Amount of time a user is locked out: 12 hours

- [x] Immediately lock out invalid usernames

Immediately block the IP of users who try to sign in as these usernames
Hit enter to add a username

x admin

Prevent the use of passwords leaked in data breaches — For admins only

Additional Options

Enforce strong passwords — Force admins and publishers to use strong passwords (recomm...

Don't let WordPress reveal valid users in login errors

Prevent users registering 'admin' username if it doesn't exist

Prevent discovery of usernames through '/?author=N' scans, the oEmbed API, the WordPress REST API, and WordPress XML Sitemaps

Disable WordPress application passwords

Block IPs who send POST requests with blank User-Agent and Referer
If you use external services that may send POST requests without these headers, do not use this option, as they will be blocked.

Custom text shown on block pages

HTML tags will be stripped prior to output and line breaks will be converted into the appropriate tags.

Check password strength on profile update

Participate in the Real-Time Wordfence Security Network

Rate Limiting

Enable Rate Limiting and Advanced Blocking
NOTE: This checkbox enables ALL blocking/throttling functions including IP, country and advanced blocking, and the "Rate Limiting Rules" below.
OFF ON

How should we treat Google's crawlers — Verified Google crawlers will not be rate-limited

If anyone's requests exceed — 120 per minute — then — throttle it

If a crawler's page views exceed — 120 per minute — then — throttle it

If a crawler's pages not found (404s) exceed — 60 per minute — then — throttle it

If a human's page views exceed — 240 per minute — then — throttle it

If a human's pages not found (404s) exceed — 60 per minute — then — throttle it

How long is an IP address blocked when it breaks a rule — 5 minutes

Allowlisted 404 URLs
These URL patterns will be excluded from the throttling rules used to limit crawlers.

```
/favicon.ico
/apple-touch-icon*.png
/*@2x.png
/browserconfig.xml
```

Allowlisted URLs

Add Allowlisted URL/Param The URL/parameters in this table will not be tested by the firewall. They are typically added while the firewall is in Learning Mode or by an admin who identifies a particular action/request is a false positive.

URL | Param Type: POST Body | Param Name | ADD

DELETE ENABLE DISABLE

Filter By: URL | Filter Value | FILTER

Enabled	URL	Param	Created	Source	User	IP
No allowlisted URLs currently set.						

Monitor background requests from an administrator's web browser for false positives

- [x] Front-end Website
- [x] Admin Panel

Blocking Options

Advanced Country Blocking Options

Put Geographic Protection In Place With Country Blocking

Wordfence country blocking is designed to stop an attack, prevent content theft, or end malicious activity that originates from a geographic region in less than 1/300,000th of a second. Blocking countries who are regularly creating failed logins, a large number of page not found errors, and are clearly engaged in malicious activity is an effective way to protect your site during an attack.

UPGRADE TO PREMIUM

Scan Options

Scan Scheduling

Schedule Wordfence Scans — DISABLED | ENABLED

- (•) Let Wordfence choose when to scan my site (recommended)
- ( ) Manually schedule scans **Premium Feature**

Basic Scan Type Options

Limited Scan	Standard Scan	High Sensitivity	Custom Scan
For entry-level hosting plans. Provides limited detection capability with very low resource utilization.	Our recommendation for all websites. Provides the best detection capability in the industry.	For site owners who think they may have been hacked. More thorough but may produce false positives.	Selected automatically when General Options have been customized for this website.

General Options

- [ ] Check if this website is on a domain blocklist **Premium Feature**
  Reputation check
- [ ] Check if this website is being "Spamvertised" **Premium Feature**
  Reputation check
- [ ] Check if this website IP is generating spam **Premium Feature**
  Reputation check
- [x] Scan for misconfigured How does Wordfence get IPs

- [x] Scan for publicly accessible configuration, backup, or log files
- [x] Scan for publicly accessible quarantined files
- [x] Scan core files against repository versions for changes
- [x] Scan theme files against repository versions for changes
- [x] Scan plugin files against repository versions for changes
- [x] Scan wp-admin and wp-includes for files not bundled with WordPress
- [x] Scan for signatures of known malicious files
- [x] Scan file contents for backdoors, trojans and suspicious code
- [x] Scan file contents for malicious URLs
- [x] Scan posts for known dangerous URLs and suspicious content
- [x] Scan comments for known dangerous URLs and suspicious content
- [x] Scan WordPress core, plugin, and theme options for known dangerous URLs and suspicious content
- [x] Scan for out of date, abandoned, and vulnerable plugins, themes, and WordPress versions
- [x] Scan for suspicious admin users created outside of WordPress
- [x] Check the strength of passwords
- [x] Monitor disk space
- [x] Monitor Web Application Firewall status
- [x] Scan files outside your WordPress installation
- [ ] Scan images, binary, and other files as if they were executable

Performance Options

- [x] Use low resource scanning (reduces server load by lengthening the scan duration)

Limit the number of issues sent in the scan results email
0 or empty means unlimited issues will be sent
1000

Time limit that a scan can run in seconds
0 or empty means the default of 3 hours will be used

How much memory should Wordfence request when scanning
Memory size in megabytes
256

Maximum execution time for each scan stage
0 for default. Must be 8 or greater and 10-20 or higher is recommended for most servers
0

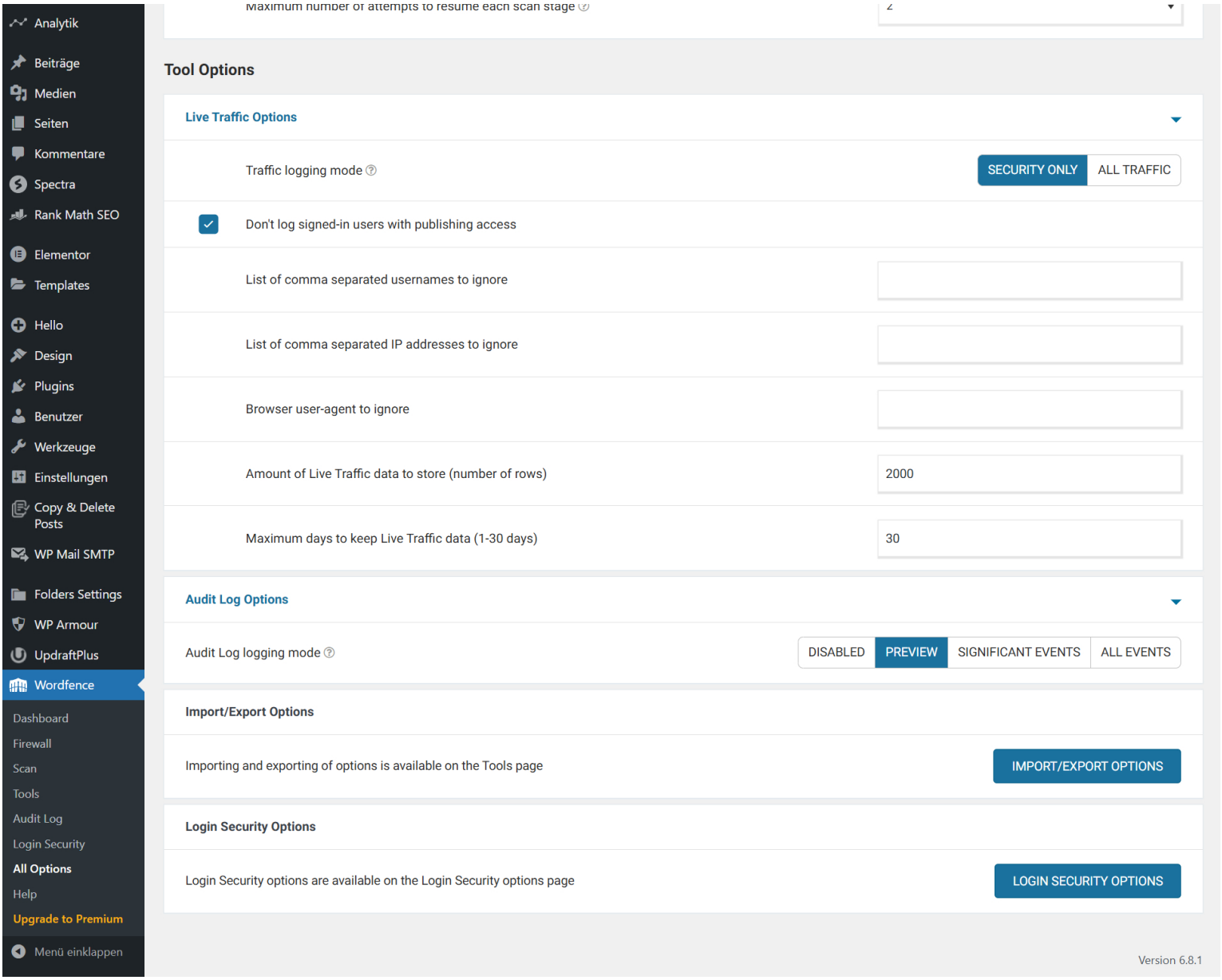
Advanced Scan Options

Exclude files from scan that match these wildcard patterns (one per line)

Additional scan signatures (one per line)

- [ ] Use only IPv4 to start scans
This option requires cURL. (This may have no effect on some old PHP or cURL versions.)

Dashboard


Maximum number of attempts to resume each scan stage
2
Tool Options
Live Traffic Options
Traffic logging mode
SECURITY ONLY
ALL TRAFFIC
Don't log signed-in users with publishing access
List of comma separated usernames to ignore
List of comma separated IP addresses to ignore
Browser user-agent to ignore
Amount of Live Traffic data to store (number of rows)
2000
Maximum days to keep Live Traffic data (1-30 days)
30
Audit Log Options
Audit Log logging mode
DISABLED
PREVIEW
SIGNIFICANT EVENTS
ALL EVENTS
Import/Export Options
Importing and exporting of options is available on the Tools page
IMPORT/EXPORT OPTIONS
Login Security Options
Login Security options are available on the Login Security options page
LOGIN SECURITY OPTIONS
Version 6.8.1
Analytik
Beiträge
Medien
Seiten
Kommentare
Spectra
Rank Math SEO
Elementor
Templates
Hello
Design
Plugins
Benutzer
Werkzeuge
Einstellungen
Copy & Delete Posts
WP Mail SMTP
Folders Settings
WP Armour
UpdraftPlus
Wordfence
Dashboard
Firewall
Scan
Tools
Audit Log
Login Security
All Options
Help
Upgrade to Premium
Menü einklappen