WordPress Security Plugins & Settings

You do realize there's a huge target on WordPress, yes?

R. Scott Granneman & Jans Carton

© 2022 R. Scott Granneman
Last updated 2022-09-14
You are free to use this work, with certain restrictions: CC BY-SA 4.0
For full licensing information, please see the last slide/page.

1.0

Plugins

Kismet

You need Akismet if you’re going to allow comments on your WordPress site

…but allowing comments is a really bad idea, so don’t do it

Akismet Spam Protection

By Automattic

Download

Details | Reviews | Installation | Support | Development

Description

Akismet checks your comments and contact form submissions against our global database of spam to prevent your site from publishing malicious content. You can review the comment spam it catches on your blog's "Comments" admin screen.

Major features in Akismet include:

- Automatically checks all comments and filters out the ones that look like spam.
- Each comment has a status history, so you can easily see which comments were caught or cleared by Akismet and which were spammed

Version:	5.0
Last updated:	2 months ago
Active installations:	5+ million
WordPress Version:	5.0 or higher
Tested up to:	6.0.2
Languages:	See all 73
Tags:	anti-spam, antispam, comments, contact form

Akismet Spam Protection

By Automattic

Download

Details | Reviews | Installation | Support | Development

Description

Akismet checks your comments and contact form submissions against our global database of spam to prevent your site from publishing malicious content. You can review the comment spam it catches on your blog's "Comments" admin screen.

Major features in Akismet include:

- Automatically checks all comments and filters out the ones that look like spam.
- Each comment has a status history, so you can easily see which comments were caught or cleared by Akismet and which were spammed

Version:	5.0
Last updated:	2 months ago
Active installations:	5+ million
WordPress Version:	5.0 or higher
Tested up to:	6.0.2
Languages:	See all 73
Tags:	anti-spam, antispam, comments, contact form

535,989,355,429

Spam comments blocked to date

Slaying spam since 2005

To date, we have kept **535,989,525,731** pieces of spam off the web, averaging about **7,500,000** per hour. That means we're stopping almost twice as much spam as there are people in Los Angeles every single hour.

For personal use

Personal

Spam protection for your personal site or blog.

Name your price

Pay what you can

Get Personal

- Spam protection

For commercial use

Plus POPULAR

Spam protection for professional or commercial sites and blogs.

Starting at

~~$10~~ $8.33

per month, billed yearly

Get Plus

- Spam protection
- **4** plan levels to choose from
- **10K to 40K** API calls/mo
- **Unlimited** sites
- **Priority** support

Enterprise

Spam protection for large networks or multisite installations.

~~$50~~ $41.67

per month, billed yearly

Get Enterprise

- Spam protection
- **60K** API calls/mo
- **Unlimited** sites
- **Priority** support

Enterprise Plus

Spam protection with custom solutions for large businesses.

Starting at

~~$250~~ $208.33

per month, billed yearly

Customize Enterprise Plus

- Spam protection
- **Custom** API limit
- **Unlimited** sites
- **Dedicated** support

Does Akismet only work with WordPress?

While Akismet is most used on the WordPress platform it is not just for WordPress. We support a variety of other platforms such as Drupal, phpBB3, Joomla, and more.

To see a list of all platforms we support – the ones we know about at least – please visit the development page.

Passwords Evolved

Passwords Evolved

By Carl Alexander

Download

Details | Reviews | Support | Development

Description

The goal of this plugin is to shore up the WordPress authentication using standard security practice recommendations. At this time, the plugin improves WordPress authentication by doing the following:

ENFORCING UNCOMPROMISED PASSWORDS

This plugin prevents someone from using passwords that have appeared in data breaches. Whenever someone logs into a WordPress site, it'll verify their password using the Have I been pwned? API. If their password appeared in a data breach, the plugin will prevent them from logging in until they reset their password.

Version:	1.3.2
Last updated:	5 months ago
Active installations:	2,000+
WordPress Version:	5.2 or higher
Tested up to:	5.9.4
PHP Version:	5.6 or higher
Languages:	See all 4
Tags:	argon2 authentication

This plugin prevents someone from using passwords that have appeared in data breaches. Whenever someone logs into a WordPress site, it'll verify their password using the Have I been pwned? API. If their password appeared in a data breach, the plugin will prevent them from logging in until they reset their password.

Home | Notify me | Domain search | Who's been pwned | Passwords | API | About | Donate

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) pwned?

629	11,923,631,961	115,310	223,129,640
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

Recently added breaches

scott@websanity.com pwned?

Oh no — pwned!

Pwned in 10 data breaches and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

APOLLO

Apollo: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles

B2B USA Businesses: In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. Read more about spam lists in HIBP.

Compromised data: Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

Evite: In April 2019, the social planning website for managing online invitations Evite identified a data breach of their systems. Upon investigation, they found unauthorised access to a database archive dating back to 2013. The exposed data included a total of 101 million unique email addresses, most belonging to recipients of invitations. Members of the service also had names, phone numbers, physical addresses, dates of birth, genders and passwords stored in plain text exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Dates of birth, Email addresses, Genders, Names, Passwords, Phone numbers, Physical addresses

Exactis: In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.

Compromised data: Credit status information, Dates of birth, Education levels, Email addresses, Ethnicities, Family structure, Financial investments, Genders, Home ownership statuses, Income levels, IP addresses, Marital statuses, Names, Net worths, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages

Factual: In March 2017, a file containing 8M rows of data allegedly sourced from data aggregator Factual was compiled and later exchanged on the premise it was a "breach". The data contained 2.5M unique email addresses alongside business names, addresses and phone numbers. After consultation with Factual, they advised the data was "publicly available information about businesses and other points of interest that Factual makes available on its website and to customers".

Compromised data: Email addresses, Employers, Phone numbers, Physical addresses

GeekedIn: In August 2016, the technology recruitment site GeekedIn left a MongoDB database exposed and over 8M records were extracted by an unknown third party. The breached data was originally scraped from GitHub in violation of their terms of use and contained information exposed in public profiles, including over 1 million members' email addresses. Full details on the incident (including how impacted members can see their leaked data) are covered in the blog post on 8 million GitHub profiles were leaked from GeekedIn's MongoDB - here's how to see yours.

LinkedIn Scraped Data: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.

Compromised data: Education levels, Email addresses, Genders, Geographic locations, Job titles, Names, Social media profiles

Onliner Spambot: In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moɈuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Compromised data: Email addresses, Passwords

Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

629	11,923,631,961	115,310	223,129,640
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
268,765,495	Wattpad accounts

Recently added breaches

349,627	Brand New Tube accounts
10,001,355	Stripchat accounts
7,455,386	START accounts
2,107,000	Banorte accounts
1,021,790	SitePoint accounts
23,817	Shitexpress accounts
6,682,453	Twitter accounts
22,229,637	QuestionPro accounts
985,586	Tuned Global accounts
437,928	Mecho Download accounts

In the last month, there were 1,260,000,000 occasions where a service somewhere checked a password against Have I Been Pwned's (HIBP's) Pwned Password API. 99.7% of the time, that check went no further than one of hundreds of Cloudflare edge nodes spread around the world (95% of the world's population is within 50ms of one). It looks like this:

Today, I'm really excited to mark a major milestone in the project thanks to the support of two of the world's foremost law enforcement agencies, the FBI and the NCA.

Last year I wrote about my intention to begin open sourcing parts of HIBP. I'm only able to run this project due to support from the community, so I wanted to start giving it back to the public in a bid to make it more open, more sustainable and in turn, more valuable to every single one of you using it. I made the decision to begin with Pwned Passwords and in May, I transitioned it into the .NET Foundation and announced we'd be building an ingestion pipeline. This pipeline enables the ingestion of passwords from law enforcement agencies, like the FBI. The premise is simple: during the course of their investigations, they come across a lot of compromised passwords and if they were able to continuously feed those into HIBP, all the other services out there using Pwned Passwords would be able to better protect their customers from account takeover attacks.

Wait so are you sending my password to a 3rd party!?

No, the plugin never sends your full password to a 3rd party for verification. The plugin only sends the first five characters of the SHA-1 hashed password to a 3rd party. The 3rd party then sends back all passwords with a hash that starts with those five characters.

The plugin then handles the rest of the password validation itself. It compares the SHA-1 hashed version of your password to the passwords returned by the 3rd party. We call this process k-anonymity. (You can read more about validating leaked passwords with it here.)

Dashboard
Jetpack
Posts
Media
Pages
Comments
HubSpot
Feedback
Rank Math
Elementor
Templates
Appearance
Plugins 1
Users
Tools
Settings
General

Passwords Evolved

"Have I been pwned?" API

Passwords Evolved uses the "Have I been pwned?" API to determine if someone is using a compromised password or not. You can read more about the API here. You can find the status of the API below.

You can also find all the roles used on your WordPress site. For each role, you can toggle password enforcement on login. If password enforcement is enabled for a role, someone with a compromised password won't be able to log in until they reset their password with an uncompromised one.

API status `Active`

Enforced roles

- [x] Administrator
- [ ] Editor
- [ ] Author
- [ ] Contributor
- [ ] Subscriber

Save changes

The plugin also encrypts passwords using either the bcrypt and Argon2 hashing functions. These are the strongest hashing functions available in PHP. Argon2 is available natively starting with PHP 7.2, but the plugin can also encrypt passwords on older PHP versions using the libsodium compatibility layer introduced in WordPress 5.2.

WP 2FA

WP 2FA – Two-factor authentication for WordPress

By WP White Security

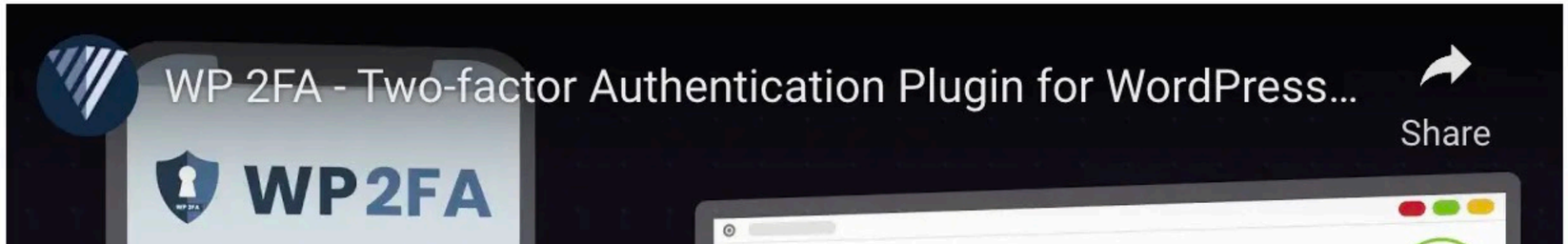
Download

Details | Reviews | Support | Development

Description

A FREE & EASY TO USE TWO-FACTOR AUTHENTICATION PLUGIN FOR WORDPRESS

Add an extra layer of security to your WordPress website login page and its users. Enable two-factor authentication (2FA), the best protection against users using weak passwords, and automated password guessing and brute force attacks.



Version:	2.3.0
Last updated:	4 days ago
Active installations:	30,000+
WordPress Version:	5.0 or higher
Tested up to:	6.0.2
PHP Version:	7.3 or higher
Languages:	See all 9
Tags:	2-factor authentication
	2FA

WP 2FA KEY PLUGIN FEATURES & CAPABILITIES

- Free Two-factor authentication (2FA) for all users
- Supports multiple 2FA methods
- Universal 2FA app support – generate codes from Google Authenticator, Authy & any other 2FA app
- Supports 2FA backup methods
- Very easy to use and simple to set up
- Use 2FA policies to enforce 2FA with a grace period
- Or require users users to instantly setup 2FA upon logging in
- Out of the box support for third party plugins such as WooCommerce and other e-commerce & membership plugins
- No WordPress dashboard access required for users to set up 2FA
- Protection against automated password & dictionary attacks
- And many other plugin features)

Works with any 2FA app

Your website users do not have to install and learn how to use a new 2FA app. WP 2FA works with all the popular 2FA smartphone apps, including Authy, Google Authenticator, Microsoft Authenticator, Lastpass, FreeOTP and many others. With an easy-to-use wizard and support for all 2FA apps, your users can configure and use 2FA without requiring any help, within just seconds.

The world's most-loved password manager

1Password is the easiest way to store and use strong passwords. Log in to sites and fill forms securely with a single click.

Get started

WP 2FA

Welcome to WP 2FA · Choose Method · Setup the 2FA method · Backup Codes

You are required to configure 2FA.

In order to keep this site - and your details secure, this website's administrator requires you to enable 2FA authentication to continue.

Two factor authentication ensures only you have access to your account by creating an added layer of security when logging in - Learn more

Next

WP 2FA

Welcome | Choose Method | Setup the 2FA method | Setup Finish | Select 2FA Methods | Backup Codes

1 Download authenticator 2 Verify configuration

Setup the 2FA method

1. Download the app of your choice
2. Scan the QR code to the right.

Otherwise, select Enter a provided key and type in the key below:

`IYUGGNB5EYSS6X3PNZCWAS3PKFDHGNCK`

For detailed guides for your desired app, click below.

AUTHY · Google Authticator · Microsoft Authenticator · DUO · LastPass AUTHENTICATOR · FreeOTP

I'm Ready

WP 2FA

Choose Method — Setup the 2FA method — Backup Codes

Backup codes generated

Here are your backup codes:

```
32608330
70699555
14463736
47358545
25318297
33339070
57884513
20636388
13972881
99829231
```

Download | Print

I'm ready

Settings

Which of the below 2FA methods can users use?

Select the methods

Primary 2FA methods:

- [x] One-time code via 2FA App (TOTP) - complete list of supported 2FA apps.
- [ ] One-time code via email (HOTP)

Allow user to specify the email address of choice

( ) Yes (•) No

Secondary 2FA methods:

- [x] Backup codes - Backup codes are a secondary method which you can use to log in to the website in case the primary 2FA method is unavailable. Therefore they can't be enabled and used as a primary method.

Do you want to enforce 2FA for some, or all the users?

When you enforce 2FA the users will be prompted to configure 2FA the next time they login. Users have a grace period for configuring 2FA. You can configure the grace period and also exclude user(s) or role(s) in this settings page. Learn more.

Enforce 2FA on

- (•) All users
- ( ) Only for specific users and roles
- ( ) Do not enforce on any users

Should users be asked to setup 2FA instantly or should they have a grace period?

When you enforce 2FA on users they have a grace period to configure 2FA. If they fail to configure it within the configured stipulated time, their account will be locked and have to be unlocked manually. Note that user accounts cannot be unlocked automatically, even if you change the settings. As a security precaution they always have to be unlocked them manually. Maximum grace period is 10 days. Learn more.

Grace period

- (●) Users have to configure 2FA straight away.
- ( ) Give users a grace period to configure 2FA

Can users access the WordPress dashboard or you have custom profile pages?

If your users do not have access to the WordPress dashboard (because you use custom user profile pages) enable this option. Once enabled, the plugin creates a page which ONLY authenticated users can access to configure their user 2FA settings. A link to this page is sent in the 2FA welcome email.

Frontend 2FA settings page ○ Yes ◉ No

Frontend 2FA settings page URL https://offsetexchange.com/

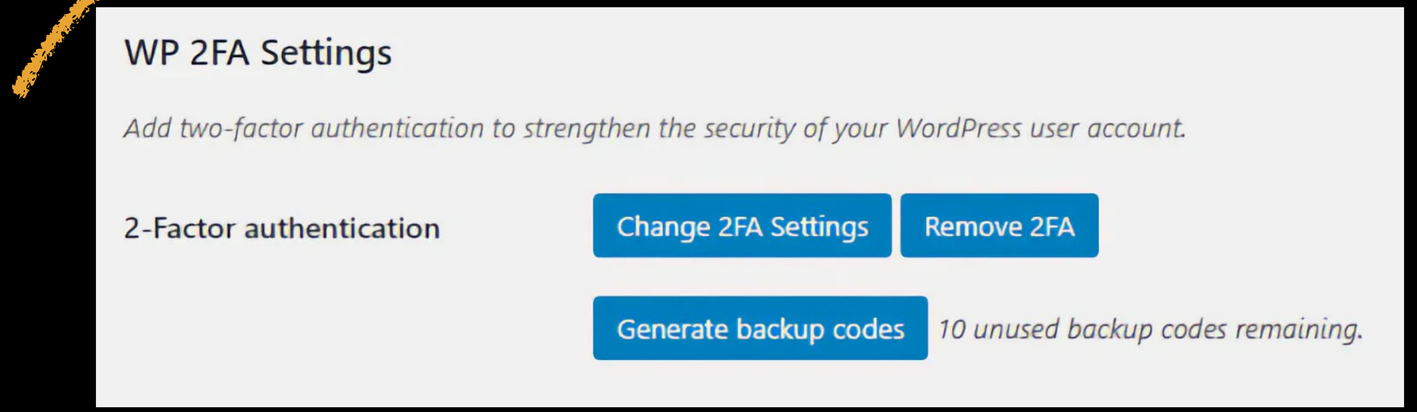
Specify the page where you want to redirect your users to after they complete the 2FA setup. This will override the global redirect setting.

Redirect users after 2FA setup https://offsetexchange.com/

Should users be able to disable 2FA on their user profile?

Users can configure and also disable 2FA on their profile by clicking the "Remove 2FA" button. Enable this setting to disable the Remove 2FA button so users cannot disable 2FA from their user profile.

Hide the Remove 2FA button ☐ Hide the Remove 2FA button on user profile pages



Should users be able to disable 2FA on their user profile?

Users can configure and also disable 2FA on their profile by clicking the "Remove 2FA" button. Enable this setting to disable the Remove 2FA button so users cannot disable 2FA from their user profile.

Hide the Remove 2FA button ☐ Hide the Remove 2FA button on user profile pages

WP 2FA Settings

Add two-factor authentication to strengthen the security of your WordPress user account.

2-Factor authentication

Change 2FA Settings | Remove 2FA

Generate backup codes *10 unused backup codes remaining.*

Should users be able to disable 2FA on their user profile?

Users can configure and also disable 2FA on their profile by clicking the "Remove 2FA" button. Enable this setting to disable the Remove 2FA button so users cannot disable 2FA from their user profile.

Hide the Remove 2FA button ☐ Hide the Remove 2FA button on user profile pages

WP 2FA Settings

Add two-factor authentication to strengthen the security of your WordPress user account.

2-Factor authentication

Change 2FA Settings

Generate backup codes *10 unused backup codes remaining.*

Premium

Upgrade to WP 2FA Premium to:

- 2FA over SMS, Push notification, WhatsApp and incoming call via Authy integration
- Add trusted devices – no need for 2FA code each time you log in
- Whitelabel all the 2FA pages – for a consistent user experience
- Give the users more 2FA methods to choose from and use
- Configure different 2FA policies for different user profiles
- More alternative 2FA backup methods
- Easily get an overview of users' 2FA setup with the reports
- And many other features

BEST DEAL

Enterprise

$99 /year

The ultimate solution with priority support

5 Users

GET STARTED

Includes:

- Everything in Business
- Priority support (6 – 8 hours response time)

Business

$69 /year

The ultimate 2FA solution for businesses

5 Users

GET STARTED

Includes:

- Everything in the Professional plan
- 2FA over SMS, Push notification, WhatsApp & incoming calls*
- White labeling (logo, text, colours & fonts)
- Reports & statistics
- Configurable 2FA code expiration time
- Sortable users' 2FA status

Professional

$59 /year

Great for businesses who want a bit more

5 Users

GET STARTED

Includes:

- Everything in Starter plan
- Trusted devices (don't ask for 2FA code)
- One-click 2FA
- Secondary 2FA backup method

Starter

$29 /year

Getting started with the essentials

5 Users

GET STARTED

Includes:

- Install on unlimited websites
- 2FA code via mobile app
- 2FA code over email
- Different 2FA policies per user role

Other Plugins from WP White Security

WPassword

No software can protect your WordPress site from weak passwords users use. Install WPassword and easily enforce strong passwords on your users and improve WordPress password security.

The plugin is very easy to setup and intuitive. Also, your site users do not have to learn anything new and their logins are not affected since the plugin is integrated in the WordPress login page.

Buy & Download

Learn More →

CAPTCHA 4WP

Show any type of Captcha (such as noCaptcha or invisible Captcha) on any form on your WordPress website, such as on comment forms, Contact Form 7, bbPress, BuddyPress, WooCommerce, Login, Register, Lost Password, Reset Password.

With this plugin, you can implement any type of Captcha check to any form easily, within just minutes.

Download Free Edition

Learn More →

WP Activity Log

WP Activity Log is the most comprehensive activity log plugin for WordPress with the broadest coverage. It allows you to keep a log of all users' and under the hood activity that happens on your site, enabling you to better manage your users, site & business.

The plugin is very easy to use, fully automated and is trusted by tens of thousands of businesses, including world renowned brands such as Disney, NASA and Intel!

Download Free Edition

Learn More →

Website File Changes Monitor

Keep an eye on your site's code & file changes. Identify developers' leftover files that can lead to data leaks, and pinpoint malware injected during hack attacks.

Use the hassle-free Website File Changes Monitor plugin and get alerted whenever files are added, modified or deleted from your WordPress website.

Download Free Plugin

Learn More →

Trusted by world renowned brands & agencies!

ManageWP

The problem: managing several WordPress sites

The solution: ManageWP

ManageWP Worker

By GoDaddy

Download

Details | Reviews | Installation | Support | Development

Description

So you're looking for a better way to manage WordPress websites? We have you covered! ManageWP is a dashboard that helps you save time and nerves by automating your workflow, so you could focus on things that matter. It is fast, secure and free for an unlimited number of websites.

EVERYTHING IN ONE PLACE

Just the hassle of logging into each of your websites is enough to ruin your day. ManageWP compiles the data from all of your sites on one dashboard, so you can check up on your websites in a single glance. And

Version:	4.9.14
Last updated:	3 months ago
Active installations:	1+ million
WordPress Version:	3.1 or higher
Tested up to:	6.0.2
Languages:	See all 33
Tags:	backup, Manage Multiple Sites, migrate, performance

ManageWP Worker

By GoDaddy

Download

Details | Reviews | Installation | Support | Development

Description

So you're looking for a better way to manage WordPress websites? We have you covered! ManageWP is a dashboard that helps you save time and nerves by automating your workflow, so you could focus on things that matter. It is fast, secure and free for an unlimited number of websites.

EVERYTHING IN ONE PLACE

Just the hassle of logging into each of your websites is enough to ruin your day. ManageWP compiles the data from all of your sites on one dashboard, so you can check up on your websites in a single glance. And

Version:	4.9.14
Last updated:	3 months ago
Active installations:	1+ million
WordPress Version:	3.1 or higher
Tested up to:	6.0.2
Languages:	See all 33
Tags:	backup, Manage Multiple Sites, migrate, performance

Backups

FREE PREMIUM

Incremental, reliable, comes with off-site storage, and capable of running on an hourly cycle.

Clone / Migrate

PREMIUM

Clone your website to a staging area, migrate to a new host, or clone to an existing site.

Uptime Monitor

PREMIUM

Get notification when your website goes down, so you could get it back online before anyone else notices.

Safe Updates

REQUIRES PREMIUM BACKUPS

Safe Updates automatically create a restore point for you, making updating safer than ever.

Sucuri Security Check

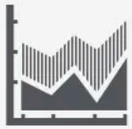
FREE PREMIUM

Make sure your sites are clean, and if any files become infected you will be able to spot them on time.

Performance Check

FREE PREMIUM

Have an insight into what is happening with your website and how it’s performing.



Client Reports

FREE PREMIUM

Keep your clients informed at all times with fully editable, professional Client Reports.

White Label

PREMIUM

White Label allows you to re-brand our tools and make them your own, or hide them entirely.

Google Analytics

FREE

All Google accounts that you need connected to Google Analytics on one dashboard. Keep track of all results.

Maintenance Mode

FREE

Maintenance Mode gives you the option of letting your visitors know that you are working on your website, updating or fixing problems.

Code Snippets

FREE

With Code Snippets you can extend the functionality of your site whilst keeping resources required to a minimum.

SEO Ranking

PREMIUM

Keep track of how your keyword ranking changes, find out who your competitors are, and how you stack up against them.

2-factor Authentication

FREE

2-factor authentication prevents any would-be hackers from gaining access to your site through means of brute force attacks.

1-click Login

FREE

You can connect all of your websites to a single dashboard, get a summary of what's going on, and log into each of them with just one click.

Manage Comments

FREE

All of your comments in one place, available for you on one screen. This way you can approve or send to spam any comment in seconds.

Local Sync

FREE WHILE IN BETA

Sync website changes between localhost and live environments with one click. No port forwarding or desktop apps needed.

Manage Plugins & Themes

FREE

Update, ignore, bulk install, deactivate, or install an older version over the current one.

Vulnerability Updates

FREE

Vulnerability check bring you real time information about what plugins are vulnerable so you can act accordingly.

Collaborate

FREE

A team is helping you, or maybe clients like a hands-on approach. Give them access to your dashboard without revealing your password.

Template Builder

FREE

Create your own WordPress website templates using the Template Builder or use an existing backup as a start point for the template creation.

Link Monitor

PREMIUM

Link Monitor is a powerful broken link checker that provides you with regular scans of an entire WordPress site for broken links.

Manage Updates, Plugins & Themes

Monthly Cloud Backup

1-Click Login

Clone (requires premium Backup)

Safe Updates (requires premium Backup)

Performance Check

Security Check

Collaborate with Team & Clients

Analytics

Manage Comments

Code Snippets

Maintenance Mode

Client Report

Vulnerability Updates

Free

Premium upgrades for those **who need more.**

Sign up

If you value your time, start saving it by letting ManageWP do the heavy lifting for you with automation, website migration, and more.

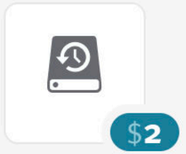
Per website

For freelancers and small agencies with up to 25 websites, looking to optimize cost.

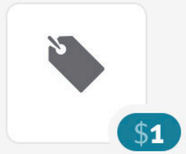
Bundle

For agencies with over 25 websites, a fixed monthly fee for up to 100 websites

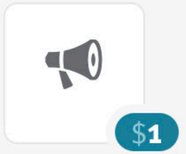
learn more



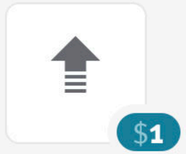
Backup



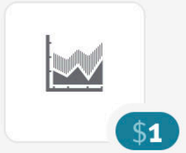
White Label



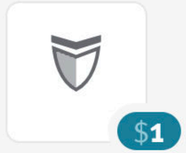
SEO Ranking



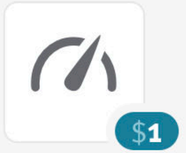
Uptime Monitor



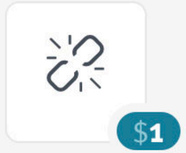
Advanced Client Report



Automated Security Check



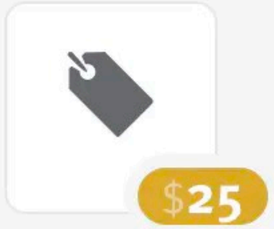
Automated Performance Check



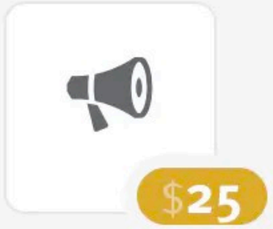
Link Monitor

Prices shown on a monthly per website, per add-on basis.

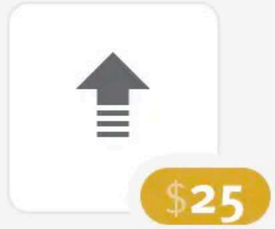
Backup



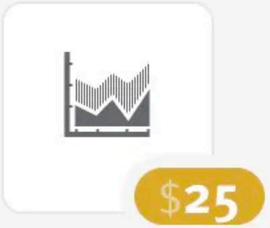
White Label



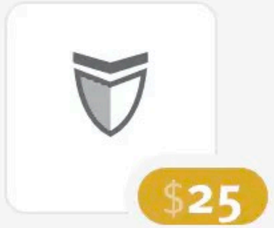
SEO Ranking



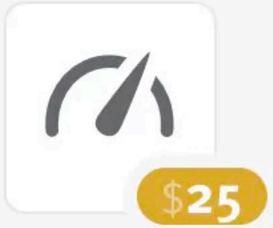
Uptime Monitor



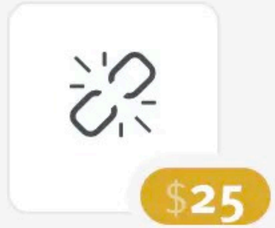
Advanced Client Report



Automated Security Check



Automated Performance Check

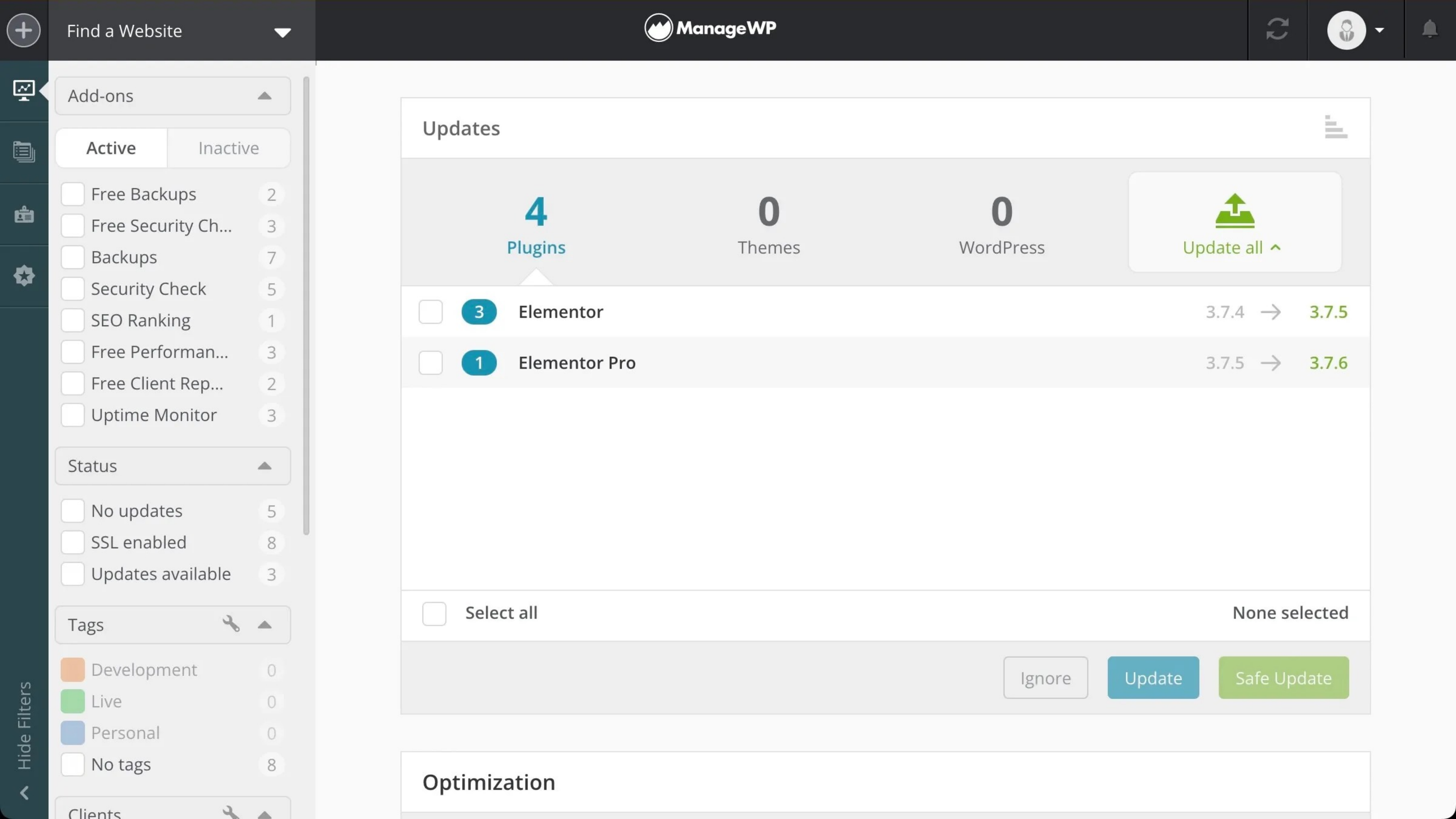


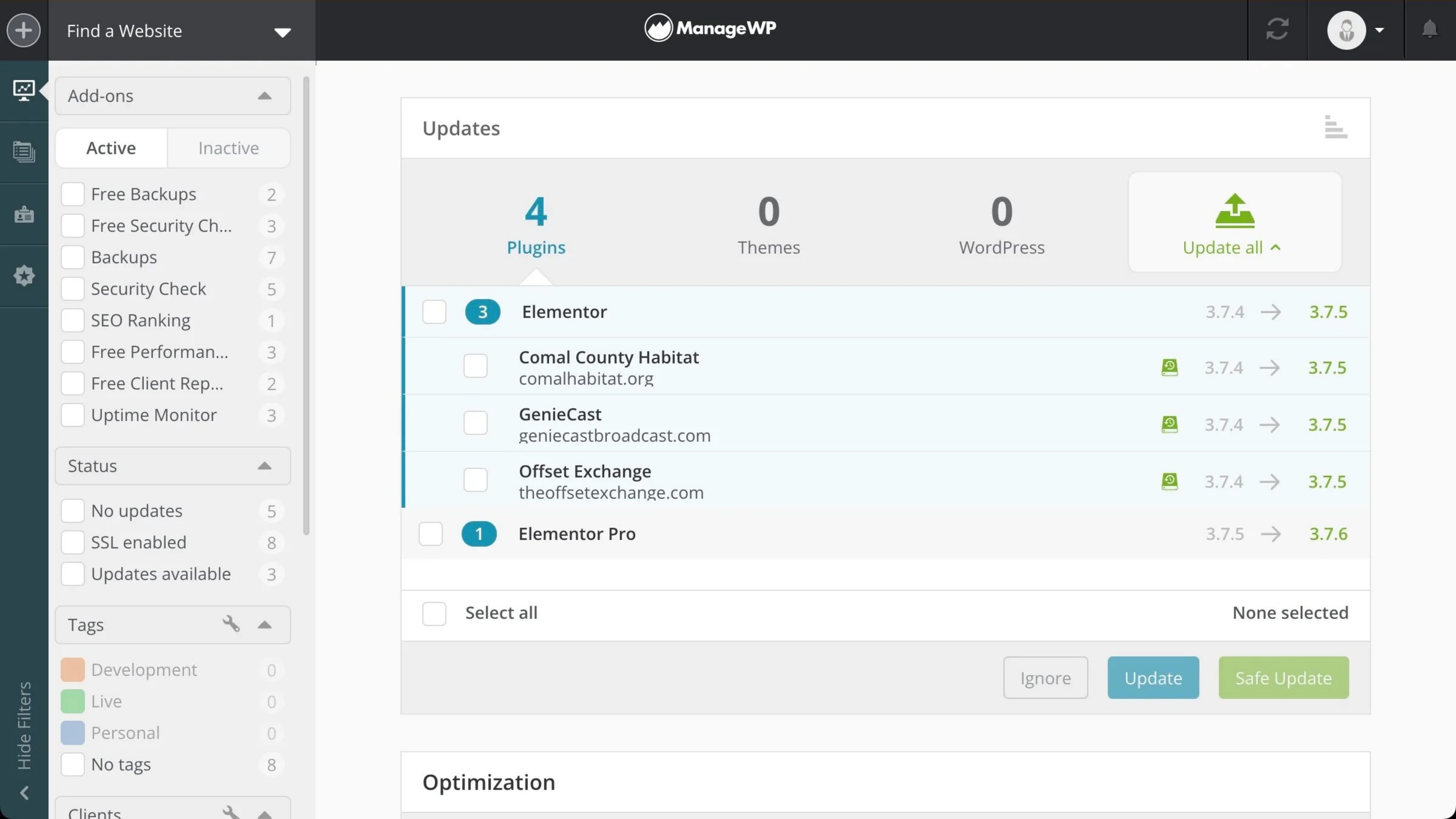
Link Monitor

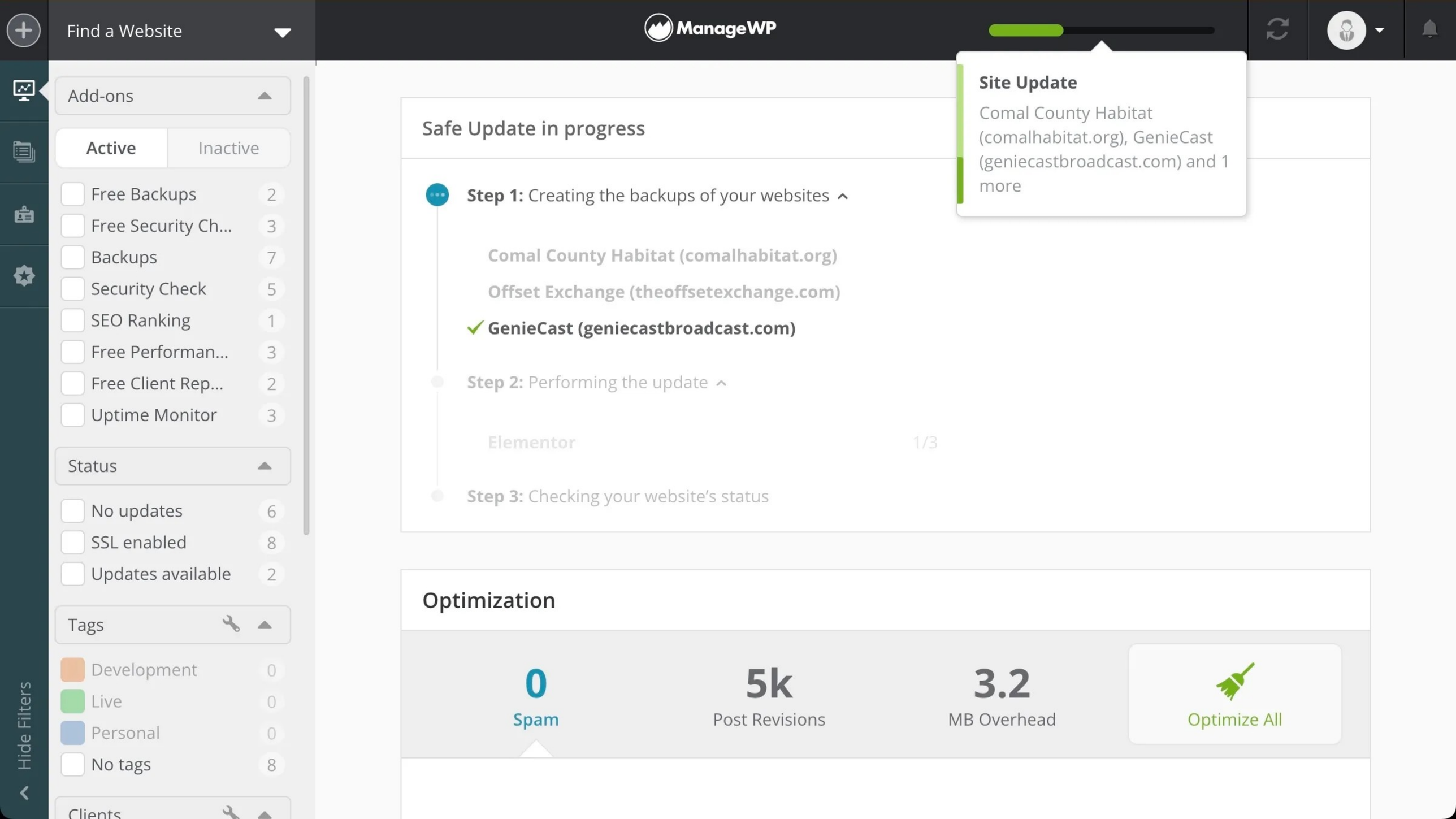
All-in-one package (all bundles combined)

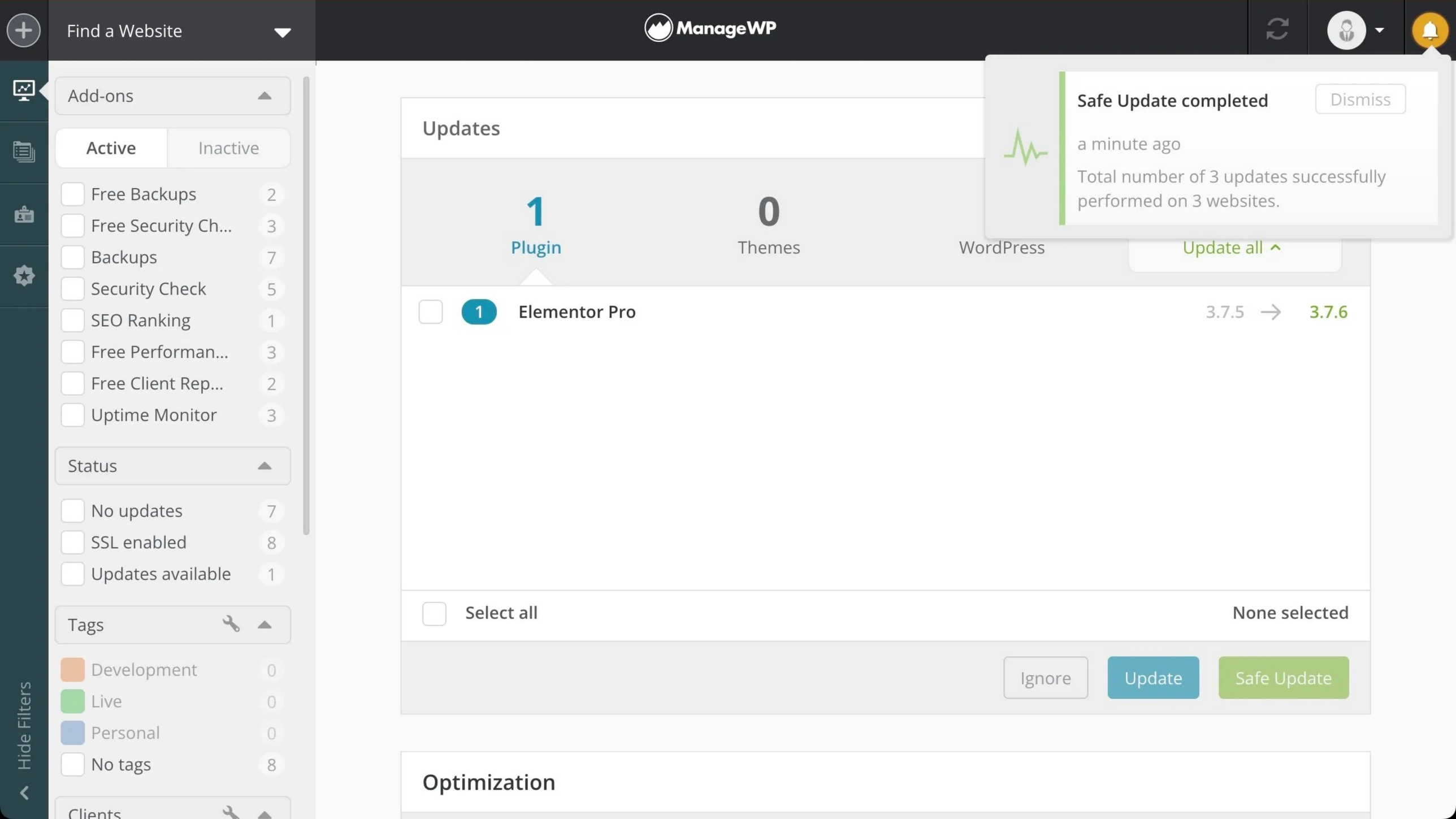
Bundle

Updates

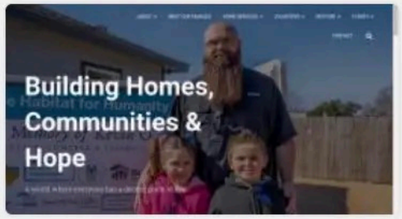

Find a Website
ManageWP
Add-ons
Active
Inactive
Free Backups 2
Free Security Ch... 3
Backups 7
Security Check 5
SEO Ranking 1
Free Performan... 3
Free Client Rep... 2
Uptime Monitor 3
Status
No updates 5
SSL enabled 8
Updates available 3
Tags
Development 0
Live 0
Personal 0
No tags 8
Hide Filters
Updates
4
Plugins
0
Themes
0
WordPress
Update all
3 Elementor 3.7.4 → 3.7.5
1 Elementor Pro 3.7.5 → 3.7.6
Select all
None selected
Ignore
Update
Safe Update
Optimization


Find a Website
ManageWP
Add-ons
Active
Inactive
Free Backups 2
Free Security Ch... 3
Backups 7
Security Check 5
SEO Ranking 1
Free Performan... 3
Free Client Rep... 2
Uptime Monitor 3
Status
No updates 5
SSL enabled 8
Updates available 3
Tags
Development 0
Live 0
Personal 0
No tags 8
Hide Filters
Updates
4
Plugins
0
Themes
0
WordPress
Update all
3 Elementor 3.7.4 → 3.7.5
Comal County Habitat
comalhabitat.org 3.7.4 → 3.7.5
GenieCast
geniecastbroadcast.com 3.7.4 → 3.7.5
Offset Exchange
theoffsetexchange.com 3.7.4 → 3.7.5
1 Elementor Pro 3.7.5 → 3.7.6
Select all
None selected
Ignore
Update
Safe Update
Optimization


Find a Website
ManageWP
Site Update
Comal County Habitat (comalhabitat.org), GenieCast (geniecastbroadcast.com) and 1 more
Add-ons
Active
Inactive
Free Backups 2
Free Security Ch... 3
Backups 7
Security Check 5
SEO Ranking 1
Free Performan... 3
Free Client Rep... 2
Uptime Monitor 3
Status
No updates 6
SSL enabled 8
Updates available 2
Tags
Development 0
Live 0
Personal 0
No tags 8
Hide Filters
Safe Update in progress
Step 1: Creating the backups of your websites
Comal County Habitat (comalhabitat.org)
Offset Exchange (theoffsetexchange.com)
GenieCast (geniecastbroadcast.com)
Step 2: Performing the update
Elementor 1/3
Step 3: Checking your website's status
Optimization
0
Spam
5k
Post Revisions
3.2
MB Overhead
Optimize All


Find a Website
ManageWP
Add-ons
Active
Inactive
Free Backups 2
Free Security Ch... 3
Backups 7
Security Check 5
SEO Ranking 1
Free Performan... 3
Free Client Rep... 2
Uptime Monitor 3
Status
No updates 7
SSL enabled 8
Updates available 1
Tags
Development 0
Live 0
Personal 0
No tags 8
Hide Filters
Safe Update completed
Dismiss
a minute ago
Total number of 3 updates successfully performed on 3 websites.
Updates
1
Plugin
0
Themes
WordPress
Update all
1
Elementor Pro
3.7.5
3.7.6
Select all
None selected
Ignore
Update
Safe Update
Optimization

Backups



Comal County Habitat
comalhabitat.org

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking

Backups

Deactivate

SEPTEMBER 2022

Mon	Tue	Wed	Thu	Fri	Sat	Sun
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

Latest backup:
2022-09-14, 14:28:06

Next backup:
2022-09-14, 15:25:46

Backup Now

Backups for 2022-09-14 **Safe Update Backup**

14:28:06

Overview | Content | Settings | Restore from ZIP

Comal County Habitat
comalhabitat.org

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking

Backups

Deactivate

‹	AUGUST 2022					›
Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

Latest backup:
2022-09-14, 14:28:06

Next backup:
2022-09-14, 15:25:45

Backup Now

Backups for 2022-08-29 **Automatic backup**

15:56:34 | 10:43:20

Overview | Content | Settings | Restore from ZIP

Comal County Habitat
comalhabitat.org

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking

Backups

Deactivate

‹	AUGUST 2022					›
Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

Latest backup:
2022-09-14, 14:28:06

Next backup:
2022-09-14, 15:25:45

Backup Now

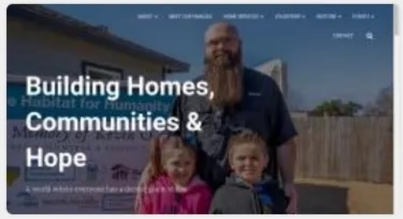
Backups for 2022-08-29 **Safe Update Backup**

15:56:34 | 10:43:20

Overview | Content | Settings | Restore from ZIP

Find a Website

ManageWP



Comal County Habitat

comalhabitat.org

WP Admin | Settings

- Dashboard
- Backups
- Plugins
- Themes
- Users
- Local Sync (BETA)
- Link Monitor
- Security
- Performance
- Uptime Monitor
- SEO Ranking

Backups

Deactivate

SEPTEMBER 2022

Mon	Tue	Wed	T
29	30	31	
5	6	7	
12	13	14	
19	20	21	
26	27	28	
3	4	5	

Where do you store my backups?
Your backups are saved on our secure cloud storage using Amazon S3 infrastructure.

What do you backup?
We backup the entire standard WordPress structure except the log files and other backup files.

How does this affect my website performance?
The incremental backup technology that we have developed will store only those files that changed after the last backup was made, meaning that the server resources usage will be minimal.
We will do all the heavy lifting and assemble full backup archives on our servers.

For how long do you keep my backups?
We keep your backup history for a full 90 days.

Backups for

14:28:06

Overview Content Settings Restore from ZIP

Comal County Habitat
comalhabitat.org

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking

Backups

Deactivate

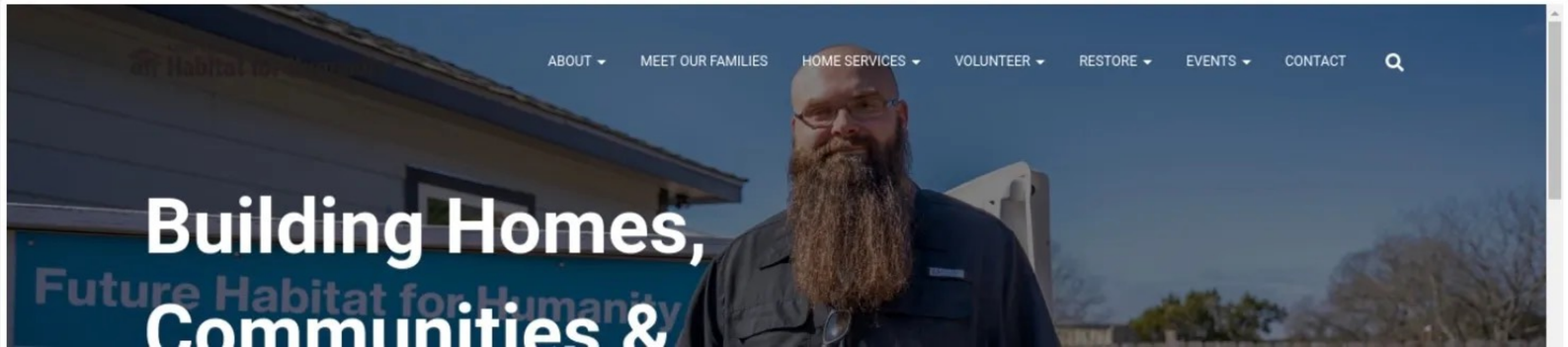
Overview | Content | Settings | Restore from ZIP

Restore backup | Download backup | Clone website | Create template

WordPress version: **6.0.2** Backup size: **888.49 MB**

Active theme: **Hestia v3.0.23**

Active Plugins: **8** Published posts: **5** Approved comments: **0**



Comal County Habitat
comalhabitat.org

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking

Backups

Deactivate

14:28:06

Overview | Content | Settings | Restore from ZIP

Restore backup | Download backup | Clone website | Create template

Files	858.32 MB
Database	30.17 MB

* You can hover over an individual file or folder to download it.

Comal County Habitat
comalhabitat.org

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking

Backups

Deactivate

Overview | Content | Settings | Restore from ZIP

Backup schedule

Engineered with highest standards. Comprehensive backup solution with automated backups, automated restores, 90-day backup archive and site migration tools.

Monthly | Weekly | **Daily** | Every 12h | Every 6h | Every 1h

Perfect for
Standard WordPress websites that get comments or content updates at least once a week

Price
No change in price (You're currently on the Daily cycle for $1.80 / month)

Scheduling time is using main account timezone:

Comal County Habitat
comalhabitat.org

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor

Backups

Deactivate

Overview | Content | Settings | Restore from ZIP

- Backup schedule
- Include/exclude content
- Storage Region
- Event notifications
- FTP Settings - Optional
- MYSQL Settings - Optional

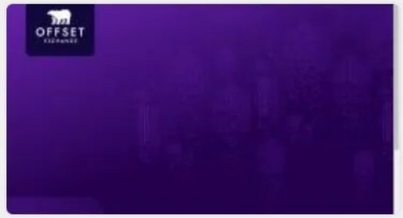
The **free backup** is ideal for small websites, and websites with static content. This backup is available to all of our ManageWP users. **Free backup spec**:

- Monthly scheduled backup
- Off-site storage
- 1-click restore
- US/EU storage choice
- exclude files and folders
- receive notifications via Email or Slack if your website is down

The **premium backup** is suited to more demanding websites and active development. **The premium add-on has everything the free version does, plus**:

- on-demand backups
- cloning/migration tool
- different backup frequencies, from weekly to near real-time (every 1h)
- download backup to your computer
- exclude as well as include files and folders
- **Starts at $2/month**
- **$75/month for up to 100 websites with a bundle**. (please note that the bundle does not include real time backup, it covers daily and weekly backups only)

Security Check



Offset Exchange
theoffsetexchange.com

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking

Security Check

Deactivate

Overview | Scheduling

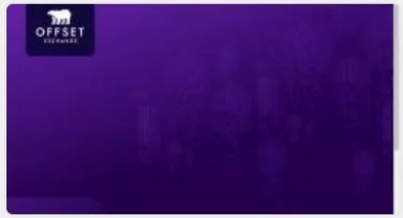
Latest security check status: **Verified clean**
Next Automated Check: **September 15**

Check Now

Latest security check: **12 hours ago**

Vulnerabilities: **Clean**
Malware: **Clean**
Web Trust: **Clean**

Date	Status
2022-09-14, 03:04:11	Verified clean
2022-09-13, 01:02:50	Verified clean
2022-09-11, 22:01:08	Verified clean
2022-09-11, 03:04:58	Verified clean



Offset Exchange
theoffsetexchange.com

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking

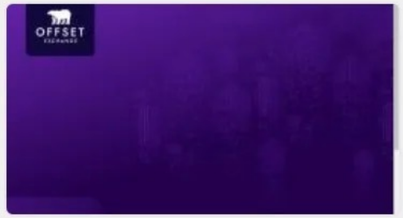
Security Check for 2022-09-14, 03:04:11

Status | Vulnerabilities | Web Trust

Domain clean on

Google Safe Browsing	theoffsetexchange.com	Learn more...
Norton Safe Web	theoffsetexchange.com	Learn more...
Phish tank	theoffsetexchange.com	Learn more...
Opera browser	theoffsetexchange.com	Learn more...
SiteAdvisor	theoffsetexchange.com	Learn more...
Sucuri Malware Labs	theoffsetexchange.com	Learn more...
SpamHaus DBL	theoffsetexchange.com	Learn more...
Bitdefender	theoffsetexchange.com	Learn more...

Uptime Monitor



Offset Exchange
theoffsetexchange.com

WP Admin | Settings

Dashboard
Backups
Plugins
Themes
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking

Uptime Monitor

Deactivate

Uptime Activity | Settings

UP

Overall uptime is **99.99%**

Up for 4d 14h

Latest downtime: 2022-09-10, 00:43:09, lasted for 1m 57s

Uptime overview

100%	99.98%	99.99%
(last 24 hours)	(last 7 days)	(last 30 days)

Latest events

↑ Up	Everything is ok	2022-09-10, 00:45:06 for 4d 14h
↓ Down	Internal Server Error	2022-09-10, 00:43:09 for 1m 57s
↑ Up	Uptime turned on	2022-08-29, 16:24:30 for 11d 8h

Offset Exchange
theoffsetexchange.com
WP Admin
Settings
Users
Local Sync (BETA)
Link Monitor
Security
Performance
Uptime Monitor
SEO Ranking
Client Report
White Label
More Tools...
System Info
Maintenance Mode
Code Snippets
History

Uptime Monitor

Deactivate

Uptime Activity | Settings

General

Monitoring interval: Every 5 minutes

1 minute | **5 minutes** | 10 minutes | 15 minutes

Notification delay: No delay

No delay | 5m | 10m | 15m | 20m | 30m | 45m | 60m

This option will delay sending of the notification by given time. If the website comes back up during this interval, the notification will not be sent.

Is ManageWP secure?

Yes. All of our code is developed in-house and we have a top notch security team. With half a million websites managed since 2012 we did not have a single security incident. We've accomplished this through high standards, vigilance and the help of security researchers, through our white hat security program.

Thank you!

scott@granneman.com
www.granneman.com
@scottgranneman

jans@websanity.com
websanity.com

WordPress Security Plugins & Settings

You do realize there's a huge target on WordPress, yes?

R. Scott Granneman & Jans Carton

© 2022 R. Scott Granneman
Last updated 2022-09-14
You are free to use this work, with certain restrictions: CC BY-SA 4.0
For full licensing information, please see the last slide/page.

1.0

Changelog

2022-09-14 1.0: Created & completed slides

Licensing of this work

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License.

To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/4.0/.

You are free to:

» *Share* — copy and redistribute the material in any medium or format
» *Adapt* — remix, transform, and build upon the material for any purpose, even commercially

Under the following terms:

Attribution. You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. Give credit to:

Scott Granneman • www.granneman.com • scott@granneman.com

Share Alike. If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions. You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Questions? Email scott@granneman.com