

WordPress Site Security & Backups

Better safe than sorry

WordPress Usage Statistics

- 58% of all websites whose CMS we know
- 27% of all websites are running WordPress
- 22 out of every 100 new domains in the US launches with WordPress
- Projected 300-500 Million WordPress sites by **2025**

What is CMS Security

- CMS security is a multifaceted hardening of your CMS site.
- This means guarding the CMS backend login page to keep crackers and automated cracking bots out.
- It means being able to identify when someone or something is trying to break into your site or compromise your CMS by inserting malicious files, and stopping them by dropping their connection and banning their IP address, essentially blocking them from future malicious intent.

How do the hackers hack WP?

- Hackers upload contaminated files via FTP or other method.
 - To deal with contaminated file, we must first be able to identify the files.
 - Identification requires file scanning and verification processing that can verify the integrity of CMS site files.
 - When contaminated files are found, we have to have clean backup versions so we can revert back to them.
- Cracking of the login username and password.
 - In this case, the rule of right is to strengthen the password.
 - I also recommend that you implement security plugins and change the WordPress login process.
- Malicious access to the core files.
 - Caused by exploiting code vulnerabilities in Themes, Plugins and WP core files.
 - In this case its up to the site admin to keep up on plugin updates and WordPress core updates and implement updates ASAP.

Web Malware Stats

- 403 Million unique variants of malware in 2011 (Symantec)
 - 140% growth since 2010
- 81% increase in malicious web-based attacks between 2010-2011

WordPress – Vulnerable to Link Injection

Link Injection

- Hacker bots look for known exploits (SQL injection, folder permissions, etc.)
 - Exploits (weaknesses) allows them to insert spam files/link into **WordPress Themes, plugins, and core files**

How To Secure WordPress Sites

- Keep your site and systems up to date
 - Keep your Themes up to date
 - Keep your Plugins up to date
 - Keep your WordPress core up to date
- Salt your keys
- Delete any WP Admin Account named “admin”
- Harden file and folder permissions
- Harden passwords – force strong passwords
- Restrict file access
- Limit Admin accounts
- Perform Frequent Backups
- Routinely Scan site for malware

WordPress Security

- Keep your WP sites and all its components up to date
- Use Secret Keys – a secret key is a hashing salt that inserts random elements into your password, making it harder to hack
- Delete the “admin” user account, after you create a new user with Administration privileges.
 - This is an old note. WP has not used the Admin account in a long time. (There used to be a user named “admin” created when you created a WP site)
- Restrict key File and folder permissions
 - Files set to 644
 - Folders set to 755

Keep your WordPress environment updated

- Each time a security issue pops up, a patch is on its way, meaning that keeping a website up and running securely is a continuous commitment. Having all your files updated to their latest available version is an excellent way to increase the security of your WordPress website.
- From WordPress 3.7+, minor and security updates happen automatically in your WordPress installation, while to perform major updates to WordPress core files, plugins and themes you'll need to either perform them via your dashboard or FTP.
- When talking about keeping all your files updated, there's more than just security enhancements like improved performances, bug fixes, better compatibility and new features.

Don't use "Admin" as your administrator username

"Admin" is the most common username for WordPress admin users. Everybody knows this, thus hackers. To make their life a little more complicated, you should prefer any other username over "admin" and pick one with capital letters. Since you already have a WordPress website, you should now:

Move the wp-config.php file

- WordPress (via plugins) has the ability to move the wp-config.php file to one directory above the WordPress root.
- Moving it out of the root folder makes it nearly impossible for anyone (the hackers, crackers, and bots) to access it.

Lock down WP Login and WP Admin

- Add the code below to wp-config.php to force SSL (https) on login
 - Define('FORCE_SSL_LOGIN', true);
- Add code below to wp_config.php to force SSL (https) on all admin pages
 - Define('FORCE_SSL_ADMIN', true);

Lock Down WP Login and WP Admin

- Create an .htaccess file in your wp-admin directory
- Add the following code to it
 - AuthUserFile /dev/null
 - AuthGroupFile /dev/null
 - AuthType Basic
 - order denyAllow
 - deny from all
 - #IP address to Whitelist – may not be relevant
 - #Allow from 67.120.83.59

Keep Your Guard Up At All Times

- Keep your computer up to date
 - If your web host isn't keeping their servers and software up to date, get a better host
- Install Anti-virus on your client computers
- Use a firewall
- Backup your File System and Database (often)
- **Have a disaster recovery plan & Practice using it**
 - Practice your disaster recovery plan until you feel comfortable with it.
 - Consider have periodic drills and **keep the plan current**, upgrading software and processes when necessary

Increase WordPress Login Password Security – Force & Enforce Strong Password

“(ALLOWING) Weak passwords have always made WordPress blogs and websites an easy target for hackers and users will always use easy passwords unless there are policies which they have to adhere to.”

[Robert Abela](#) 2014

WordPress Allows Weak Passwords

- By default WordPress does not have any built in tools that allow you to enforce passwords policies.
- It only has a strength indicator, but that does not stop users from using weak passwords.
- **The best way to ensure all your users uses strong WordPress passwords is by configuring password policies** with a plugin that forces users to adhere a strong password policy.

Pick strong passwords (long, with numbers, capital letters, and symbols)

- Long story short: passwords are vital to your WordPress security. That's why you need to start using passwords that have the following features:
- have no words in it to prevent dictionary attack
- have symbols and numbers in it
- be at least 15 characters long

Password Policy Managers Are not Free

The screenshot shows a web browser window with the URL `wpwhitesecurity.com/wordpress-plugins/password...`. The browser's address bar and bookmarks are visible. The website header includes the WP WhiteSecurity logo and navigation links for Activity Logs, Password Policies Manager, WordPress File Changes Monitor, and a Blog. The main content area features the title "Password Policy Manager for WordPress" and the tagline "STRONG PASSWORDS = MORE SECURE WORDPRESS". A paragraph explains that website security is as strong as the weakest password and that the plugin helps configure policies. Below this are two buttons: "Buy Plugin" and "Watch Video". On the right, there is a graphic showing a login form with fields for "Username or email address" and "Password", a "Remember Me" checkbox, and a "Log In" button. Next to the login form is a password strength indicator showing a green bar and the word "HIGH". Below the login form is a circular icon with a blue padlock, and at the bottom right is the WordPress logo.

wpwhitesecurity.com/wordpress-plugins/password...

WP WhiteSecurity
Developers of high-quality niche
WordPress security and admin plugins.

Activity Logs for WordPress Password Policies Manager WordPress File Changes Monitor Blog

Password Policy Manager for WordPress

STRONG PASSWORDS = MORE SECURE WORDPRESS

The security of your website & WooCommerce store is as strong as the weakest password! Configure policies with the Password Policy Manager to ensure users & customers use strong passwords.

Buy Plugin **Watch Video**

Username or email address
Password
Remember Me Log In
HIGH
WordPress logo

Default WordPress Allows Weak Passwords

Share a little biographical information to fill out your profile. This may be shown publicly.

Profile Picture

Account Management

New Password

xxx

Hide Cancel

Very weak

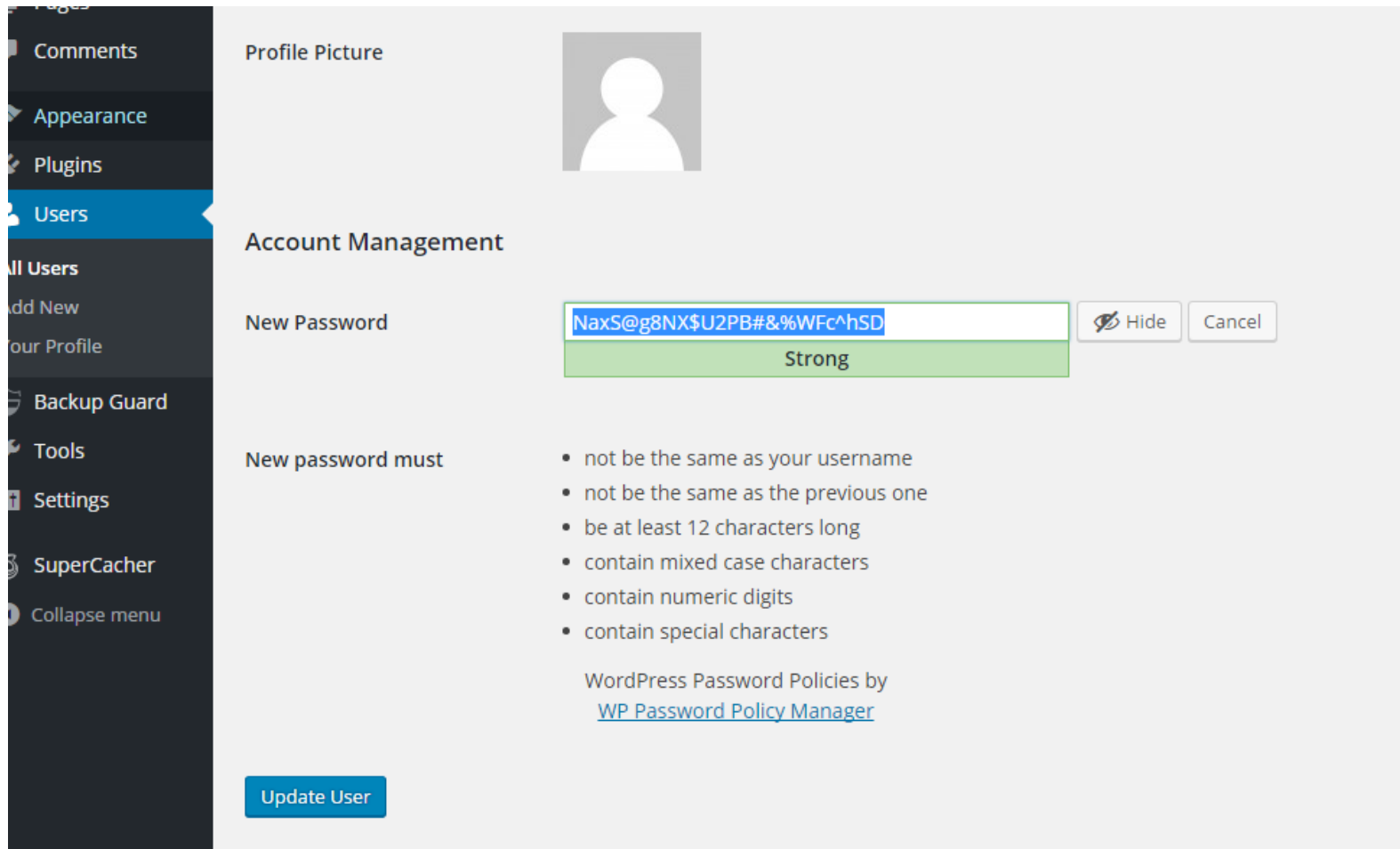
Confirm Password

☐ Confirm use of weak password

This allows users to add

Update User

WordPress with a Password Policy Manager Prevents Weak Passwords



The screenshot shows the WordPress admin interface. On the left is a dark sidebar menu with options: Pages, Comments, Appearance, Plugins, Users (highlighted), All Users, Add New, Your Profile, Backup Guard, Tools, Settings, SuperCacher, and Collapse menu. The main content area is titled 'Profile Picture' and 'Account Management'. Under 'Account Management', there is a 'New Password' section with a text input field containing 'NaxS@g8NX\$U2PB#&%WfC^hSD'. Below the input field is a green bar with the word 'Strong'. To the right of the input field are 'Hide' and 'Cancel' buttons. Below the 'New Password' section is a 'New password must' section with a bulleted list of requirements: not be the same as your username, not be the same as the previous one, be at least 12 characters long, contain mixed case characters, contain numeric digits, and contain special characters. At the bottom of the 'New password must' section is a link: 'WordPress Password Policies by WP Password Policy Manager'. At the bottom left of the main content area is a blue 'Update User' button.

Profile Picture

Account Management

New Password

NaxS@g8NX\$U2PB#&%WfC^hSD

Hide Cancel

Strong

New password must

- not be the same as your username
- not be the same as the previous one
- be at least 12 characters long
- contain mixed case characters
- contain numeric digits
- contain special characters

WordPress Password Policies by [WP Password Policy Manager](#)

Update User

The better Login policy managers allow you to configure the password – How many character, must contain # of digits or special characters.

WordPress Password Policy Manager Settings

Password Expiration Policy

Examples: 5 days 20 days 6 hours 3 weeks

Leave blank to disable Password Expiry policy.

Password Length Policy

 characters

Leave blank to disable Password Length policy.

Mixed Case Policy

☒ Password must contain a mix of uppercase and lowercase characters.

Numeric Digits Policy

☒ Password must contain numeric digits (0-9).

☐

Special Characters Policy

☒ Password must contain special characters (eg: . , ! # \$ _ +).

Current Password Policy

☐ When changing password on the profile page, the user must supply the current password.

Password History Policy

Remember old passwords

Leave blank to disable password history policy.

Users and Roles Exempt From Policies

Users and Roles in this list are free of all Password Policies.

Reset All Users' Passwords

Use WP Cron

☐

Only check this option if your site has many users.

WP Security Plugin List

- WordFence Login Security
- WordFence Security – Firewall & Malware Scan
- All In One WP Security and Firewall
- Sucuri Security – Auditing, Malware, Scanner and Security Hardening
- BullitProof Security
- Login Security Recaptcha
- Defender WordPress Security, Malware Detection and Firewall
- iThemes Security (formerly Better WP Security)

Types of Security

- Password Requirements - Manage and configure Password Requirements for users.
- **Two Factor Authentication (2FA)**
- 404 Detection - Automatically block users snooping around for pages to exploit.
- Banned Users - Block specific IP addresses and user agents from accessing the site
- File Change Detection - Monitor the site for unexpected file changes.
- Local Brute Force Protection - Protect your site against attackers that try to randomly guess login details to your site.
- Scan for Malware

Two-Factor Authentication Plugins

- Two-Factor Authentication, (aka Two-Step Verification, 2FA) is an additional layer of security you can add to your WordPress login page.
- With 2FA it is virtually impossible for attackers to login to your WordPress, even if they guess your user's password.
- Two-factor authentication is also good to help mitigate WordPress brute force attacks.

Two Factor Authentication Plugins

Purpose - Secure WordPress login with Two Factor Authentication - supports WP, Woo + other login forms, HOTP, TOTP (Google Authenticator, Authy, etc.)

Two Factor Authentication

Google Authenticator

WordFence Login Security

Two Factor Authentication Plugin



Two Factor Authentication

[Install Now](#)[More Details](#)

Secure WordPress login with Two Factor Authentication - supports WP, Woo + other login forms, HOTP, TOTP (Google Authenticator, Authy, etc.)

*By David Nutbourne + David Anderson,
original plugin by Oskar Hane*

★★★★☆ (59)

1,000+ Active Installations

Last Updated: 2 months ago

✓ Compatible with your version of WordPress

Google Authenticator



Google Authenticator – WordPress Two Factor Authentication (2FA)

[Install Now](#)

[More Details](#)

Simple & Easy 2FA setup with any App supporting TOTP algorithm like Google, Authy, LastPass Authenticator & other 2FA methods.

By *miniOrange*

★★★★★ (194)


20,000+ Active Installations

Last Updated: 4 days ago

✓ **Compatible** with your version of WordPress

WordFence Login Security – Offers 2FA

72 items « < 1 of 2 > »



Wordfence
LOGIN SECURITY

Wordfence Login Security

Secure your website with Wordfence Login Security, providing two-factor authentication, login and registration CAPTCHA, and XML-RPC protection.

By Wordfence

Active

[More Details](#)

★★★★★ (2)

8,000+ Active Installations

Last Updated: 2 months ago

✓ Compatible with your version of WordPress

WordFence Login Security – 2FA

Easy to setup and configure

The screenshot shows the WordPress dashboard with the WordFence Login Security plugin installed. A blue notification banner at the top states: "Wordfence Login Security Installed". Below this, a message explains that the plugin contains a subset of the full Wordfence plugin's functionality, including Two-factor Authentication, XML-RPC Protection, and Login Page CAPTCHA. It also mentions that the full Wordfence plugin includes more features like a WordPress firewall and a security scanner, which can be upgraded via a Premium license key.

The interface has a sidebar on the left with the following menu items: Dashboard, Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, All-in-One WP Migration, Settings, Login Security (highlighted), and Collapse menu.

The main content area is titled "Wordfence Login Security Installed" and contains a "Two-Factor Authentication" tab and a "Settings" tab. The "Settings" tab is active, showing the "Login Security Settings" page. A link "Learn more about Login Security" is visible in the top right corner of the settings area.

The "User Summary" section displays a table with the following data:

Role	Total Users	2FA Active
Administrator	2	1
Total	2	1

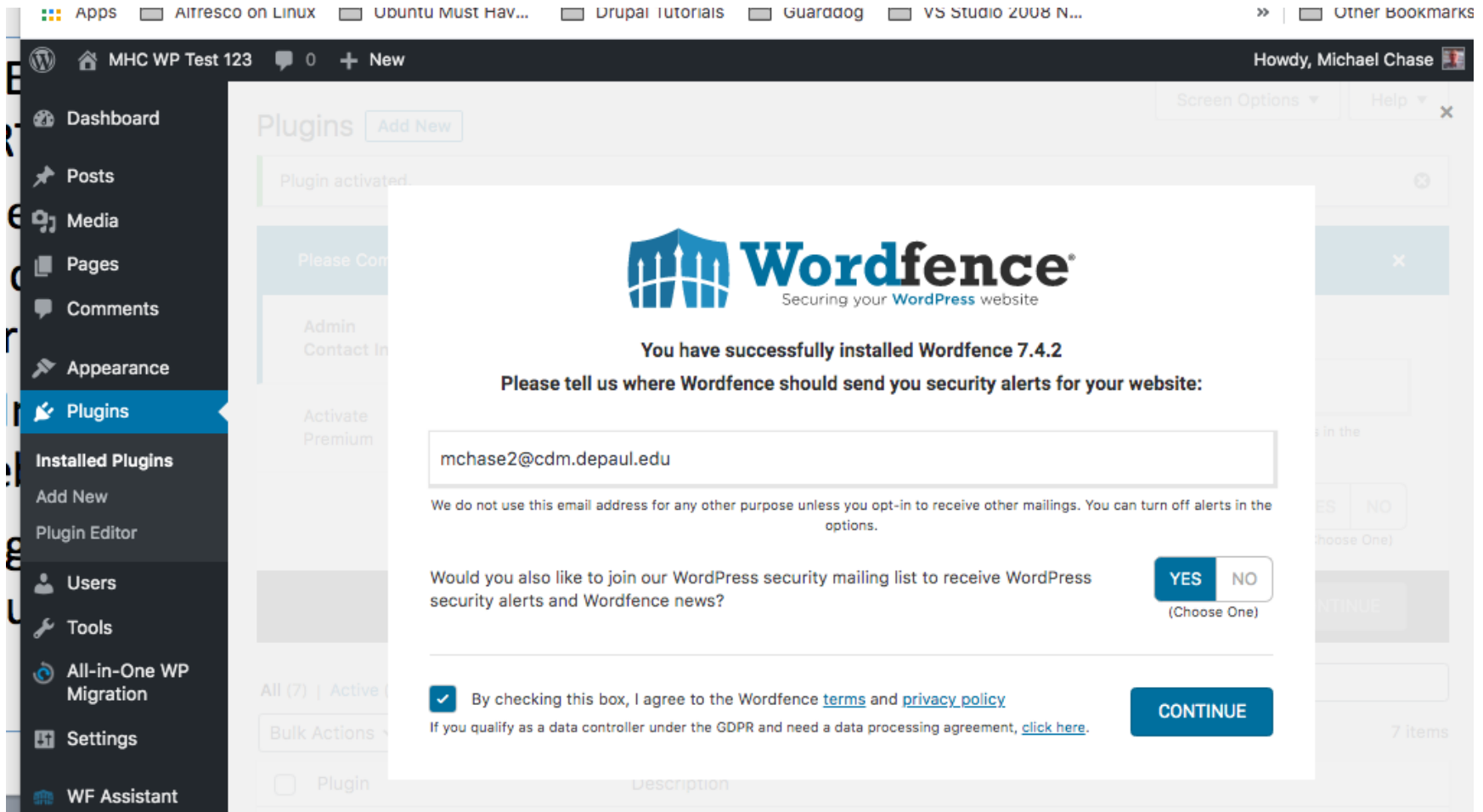
A "Manage Users" link is located in the top right corner of the "User Summary" section.

The "Settings" section includes a "CANCEL" button and a "SAVE" button. Below the buttons, the "Enable 2FA for these roles" section shows checkboxes for the following roles: Administrator (checked), Editor, Author, Contributor, and Subscriber.

All-in-one WP Security Plugin

- COMPREHENSIVE, EASY TO USE, STABLE AND WELL SUPPORTED WORDPRESS SECURITY PLUGIN
- WordPress itself is a very secure platform. This plugin adds extra security and firewall to your site by enforcing good security practices.
- The All In One WordPress Security plugin will take your website security to a whole new level.
- This plugin is designed and written by experts and is easy to use and understand.

Register the Website and Get Notified of Security Issues



All-in-one WP Security Plugin

- It reduces security risk by **checking for vulnerabilities**, and by **implementing and enforcing the latest recommended WordPress security practices and techniques**.
- All In One WP Security also uses an unprecedented security points grading system to measure how well you are protecting your site based on the security features you have activated.
- **The All In One WordPress Security plugin **doesn't slow down your site** and it is 100% free.**

All-in-one WP Security Dashboard

To make your site as secure as possible, take a moment to optimize the Wordfence Web Application Firewall:

[CLICK HERE TO CONFIGURE](#)

[DISMISS](#)

If you cannot complete the setup process, [click here for help](#).

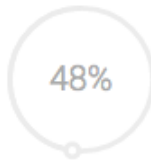
Do you want Wordfence to stay up-to-date automatically? [Yes, enable auto-update.](#) | [No thanks.](#)



Wordfence Dashboard

[Learn more about the Dashboard](#)

Wordfence Protection Activated



Firewall

WAF Currently in Learning Mode

[Manage Firewall](#)



Scan

Detection of security issues

[Manage Scan](#)

Premium Protection Disabled

As a free Wordfence user, you are currently using the Community version of the Threat Defense Feed. Premium users are protected by an additional 1 firewall rules and malware signatures. Upgrade to Premium today to improve your protection.

[UPGRADE TO PREMIUM](#)

[LEARN MORE](#)

Notifications

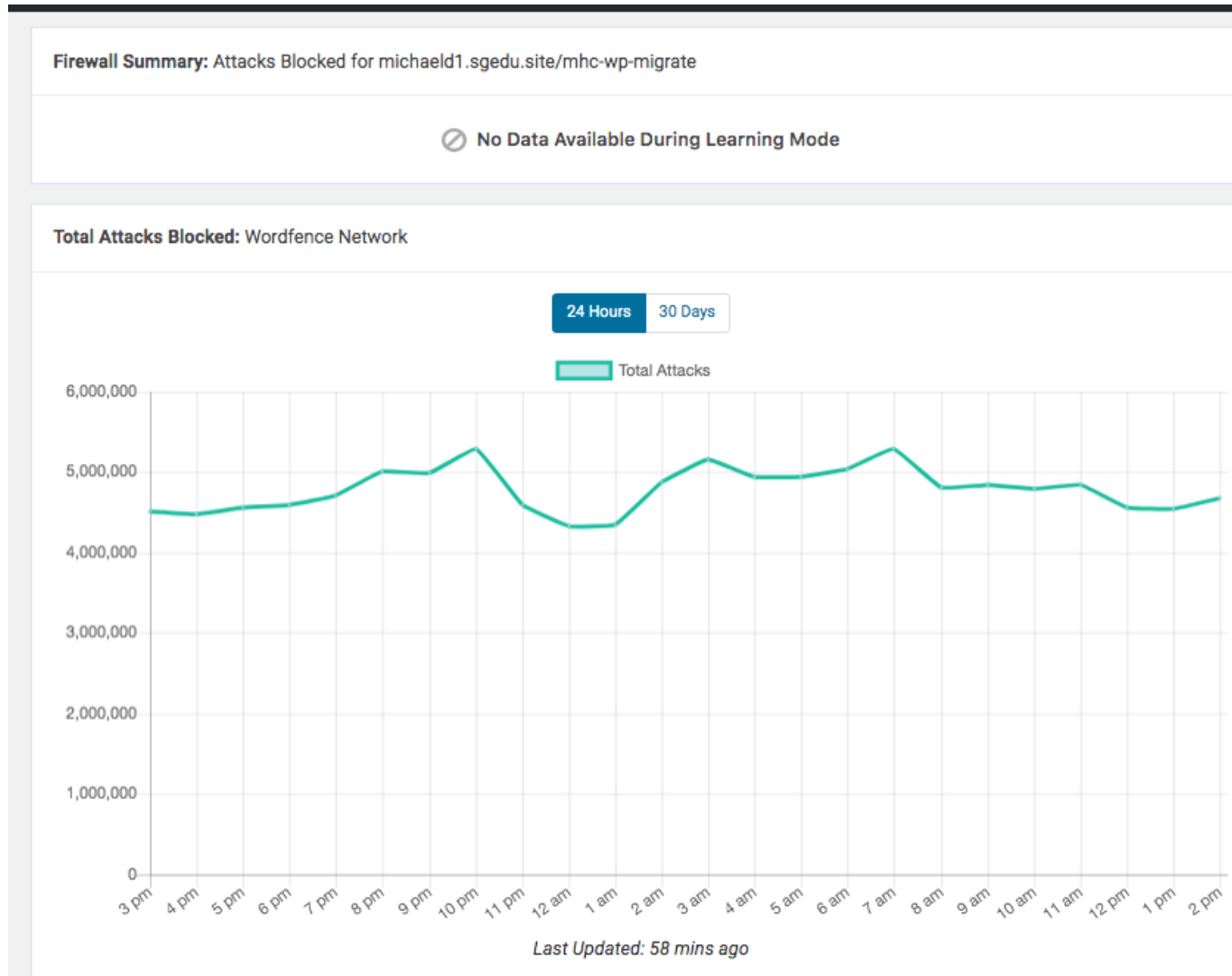
No notifications received



Wordfence Central Status

Wordfence Central allows you to manage Wordfence on multiple sites from one location. It makes security monitoring and configuring Wordfence easier.

More WordFence Dashboard



IP Geo Block with Zero Day Exploit Protection

- There are some cases of a site being infected.
 - The first one is the case that contaminated files are uploaded via FTP or some kind of up-loaders. In this case, scanning and verifying integrity of files in your site is useful to detect the infection.
 - The second one is cracking of the login username and password. In this case, the rule of right is to strengthen the password.
 - The third one is caused by malicious access to the core files.
 - The major issue in this case is that a plugin or theme in your site can potentially has some vulnerability such as XSS, CSRF, SQLi, LFI and so on.
 - For example, if a plugin has vulnerability of Local File Inclusion (LFI), the attackers can easily download the wp-config.php without knowing the username and password by simply hitting wp-admin/admin-ajax.php?action=show&file=../wp-config.php on their browser.
- For these cases, the protection based on the **IP address is not a perfect solution for everyone.**
- But for some site owners or some certain cases such as 'zero-day attack', combination with WP-ZEP can still reduce the risk of infection against the specific attacks.
- That's why this plugin is here.

Like most advanced options, Country blocking is not free with WordFence

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.



IP Geo Block Dashboard

The screenshot shows the IP Geo Block dashboard within a WordPress environment. The top navigation bar includes the WordPress logo, site name 'My WordPress Demo Site 1', a comment count of 0, a 'New' button, and a 'Purge SG Cache' button. The left sidebar contains a menu with icons and labels for Dashboard, Jetpack, Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, Settings (highlighted in blue), General, Writing, Reading, Discussion, Media, Permalinks, CodePeople Post Map, IP Geo Block, SuperCacher, and Collapse menu. The main content area is titled 'IP Geo Block' and features a green success message: 'IP Geo Block: Downloading geolocation databases was successfully done.' Below this is a tabbed interface with 'Settings', 'Statistics', 'Logs', 'Search', and 'Attribution' tabs. The 'Settings' tab is active, showing a section titled 'Validation rule settings'. This section contains several configuration options: 'Your IP address / Country' (69.243.146.71 / US (Cache) with a 'Scan your country code' button), 'Matching rule' (a dropdown menu set to 'White list'), 'Country code for matching rule (ISO 3166-1 alpha-2)' (a text input field containing 'US' with '(comma separated)' text), 'White list of extra IP addresses prior to country code (CIDR)' (an empty text input field with '(comma separated)' text), 'Black list of extra IP addresses prior to country code (CIDR)' (an empty text input field with '(comma separated)' text), '\$_SERVER keys to retrieve extra IP addresses' (an empty text input field with '(comma separated)' text), 'Response code (RFC 2616)' (a dropdown menu set to '403 Forbidden'), and 'Max number of failed login attempts per IP address' (a spinner control set to '5').

My WordPress Demo Site 1 0 + New Purge SG Cache

IP Geo Block

IP Geo Block: Downloading geolocation databases was successfully done.

Settings Statistics Logs Search Attribution

Validation rule settings

Your IP address / Country 69.243.146.71 / US (Cache)

Matching rule White list ▾

Country code for matching rule (ISO 3166-1 alpha-2) (comma separated)

White list of extra IP addresses prior to country code (CIDR) (comma separated)

Black list of extra IP addresses prior to country code (CIDR) (comma separated)

\$_SERVER keys to retrieve extra IP addresses (comma separated)

Response code (RFC 2616) 403 Forbidden ▾

Max number of failed login attempts per IP address 5 ▾

Country Codes – For Blocking Countries

	Not used: not used in ISO 3166-1 in deference to intergovernmental intellectual property organisation names.
	Unassigned: free for assignment by the ISO 3166/MA only.

Officially assigned code elements [\[edit \]](#)

The following is a complete list of the 249 current officially assigned ISO 3166-1 alpha-2 codes, with the following columns:

- **Code** — ISO 3166-1 alpha-2 code
- **Country name** — English short country name officially used by the ISO 3166 Maintenance Agency (ISO 3166/MA)^[15]
- **Year** — Year when alpha-2 code was first officially assigned (1974, first edition of ISO 3166)
- **ccTLD** — Corresponding [country code top-level domain](#) (note that some are inactive); exceptions where another ccTLD is assigned for the country are shown in parentheses
- **ISO 3166-2** — Corresponding [ISO 3166-2](#) codes
- **Notes** — Any unofficial notes

Code ↕	Country name ↕	Year ↕	ccTLD ↕	ISO 3166-2 ↕	Notes
AD	Andorra	1974	.ad	ISO 3166-2:AD	
AE	United Arab Emirates	1974	.ae	ISO 3166-2:AE	
AF	Afghanistan	1974	.af	ISO 3166-2:AF	
AG	Antigua and Barbuda	1974	.ag	ISO 3166-2:AG	
AI	Anguilla	1983	.ai	ISO 3166-2:AI	AI previously represented French Afar and Issas
AL	Albania	1974	.al	ISO 3166-2:AL	
AM	Armenia	1992	.am	ISO 3166-2:AM	
AO	Angola	1974	.ao	ISO 3166-2:AO	
AQ	Antarctica	1974	.aq	ISO 3166-2:AQ	Covers the territories south of 60° south latitude Code taken from name in French : <i>Antarctique</i>
AR	Argentina	1974	.ar	ISO 3166-2:AR	
AS	American Samoa	1974	.as	ISO 3166-2:AS	
AT	Austria	1974	.at	ISO 3166-2:AT	
AU	Australia	1974	.au	ISO 3166-2:AU	Includes the Ashmore and Cartier Islands and the Coral Sea Islands
AW	Aruba	1986	.aw	ISO 3166-2:AW	

Additional Web Resources

- **Security Related Articles**

- http://codex.wordpress.org/Hardening_WordPress
- <http://blog.sucuri.net/2012/04/lockdown-wordpress-a-security-webinar-with-dre-armeda.html>
- <http://blog.sucuri.net/2012/04/ask-sucuri-how-to-stop-the-hacker-and-ensure-your-site-is-locked.html>
- <http://blog.sucuri.net/2012/04/ask-sucuri-what-should-i-know-when-engaging-a-web-malware-company.html>

- **Clean a Hacked Site**

- http://codex.wordpress.org/FAQ_My_site_was_hacked
- <http://www.marketingtechblog.com/wordpress-hacked/>

- **Support Forums**

- Hacked: <http://wordpress.org/tags/hacked>
- Malware: <http://wordpress.org/tags/malware>

Wordfence & Wordfence Assistant

The screenshot shows the WordPress dashboard for a site named 'My WP Backup Test Site'. The user is logged in as 'mchase'. The 'Add Plugins' section is active, displaying search results for 'WordFence'. The left sidebar shows the 'Plugins' menu item is selected. Two plugins are featured:

- Wordfence Security**: A security plugin with a blue logo. It is described as providing free enterprise-class WordPress security. It has a 5-star rating from 2,707 reviews, over 1 million active installs, and was last updated 2 days ago. It is compatible with the user's version of WordPress.
- Wordfence Assistant**: A plugin with a brown geometric logo. It provides data management utilities for Wordfence users. It is developed by Mark Maunder, has a 4.5-star rating from 3 reviews, over 3,000 active installs, and was last updated 2 days ago. It is also compatible with the user's version of WordPress.

Wordfence – Free version is limited

- Its worth installing just for the security scan
- Its complicated to learn and use
- Be patient and take your time and always install the additional assistant plugin – so you can get in if and when you lock yourself out of the site

Wordfence Assistant

Why does this additional plugin exist?

- In rare cases, Wordfence users can accidentally lock themselves out of their system.
- Wordfence provides a built-in user-friendly system to regain access to your website which allows site administrators to send themselves an unlock email which contains a link that unlocks their website.
- Because Wordfence has become so popular, we see edge cases where systems administrators no longer have access to their old email address or the email unlock does not work for another reason.
- To help unlock sites with that problem, we've provided this plugin which you can install after you've removed Wordfence from your system.
- You can use this plugin to modify the Wordfence data in your database and disable the Wordfence firewall so that if you reinstall Wordfence the firewall won't lock you out again.
- You can also use this plugin to delete all Wordfence data.

WordFence Scan

To make your site as secure as possible, take a moment to optimize the Wordfence web Application Firewall:

[Click here to configure.](#)

[Dismiss](#)

If you cannot complete the setup process, [click here for help](#).



Wordfence Scan

You have not set an administrator email address to receive alerts for Wordfence. Please [click here to go to the Wordfence Options Page](#) and set an email address where you will receive security alerts from this site.

[Use My Email Address](#)

[Dismiss](#)

[Learn more about scanning](#)

[Start a Wordfence Scan](#)

[Click to kill the current scan.](#)

[Read our scanning documentation](#). You can also [start the tour again](#), [subscribe to get WordPress Security Alerts and Product News](#) or [visit our support website help](#). Love Wordfence? You can help by doing two simple things: [Go to WordPress.org now and give this plugin a 5★ rating](#). Blog about Wordfence and link to the [plugin page](#) or [www.wordfence.com](#). Spreading the word helps us keep the best features free.

Scan Summary



[Jun 22 23:02:21] Scanning comments for URL's in Google's Safe Browsing List	Secure.
[Jun 22 23:02:21] Scanning for weak passwords	Secure.
[Jun 22 23:02:21] Scanning DNS for unauthorized changes	Secure.
[Jun 22 23:02:21] Scanning to check available disk space	Secure.
[Jun 22 23:02:21] Scanning for old themes, plugins and core files	Problems found.
[Jun 22 23:02:22] Scanning for admin users not created through WordPress	Secure.
[Jun 22 23:02:22] Scan complete. You have 15 new issues to fix. See below.	Scan Complete.

You are running the Wordfence Community Scan signatures

WordFence – Issue alters

you have fixed all the issues below, you can [click here to mark all new issues as fixed](#). You can also [ignore all new issues](#) which will exclude all issues listed below from future scans.

[Bulk operation»»](#)

SEVERITY	ISSUE
	<p>Your WordPress version is out of date</p> <p>Current WordPress Version: 4.5.2 New WordPress Version: 4.5.3 Severity: Critical Status: New</p> <p>WordPress version 4.5.3 is now available. Please upgrade immediately to get the latest security updates from WordPress. Click here to update now.</p> <hr/> <p>Resolve: I have fixed this issue Ignore this issue</p>
	<p>The Plugin "Akismet" needs an upgrade.</p> <p>Plugin Name: Akismet Plugin Website: http://akismet.com/ Current Plugin Version: 3.1.10 New Plugin Version: 3.1.11 Severity: Critical</p>

Spam Honey Pot

Add Plugins [Upload Plugin](#)


You have not set an administrator email address to receive alerts for Wordfence. Please [click here to go to the Wordfence Options Page](#) and set an email address where you will receive security alerts from this site.

[Use My Email Address](#) [Dismiss](#)

[Search Results](#) [Featured](#) [Popular](#) [Recommended](#) [Favorites](#)

Keyword

109 items [«](#) [<](#) **1** of 4 [>](#) [»](#)



Spam Honey Pot


Adds a hidden text field to the comment form to trap spam bots.

By Matthew Turland

★★★★★ (3)
2,000+ Active Installs

Last Updated: 1 year ago
Untested with your version of WordPress

[Install Now](#) [More Details](#)



PWH Honey Pot


This plugin adds an email honey pot address to catch spammers and email harvesters.

By InfoBahn

☆☆☆☆☆ (0)
100+ Active Installs

Last Updated: 3 months ago
Untested with your version of WordPress

[Install Now](#) [More Details](#)



AVH First Defense Against Spam


The AVH First Defense Against Spam plugin gives you the ability to block spammers before any content is served.

By Peter van der Does

★★★★☆ (14)
10,000+ Active Installs

Last Updated: 1 year ago
Untested with your version of WordPress

[Install Now](#) [More Details](#)



Spam Oborona YandexCleanWeb

The fight against spam in comments by free service Yandex .NET Web

By Djon

★★★★★ (2)
0+ Active Installs

Last Updated: 2 years ago
Untested with your version of WordPress

[Install Now](#) [More Details](#)

SpamPot Plugin

Blocks spam signups by adding an invisible field to your registration and login forms, and switching its id with the real username or email form field.

When spam bots blindly fill the “required” fake field in, WP will redirect them to an error message and not let them register or login.

No 3rd party service, no intrusive captchas.

SpamPot

Add Plugins [Upload Plugin](#)

You have not set an administrator email address to receive alerts for Wordfence. Please [click here to go to the Wordfence Options Page](#) and set an email address where you will receive security alerts from this site.

Use My Email Address

Dismiss

Search Results

Featured

Popular

Recommended

Favorites

Keyword ▾

SpamPot



SpamPot

Installed

Adds a honeypot form field on the registration and login pages to trap spammers.

[More Details](#)

By *Keith Drakard*

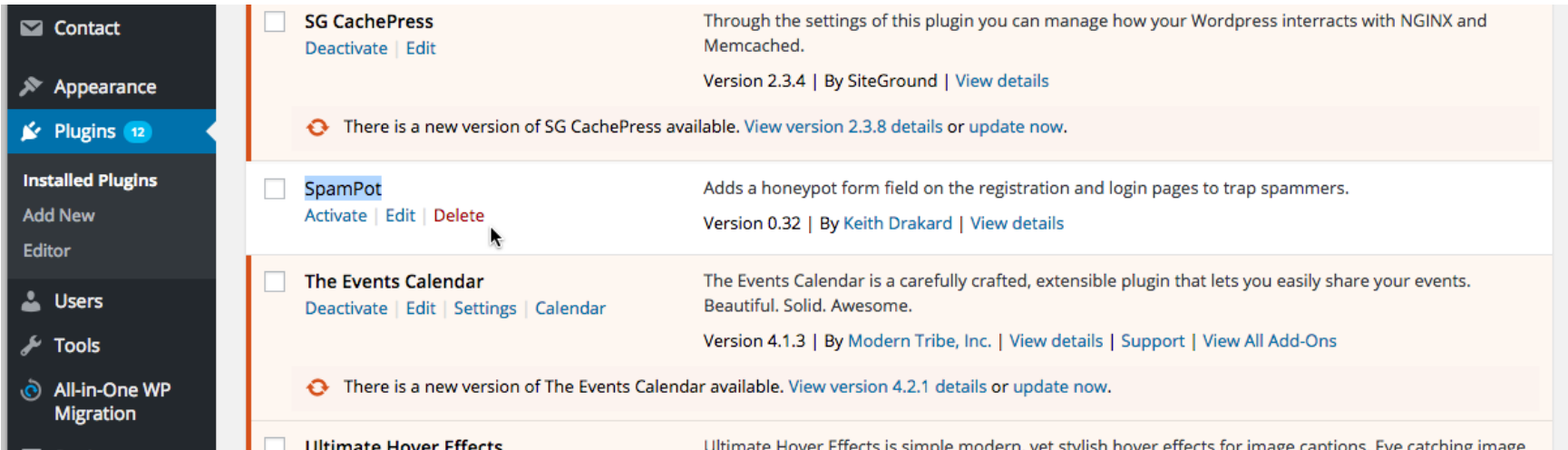
☆☆☆☆☆ (0)

20+ Active Installs

Last Updated: 2 months ago

✓ Compatible with your version of WordPress

SpamPot On WP Site



The screenshot shows the WordPress dashboard's 'Plugins' page. On the left is a dark sidebar with navigation links: 'Contact', 'Appearance', 'Plugins 12' (highlighted in blue), 'Installed Plugins', 'Add New', 'Editor', 'Users', 'Tools', and 'All-in-One WP Migration'. The main content area lists installed plugins. The first plugin is 'SG CachePress', which is active and has a notification for a new version (2.3.8). The second plugin is 'SpamPot', which is also active and highlighted with a blue selection box. It has a description: 'Adds a honeypot form field on the registration and login pages to trap spammers.' and version information: 'Version 0.32 | By Keith Drakard | View details'. The third plugin is 'The Events Calendar', which is active and has a notification for a new version (4.2.1). The fourth plugin is 'Ultimate Hover Effects', which is inactive. Each plugin entry includes checkboxes for activation, and links for 'Deactivate', 'Edit', 'Settings', and 'Calendar' (for The Events Calendar).

Plugin Name	Status	Description	Version	Author	Actions
SG CachePress	Active	Through the settings of this plugin you can manage how your Wordpress interracts with NGINX and Memcached.	2.3.4	By SiteGround	Deactivate Edit View details
There is a new version of SG CachePress available. View version 2.3.8 details or update now .					
SpamPot	Active	Adds a honeypot form field on the registration and login pages to trap spammers.	0.32	By Keith Drakard	Deactivate Edit Delete View details
The Events Calendar	Active	The Events Calendar is a carefully crafted, extensible plugin that lets you easily share your events. Beautiful. Solid. Awesome.	4.1.3	By Modern Tribe, Inc.	Deactivate Edit Settings Calendar View details Support View All Add-Ons
There is a new version of The Events Calendar available. View version 4.2.1 details or update now .					
Ultimate Hover Effects	Inactive	Ultimate Hover Effects is simple modern, vet stvlsh hover effects for image captions. Eve catching image			

WordPress Site Backups

- Its important to make and store site backups during site development
- It's embarrassing to kill your site the day before its due, while **adding that last plugin**, and not having a way to recover a working version.
- WordPress offers many different plugins for site backups and disaster recovery
- Your web host also offers a backup and restore service (usually its an extra cost)

About Plugin Backups

- Backup and restore plugins that run from **within** the WordPress admin dashboard are not the best solution
 - If you kill your site and can not login, so what if you have a backup, you can not login to restore the site
 - You will end up deleting the site, re-creating it, installing the backup plugin, and then use the last backup to restore the site. This takes a lot of time and energy

Additional Plugin Backup Issues

- Most free backup plugins only backup to the Web Host server.
- All our Service learning sites are on a shared web host. If you use one of these backup plugins, you will use up our **free** space and **shut us down**.
- If you use a backup plugin, use one like ALL IN ONE MIGRATION, which copies the backup to your desktop computer, not the Web Host server file system.

WordPress Backup Plugins

- **UpdraftPlus Backup and Restoration**
 - **WP-DB-Backup**
 - **Duplicator**
 - **BackUpWordPress**
 - **WordPress Backup to Dropbox**
 - **All In One Migration**
-
- Do not use Revisor – communication with GIT shuts our SiteGround down

UpdraftPlus Backup and Restoration

- UpdraftPlus Backup and Restoration is one of the most popular free backup plugins available for WordPress.
 - With more than half a million installs and an extraordinarily favorable 4.9 (out of a possible five) star rating, it should definitely make your shortlist.
- You can use Updraft to back up your files to the cloud via Amazon S3, as well as other popular online file storage solutions including Google Drive, Dropbox, Rackspace Cloud.
 - You can also backup your files to the server of your choice with an FTP transfer. (DO NOT BACKUP TO SITEGROUND, please)
- UpdraftPlus is also offered as a premium version.
 - Premium gives you a gigabyte of backup storage on the
 - Updraft Vault, additional backup options (including Microsoft OneDrive, SCP, WebDAV, and OpenStack Swift), secure FTP, the ability to clone databases, automatic backup when updating WordPress themes, and the ability to send backups to remote destinations.
 - The premium version costs between \$70 and \$145, depending on the number of sites.

WP-DB-Backup

Database only backup, not Files

- Very little is written about WP-DB-Backup on its plugin page. However, its lack of a thorough marketing message apparently hasn't diminished its popularity.
 - The plugin has been downloaded more than half a million times and enjoys a 4.6 star rating.
- WP-DB-Backup, as the name implies, **backs up your database, not your files**. If you want your files backed up as well, you'll need to look for an alternative solution.

Duplicator

- Duplicator is a backup solution that not only backs up your data, but also duplicates your entire WordPress site.
- This is a powerful backup solution. Maybe that's why the plugin has been installed more than half a million times and currently enjoys a 4.9 star rating.
- This plugin gives you the opportunity to migrate, copy, or clone your entire site from one location to another, which is a great solution if you're looking for complete redundancy in the event that you need a failover option if your primary site goes down.
- **Just make sure you do not store the backup file on the SiteGround server.**

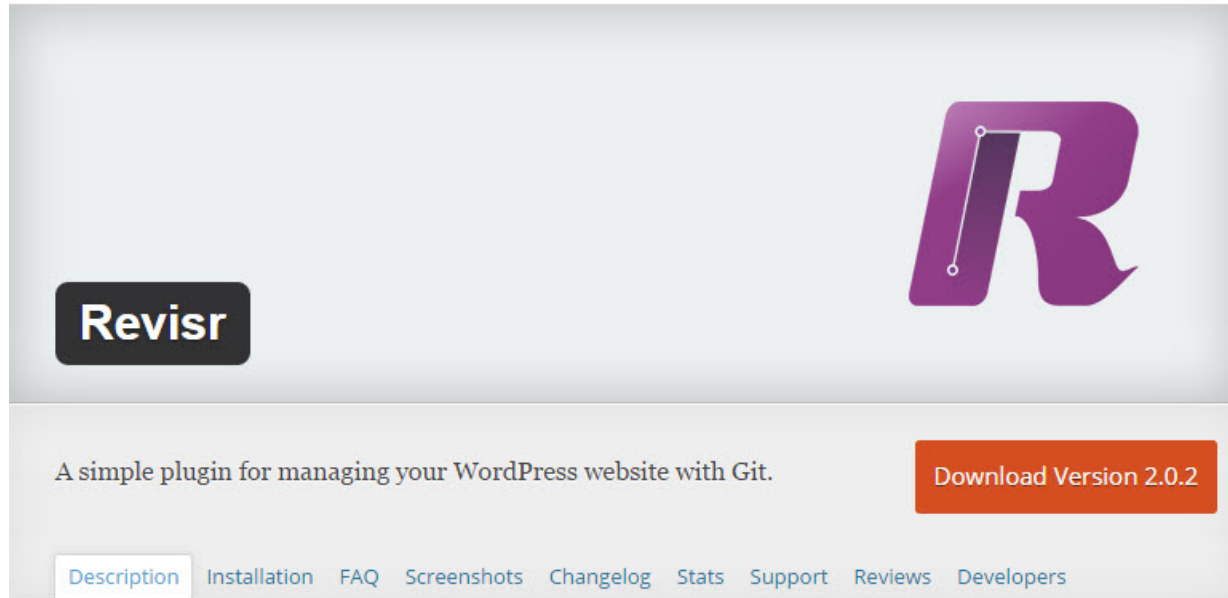
BackUpWordPress

- The appropriately named BackUpWordPress is another excellent option if you're looking for a free WordPress backup system.
 - It's been installed more than 200,000 times, and enjoys a 4.7 (out of a possible 5) star rating.
- This plugin requires PHP version 5.3.2 or later.
 - It's not too likely that your WordPress installation is using an old version of PHP, but you'll want to ensure that your version is compliant with this plugin before you install it.
- BackUpWordPress **will back up your entire site, including your files and your database, at a schedule that suits your needs.**
 - It requires no setup and works on low memory
 - **This is an excellent advantage if you're operating on a shared host environment.**
- The plugin also gives you the option to use zip and mysqldump for faster backups. That can be a significant benefit if time is of the essence.
- The plugin offers numerous extensions for various cloud storage services, such as **Dropbox and Google Drive.**
 - **You can also purchase a bundle option that will enable you to back up your files to multiple locations. This additional option is highly recommended.**

WordPress Backup to Dropbox

- You won't be surprised to learn that WordPress Backup to Dropbox is a backup solution that works with Dropbox.
- It's also a popular solution with more than 100,000 installations.
- With this backup, you'll obviously need a Dropbox account for your backup.
 - That will cost money if your backup is more than 2Gb. Setup is easy – you just authorize the plugin with Dropbox. Once that's completed, your backups are fully automated.
- This plugin requires PHP version 5.2.16 or higher with cURL support. Check with your host administrators to check you have the required versions installed.
- The tool also claims to have premium options available for people who need additional functionality, and also offers support for multiple languages.

DO NOT USE – Revisor for any DePaul Web Hosted WP Sites



Revisor allows you to manage your WordPress website with a Git repository. With Revisor, you can:

- Track changes to your entire WordPress installation, or just the parts that you prefer
- Commit changes from within the WordPress dashboard
- Backup or restore your entire website in seconds
- Set up daily or weekly automatic backups
- Optionally push or pull changes to a remote repository, like Bitbucket or Github
- Test changes out before deploying them to another server
- Revert your website files and/or database to an earlier version
- Quickly discard any unwanted changes

Requires: 3.9.2 or higher
Compatible up to: 4.4.4
Last Updated: 7 months ago
Active Installs: 2,000+

Ratings



Revisor works with GIT. Using this plugin will shut us down on SiteGround. It uses a tremendous amount of communication between the website and GIT and uses up our bandwidth allocation and SiteGround turns us off.

Do Use – All In One Migration for WP Site Backups (covered in Migration Lecture)

 **WORDPRESS.ORG**

Search WordPress.org 

Showcase Themes **Plugins** Mobile Support Get Involved About Blog Hosting

Download WordPress

Plugin Directory

Username Password Log in (forgot?) or Register

Featured
Popular
Favorites
Beta Testing

Developers

Search Plugins

Search

Popular Tags
widget (5,926)
Post (3,671)
plugin (3,617)
admin (3,136)
posts (2,807)
shortcode (2,399)
sidebar (2,226)
google (2,104)
twitter (2,052)



The Complete Wordpress Migration

Focus on creating engaging websites.
We take care of moving your website to any server.

All-in-One WP Migration

All-in-One WP Migration is the only tool that you will ever need to migrate a WordPress site.

Download Version 5.43

Description Installation Screenshots Changelog Stats Support Reviews Developers

The plugin allows you to export your database, media files, plugins, and themes. You can apply unlimited find/replace operations on your database and the plugin will also fix any serialization problems that occur during find/replace operations.

All in One WP Plugin is the first plugin to offer true mobile experience on WordPress versions 3.3 and up.

Requires: 3.3 or higher
Compatible up to: 4.5.3
Last Updated: 1 week ago
Active Installs: 200,000+

Ratings

GitHub

- Consider backing up and providing versioning of your WordPress site by establishing a GitHub repository
- Setting up the repo is complex, and you must take extra steps to secure the WP database and configuration settings