

Admin Tools for WordPress

Nicholas K. Dionysopoulos

Davide Tampellini

Admin Tools for WordPress

Nicholas K. Dionysopoulos

Davide Tampellini

Copyright © 2017-2021 Akeeba Ltd

Abstract

This book covers the use of the Admin Tools for WordPress site security plugin for WordPress™ -powered web sites. Both the free Admin Tools Core and the subscription-based Admin Tools Professional editions are completely covered.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the appendix entitled "The GNU Free Documentation License".

Table of Contents

1. Getting Started	1
1. What is Admin Tools?	1
1.1. Disclaimer	1
1.2. The philosophy	2
2. Server environment requirements	2
3. Installing Admin Tools	3
3.1. Updating to the latest version	3
4. Upgrading from Core to Professional	4
5. Requesting support and reporting bugs	4
6. Quick Setup	4
2. Using Admin Tools	7
1. The Control Panel	7
2. The Plugin Params page	9
3. Fixing the permissions of files and directories	11
3.1. Configuring the permissions of files and directories	13
4. Emergency Off-Line Mode	14
5. Protecting Admin Tools with a password (Master Password)	17
6. Protect your WordPress administration with a password	19
7. The .htaccess maker	21
7.1. Basic Security	23
7.2. Server protection	29
7.2.1. How to determine which exceptions are required	31
7.3. Custom .htaccess rules	32
7.4. Optimisation and utility	33
7.5. System configuration	39
8. Malware Detection (the PHP File Scanner)	40
8.1. How does it work and what should I know?	42
8.2. Configuration	43
8.3. Scanning and administering scans	45
8.4. Reading the reports	47
8.5. Automating the scans (CRON jobs)	49
8.6. Automating the scans (scheduling URL)	49
9. Web Application Firewall	51
9.1. How WAF works and optimization	54
9.2. Configure	57
9.2.1. Basic Protection Features	58
9.2.2. Request Filtering	63
9.2.3. Hardening Options	65
9.2.4. Cloaking	68
9.2.5. Project Honeypot	69
9.2.6. Exceptions	71
9.2.7. Auto-ban	73
9.2.8. Logging and reporting	75
9.2.9. Customisation	78
9.3. WAF Exceptions	79
9.4. Administrator IP Whitelist	81
9.5. Site IP Blacklist	84
9.6. Anti-spam Bad Words	87
9.7. Security Exceptions Log	88
9.7.1. List of blocking reasons	88
9.8. Auto IP Blocking Administration	90
9.9. Auto IP Blocking History	91
9.10. Email templates	92
10. WordPress tools	95
10.1. Update WordPress salts	96

10.2. Password expiration	97
10.3. Advanced WordPress options	97
10.3.1. Post settings	98
10.3.2. System settings	99
11. Database tools	100
12. HTTPS Tools	101
13. URL Redirection	101
14. Import and Exporting Settings	104
A. GNU General Public License version 3	105
B. GNU Free Documentation License	114

Chapter 1. Getting Started

1. What is Admin Tools?

Admin Tools is a security plugin, a software solution which will help you tighten the security of your WordPress site. Moreover, it has several features which will help you enhance the performance of your site and make your life administering the site a bit easier.

Admin Tools is written with PHP and WordPress best practices in mind. It uses a native WordPress plugin to apply its security and performance enhancing features. It does not modify WordPress' core files ("core hacks"), therefore allowing you to update WordPress trouble-free. In fact, we only support the latest published version of WordPress at all times: it makes no sense thinking about a secure site while running old, insecure code.

Admin Tools comes in two editions, the free of charge Core edition and the subscription-only Professional edition. The Core edition only has basic utility and security features. The full suite of security features can only be found in the Professional edition.

1.1. Disclaimer

Security plugins —like Admin Tools— are designed to help you enhance your site's security, not make it invulnerable against all hacking attempts. Whereas it will make it harder for a potential attacker to figure out information pertaining your site and will give them a hard time attacking your site, there is nothing that can stop a determined attacker with plenty of resources from hacking your site. For instance, if you have an outdated WordPress installation or a vulnerable plugin installed on your site there is nothing —and, let us stress that, NOTHING— which can stop a hacker from successfully attacking your site.

Security software is like a bulletproof vest. You don't wear it for total invincibility against all attacks (a lucky shot in an area not covered by it, a high power, penetrating round and an explosion can still kill you). You are wearing it because what is most likely to get you is what the vest can stop.

In the end of the day *you* are ultimately responsible for the security of your site, employing a holistic approach to security including sane personal security practices. Installing and configuring Admin Tools is meant to be *part* of your security regimen. At the very least you are expected to take frequent backups, stored in safe locations outside of your server, apply security-conscious password management, maintain a secure working environment (as in: if your computer is full of malware your site is as good as hacked no matter if you use Admin Tools or not) and keep an eye for any abnormal behaviour on your site.

Moreover, let it be stated in no uncertain terms that **security is not something you install and forget about it**. Admin Tools, like all security plugins, is a *tool*. You use it to improve your site's security. As such, you *do* need to configure it, you *do* need to check for false positives and ultimately make decisions which boil down to trading security for convenience. No two sites are the same. *You* are the person who best knows the needs and requirements for your site, therefore *you* are the most fit person to make such decisions.

Finally, we are legally obliged to draw your attention to the warranty and liability waiver Sections 15 through 17 of the software's license, copied here for your convenience:

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

1.2. The philosophy

Admin Tools is a tool which helps you tighten the security of your site. Admin Tools, like every security software, is not something that you install and immediately become invulnerable to hackers. This is not something particular to Admin Tools. All firewalls, Internet security, antivirus and other security software are just tools. If someone had a magic solution that makes sites or computers invulnerable to hackers they would be billionaires: every major corporation and government in the world would like to have such a solution.

Admin Tools is a very capable security solution which can protect you against many different types of common attacks. However, there are some limits to what it can do. You cannot install an old version of Admin Tools on an obsolete version of WordPress and expect that site to be impregnable by hackers. Old versions of WordPress most certainly have known security issues which, from the point of view of a web application firewall, look like legitimate requests. These attacks cannot be addressed unless the vulnerable WordPress core or third party extension code itself is updated. That is why we will only officially provide support to the latest WordPress version. There's no point trying to secure an out of date site.

Finally, please keep in mind that your site evolves over time. You may have to adjust your Admin Tools settings over time. Sometimes updating a third party plugin will break something because its author is doing something ill-advised that Admin Tools protects you against (yes, some developers manage to make their software behave in the same way malware does, mainly because they are unaware of those malicious patterns). Sometimes you may install something new which needs a few adjustments in the protection to make it work. This is all normal. Security is something you do, not something you install and forget about it.

2. Server environment requirements

In order to work, Admin Tools requires the following server software environment:

- WordPress and PHP version compatibilities are detailed in our Compatibility page [<https://www.akeeba.com/compatibility.html>]. We only recommend using the latest WordPress version [<https://wordpress.org/download/>] with an actively supported version of PHP [<http://php.net/supported-versions.php>].
- MySQL 5.0.42 or later. MySQL 5.6 or later recommended. You can use compatible database servers, such as MariaDB 10.1 or later.
- For the PHP File Change Scanner feature: Minimum 24MB of PHP `memory_limit` (sufficient *only* for smaller web sites, without many plug-ins and modules running). More is better. 32MB to 64MB recommended for optimal performance on large sites. 128MB is recommended for sites containing deep-nested directories with thousands of files.
- The cURL PHP module must be installed for Admin Tools to be able to find and install updates.

As far as the browser is concerned, you can use any modern version (i.e. published within the last year) of Microsoft Edge, Safari, Opera, Firefox or Google Chrome. We no longer support Internet Explorer; our software will display incorrectly or not work at all on this old, buggy and obsolete browser.

In any case, you must make sure that JavaScript is enabled on your browser. If you are using AVG antivirus, please disable its Link Checker feature (and reboot your computer) as it is known to cause problems with several JavaScript-based web applications.

You are very strongly advised to disable Internet firewalls, antivirus applications and browser extensions which interfere with the site's loading such as script blockers (such as NoScript) and ad blockers (such as AdBlockPlus) *only for the domains of your sites*. Remember that these applications and browser extensions are designed to protect you against third party sites. As a result they are very aggressive and WILL break your own sites. We can't do anything about it: your computer and your browser are under your control alone.

3. Installing Admin Tools

Installing Admin Tools for WordPress is simple. The first thing you need to do is to download the plugin from our site. It's a ZIP file. You now have two different ways of installing it on your WordPress site.

Using WordPress' plugin installer

Go to your site's wp-admin section and click on Plugins, Add New. Select Upload from the top of the page. Click on the file selection area and select the ZIP file you downloaded from us. Then click on the Install Now button.

Important

This may not work if your server has an relatively low upload size limit or if it's too slow. In this case please follow the manual installation procedure below.

Manual installation

Extract the ZIP archive you downloaded from us. Connect to your site by FTP and go into the directory `wp-content/plugins`. Upload the extracted directory `admintoolswp` inside it. This means that you will now have a directory `wp-content/plugins/admintoolswp` on your site with Admin Tools' files.

Finally, log in to your site's administrator panel (wp-admin). Go to Plugins and activate the Admin Tools for WordPress plugin.

3.1. Updating to the latest version

Live update

The best way to determine whether there are updates available and installing them is the Live Update feature, if your server supports it. Whenever you visit the Admin Tools main page, it will automatically check for the existence of an updated version and it will notify you. Clicking on the notification icon allows you to perform a direct update without further interaction. Do note that if your server is protected by a firewall you'll have to enable port 80 and 443 TCP traffic to `www.akeeba.com` and `cdn.akeeba.com` for this feature to work properly.

Manual update method

You can easily check for the latest published version of the Admin Tools application by visiting <https://www.akeeba.com/downloads.html>. The page lists the latest versions of our software and lets you download them as well. You can check the version number against the information which appears on the right-hand pane of your Admin Tools Control Panel. If your release is out of date, simply download the ZIP package of the latest release to your computer.

You can update **Admin Tools for WordPress** manually doing the following:

1. Download the latest version of Admin Tools' installation ZIP file.
2. Extract the contents of the ZIP file on your computer. You will see an extracted folder named `admintoolswp`.
3. Upload the files from the extracted `akeebabackupwp` folder into your site's `wp-content/plugins/admintoolswp` folder, using FTP or SFTP, overwriting your existing files. Please note that the name of the folder on your site *may* be different than `admintoolswp`, e.g. `admintoolswpcore`, `admintoolswp (1)` or something similar. It depends on how you installed the plugin.
4. Log in to WordPress' wp-admin and access Admin Tools for WordPress to automatically complete the update process. There is no message when the process completes. You just see the main page of Admin Tools for WordPress (this means the update succeeded).

Warning

Attention Mac OS X users! By default, most Mac OS X FTP/SFTP applications will delete and overwrite entire directories. This means that you may lose data stored inside the plugin's directory. We recommend using FileZilla (free, not very secure), CyberDuck (free, much more secure) or Transmit (paid), as they will never perform directory deletion without your knowledge.

4. Upgrading from Core to Professional

Upgrading from Admin Tools Core to Admin Tools Professional is by no means different than doing a manual update as described above. Simply upload the Admin Tools Professional files over the same or an earlier version of Admin Tools Core. Done!

5. Requesting support and reporting bugs

Support can be provided only to subscribers and only through our site's Support section. If you already have an active subscription which gives you access to the support for Admin Tools for WordPress you can request support for it through our site. You will need to log in to our site and go to Support, Admin Tools for WordPress and click on the New Ticket button. If you can't see the button please make sure you have an active subscription that gives you access to Admin Tools for WordPress support. If you do and still don't see the button please use the Contact Us page to let us know of the ticket system problem and remember to tell us your username.

If you want to report a bug, please use the Contact Us page of our site. You don't need to be a subscriber to report a bug. Please note that unsolicited support requests sent through the Contact Us page will not be addressed. An issue is not a bug unless it can be reliably reproduced *on multiple sites*. Please make sure you include clear instructions on reproducing the issue. If the issue cannot be reproduced it's not a bug report, it's a support request.

Important

Support cannot be provided over Twitter, Facebook, email, Skype, telephone, the WordPress plugin directory, the WordPress forum, our Contact Us page or any other method except the Support section on our site. We also cannot take bug reports over any other medium except the Contact Us page and the Support section on our site. Support is not provided to non-subscribers; if you are using the Core version you can request support from other users in any forum of your choosing, just like you would for WordPress itself. We have to impose those restrictions in support to ensure a high level of service and quality. Thank you for your understanding.

6. Quick Setup

Important

This section is written with Admin Tools Professional in mind. If you are using Admin Tools Core you will not see all of these features.

Tip

You can quickly apply all of the following settings by using the Quick Setup Wizard page of Admin Tools. A prominent link to that page will appear at the top of your site's administrator (wp-admin) section as a standard WordPress notification until you run the wizard or manually configure Admin Tools through the Configure WAF and .htaccess Maker pages or import a configuration from the Import Settings page.

While the Quick Setup documentation section and the Quick Setup Wizard feature will help you to get started with basic protection for your site it is very strongly advisable that you read the documentation in its entirety. It will help you understand the different ways Admin Tools protects your site and the impact each option may have to your site's operation.

Warning

If you have already configured Admin Tools and wish to change its configuration you are NOT supposed to use the Quick Setup Wizard. In fact, this is not supported and we will provide no support if you choose to do that. Instead go to Admin Tools, Web Application Firewall, Configure WAF to configure the security protection settings or Admin Tools and .htaccess Maker to configure the server-level protection settings.

The fundamental functionality of Admin Tools is to allow you to secure your site. However, setting up your site's security does require some tweaking, as each site has different structure and needs than the next. When you first install Admin Tools Professional you may feel a bit overwhelmed by the abundance of security options. Well, the good news is that setting it up is not even half as hard as it looks! The Quick Setup Wizard lets you get up to speed very fast. It has the following options:

1. Administrator secret URL parameter If you enter "foobar" (without the quotes) in here, then you must access your site's backend as `http://www.example.com/wp-admin/?foobar` i.e. append a questionmark and the secret word. If you skip the `?foobar` part, you can't even see the login page. If you do not want to enable this feature please delete its contents and leave this field blank.

Important notes: This field will contain either your existing Administrator secret URL parameter (if you have already configured one) or a new, random one if there is no Administrator secret URL parameter already set up on your site. Do keep in mind that if you have disabled the Administrator secret URL parameter and you run the Quick Setup Wizard again a NEW, COMPLETELY RANDOM value will be shown in this field.

2. Password-protect WP administration This is designed to add an extra level of protection to your site's administrator (wp-admin) back-end, asking for a username and password before accessing the administrator login page or any other file inside the `wp-admin` directory of your site. It does so by using Apache `.htaccess` and `.htpasswd` files, so it won't work on IIS or NginX hosts.
3. Enter your email address in Send an email for all administrator login attempts. Admin Tools will be sending you an email whenever anyone tries to log in to your site's wp-admin as an Administrator. The minute you receive an email which wasn't triggered by a trusted person, you know you have to get your site off-line a.s.a.p. Do note that this is a very useful feature! It will send you an email even in the unlikely case that someone, for example, hacks your Wi-Fi, steals your login cookie and then uses your own Wi-Fi connection and login cookie to log in to your site.
4. Allow administrator access only to IPs in Whitelist will prevent anyone from accessing wp-admin unless they are coming from an IP address in the whitelist. Please only use this if your ISP assigns you a static IP. If you are on a dynamic IP, like most people, enabling this feature will only keep locking you out of your site all the time. If you are unsure set it to No.
5. Disable editing users' properties prevents any operation on users which would allow the creation of an Administrator user or the elevation of a user's privileges to Administrator status. You will not be able to edit Administrator users or create new Administrator users until you disable this feature!
6. Enable Web Application Firewall activates the security features which block malicious access attempts to your site.

7. Enable IP workarounds is only necessary when your site is behind a proxy server. While Admin Tools tries to detect the recommended setting for your site this cannot always be accurate. If you start getting locked out of your site and you see that all blocked access attempts seem to originate from the same IP address - which is different than the IP address you access your site from - you most definitely need to set this to Yes.
8. Automatically block repeat offenders blocks IPs raising repeated security exceptions on your site, i.e. we have strong reasons to suspect they are hackers. Please note that you may not want to enable this feature until you are sure everything is working smoothly, so that you don't accidentally block yourself out of your site.
9. Blacklist incorrigible offenders is an extension of the previous feature. If an IP address gets blocked automatically all the time it means that it's very likely not a user who screwed up but a hacker who tries hard to get into your site. Enabling this option will permanently blacklist their IP address so they don't bother you anymore.
10. Email this address on security exceptions. Enter your email address here to get email notifications about every blocked malicious access attempt. You should be aware that in case of a massive attack against your site you might get *plenty* of emails. This feature does not serve any real security purpose, it's basically there to make you and your clients feel good by receiving emails whenever something is blocked.
11. Optional but highly recommended, go to http://www.projecthoneypot.org/httpbl_configure.php and open yourself a Project HoneyPot account. After your registration, visit that URL again and you'll see something called "HTTP:BL key". Copy it and paste it into the Project HoneyPot HTTP:BL Key field. Project HoneyPot analyses data from a vast number of sites and positively identifies IPs currently used by hackers and spammers. This Admin Tools feature integrates with Project HoneyPot, examining your visitors' IP addresses. If they are in the black list (known hacker or spammer) they will be blocked from accessing WordPress.
12. Create a security tightening .htaccess is for advanced users who are using the Apache web server. This feature adds carefully curated directives to increase the performance and tighten the security of your site at the web server level - long before PHP, let alone WordPress, has the chance to run. This is a great line of defense but it may also cause problems with third party plugins. Please read the documentation to understand how it all works!

After applying all of the above protections, it is very likely that some of your site's functionality is no longer working or you can't access your site anymore. This is normal. The default settings are very restrictive by design. That's why you get a list of URLs with troubleshooting instructions. Make sure you print them out before you save the changes. If you get locked outside of your site or cannot access your site follow their instructions to regain access.

Chapter 2. Using Admin Tools

1. The Control Panel

The main page of the plugin which gives you access to all of its functions is called the Control Panel.

The Control Panel page

Admin Tools

You need to enter your Download ID
 You must enter your **Download ID** before you can update Admin Tools Professional. [If you don't know your download ID, please click here.](#)
 Paste your Download ID and press the button

GeoIP Database Maintenance
 Admin Tools finds the country and continent of your visitors' IP addresses using the MaxMind GeoLite2 Country database. You are advised to update it at least once per month. On most servers you can perform the update by clicking the button below. If that doesn't work on your server, please consult our documentation.

Security

- Emergency Off-Line
- Master Password
- Password-protect WP administration
- .htaccess Maker
- Malware detection
- Web Application Firewall

Tools

- Plugin params
- WordPress tools
- HTTPS Tools
- Repair & Optimise Tables
- URL Redirection
- Export settings
- Import settings
- Permissions Configuration
- Fix Permissions

Quick Setup

You should only run the Quick Setup Wizard once, when you first install Admin Tools. If you run it again it will override all

Updates
 Admin Tools version revB4BFE61 • [CHANGELOG](#)
 Copyright © 2017–2018 Nicholas K. Dionysopoulos / [Akeeba Ltd](#)

Exceptions Graph
 From
 1.0
 0.9
 0.8
 0.7
 0.6
 0.5
 0.4
 0.3
 0.2
 0.1
 0
 2018-02-27 2018-03-01

Exceptions per type

adminpw

Statistics

Last year	0
This year	2
Last month	1

The messages area

At the top of the Control Panel you can see one of several messages.

If there is an update available you will get a notification with a link to update Admin Tools. Clicking on it will take you to the Update page where you can apply the update.

If you are using Admin Tools Professional, our for-a-fee version, but have not yet entered your Download ID you will be given instructions on how to do it. The Download ID is necessary for receiving updates to the Professional version.

If Admin Tools detects that the IP you are currently using has been blocked automatically it will offer you the option to unblock it with the click of a single button.

Other informative messages may also appear in this area. We strongly advise you to read them carefully. We only show you messages when we believe you need to take some action with relevance to your site's security.

The main control panel (buttons) area

The left hand side of the main area of the page contains the main control panel. It consists of several groups of buttons. Each button corresponds to a feature available to Admin Tools. The rest of the documentation will describe each of these features in more detail.

The updates and statistics area

The right had side of the main area of the page contains the updates and statistics area.

Towards its top you can see the Admin Tools version information and the availability of updates. You can also review the changelog of the currently installed Admin Tools version.

Below that you will see the graphs showing the number of logged security exceptions (attacks Admin Tools Professional has protected you against), their distributions by type and a few statistics about them, e.g. how many exceptions have occurred in the last year, month, week, day and so on.

2. The Plugin Params page

This button, found in the Control Panel of Admin Tools, lets you set up options other than those pertaining to the security features of Admin Tools.

The Plugin Params page

The screenshot shows the 'Plugin params' settings page in the Admin Tools plugin. The page has a teal header with the title 'Settings'. Below the header, there are five settings, each with a label, a control, and a description:

- Maximum security exceptions log entries:** A text input field containing '0'. The description states: 'Specify the maximum number of entries to keep in the security exceptions log. Excess records will be deleted. Use 0 to turn off this feature and keep all security exceptions log entries (recommended). Note: if you have thousands of old entries it will take a while for Admin Tools to remove all of the old entries. Old records are deleted in 100 record batches on each page load for performance reasons.'
- Long Configure WAF page:** A toggle switch with 'Yes' and 'No' options. The 'No' option is selected. The description states: 'When this option is disabled (default) the Configure WAF page will be shown using tabs. When this option is enabled the Configure WAF page will be shown in the old format: one long page.'
- Show graphs and statistics:** A toggle switch with 'Yes' and 'No' options. The 'Yes' option is selected. The description states: 'Display graphs and statistics about security exceptions (Professional release only)'. The 'Yes' option is highlighted in green.
- Enable anonymous PHP, MySQL and WordPress version reporting:** A toggle switch with 'Yes' and 'No' options. The 'Yes' option is selected. The description states: 'Help us improve our software by anonymously and automatically reporting your PHP, MySQL and WordPress versions. This information will help us decide which versions of WordPress, PHP and MySQL to support in future versions. Note: we do NOT collect your site name, IP address or any other directly or indirectly unique identifying information.' The 'Yes' option is highlighted in green.
- Timezone for emails:** A dropdown menu with 'UTC' selected. The description states: 'All dates and times in the emails sent by Admin Tools to warn you about potential security issues will be expressed in the selected timezone. Default: UTC'.

At the bottom of the settings area, there is a teal bar labeled 'Updates'.

Settings

Maximum security exceptions log entries

Admin Tools keeps track of the malicious requests it has blocked (security exceptions) in a database table. Over time this time can grow very big and have a performance impact on your site. Setting this value to a number higher than zero will prevent the table from growing big. Only up to this many log entries will be kept at one time. Older log entries will be automatically deleted.

Note: if you have thousands of old entries it will take a while for Admin Tools to remove all of the old entries. Old records are deleted in 100 record batches on each page load for performance reasons.

Long Configure WAF page

When this option is set to No, the Configure WAF page uses tabs to display the different option groups. When this option is set to Yet the Configure WAF page is one very long form. Each group simply has a header before its options.

If you are using a very old browser, e.g. Internet Explorer 11, or you have disabled JavaScript you may want to enable this option. The tabs only work on modern browsers with JavaScript enabled.

Show graphs and statistics

Display graphs and statistics about security exceptions (Professional release only) in the Control Panel page. This is useful visualisation to see the rate at which your site is being attacked. Lack of attacks does not mean that your site is at risk! Quite the contrary, it means that at this time period hackers have not been trying to attack your site.

Enable anonymous PHP, MySQL and WordPress version reporting	<p>Help us improve our software by anonymously and automatically reporting your PHP, MySQL and WordPress versions. This information will help us decide which versions of WordPress, PHP and MySQL to support in future versions.</p> <p>We do NOT collect your site name, IP address or any other directly or indirectly unique identifying information. The information collected is anonymized and we have taken extra care to make deanonymization impossible for us, i.e. we can NOT trace that information back to a specific site or user account.</p>
Timezone for emails	<p>All dates and times in the emails sent by Admin Tools to warn you about potential security issues will be expressed in the selected timezone.</p> <p>Default: UTC (a.k.a. GMT)</p>

Updates

Download ID	<p>Only for the Professional edition. If and only if you are using the Professional release you have to specify your Download ID for the live update feature to work properly. You can get your Download ID by visiting our site, logging in and clicking My Subscriptions. Your Download ID is printed below the list of subscriptions. Filling in this field is required so that only users with a valid Professional subscription can download update packages, just as you'd expect from any commercial software.</p>
-------------	---

Note

Users of Admin Tools Core do not need to supply this information.

Minimum stability	<p>Choose the minimum stability of the updates. If you are unsure set this to Stable. This is the safest option.</p> <p>If you want to help us provide better software set this to Beta. Our beta versions are very well tested and usually have only minor issues - they're not stable but they're very close and don't cause any trouble. We run our betas on <i>our</i> production sites but we want you to only use them on your least important sites.</p> <p>If you are really adventurous you can try Alpha versions but there are no guarantees about their stability and performance.</p>
-------------------	--

3. Fixing the permissions of files and directories

As any web site administrator knows, file and directories permissions are the first gatekeeper on the way to having a site hacked. Having 0777 permissions lying around is a big mistake and could prove fatal to your site. For more information, read my blog post [<http://www.dionysopoulos.me/blog/777-the-number-of-the-beast>]. Ideally, you should only have 0755 permissions for your directories and 0644 for your files.

On other occasions, we have all run across a misconfigured server which gives newly created files and directories impractical permissions, like 0600. This has the immediate effect that newly uploaded or created files are not accessible from the web. Fixing those permissions is a tedious process, hunting down the files with FTP and changing their permissions manually. Ever so often this becomes so tedious that we are tempted to just give 0777 permissions to everything and get done with it. Big, fatal mistake.

The solution to those permissions problems is the Fix permissions tool of Admin Tools. Its mission is as simple as it gets: it will give all your directories 0755 permissions and all of your files 0644 permissions. Obviously, this only has effect on Linux, Mac OS X, Solaris and other hosts based of UNIX-derivative Operating Systems, i.e. everything except servers running on Windows.

Note

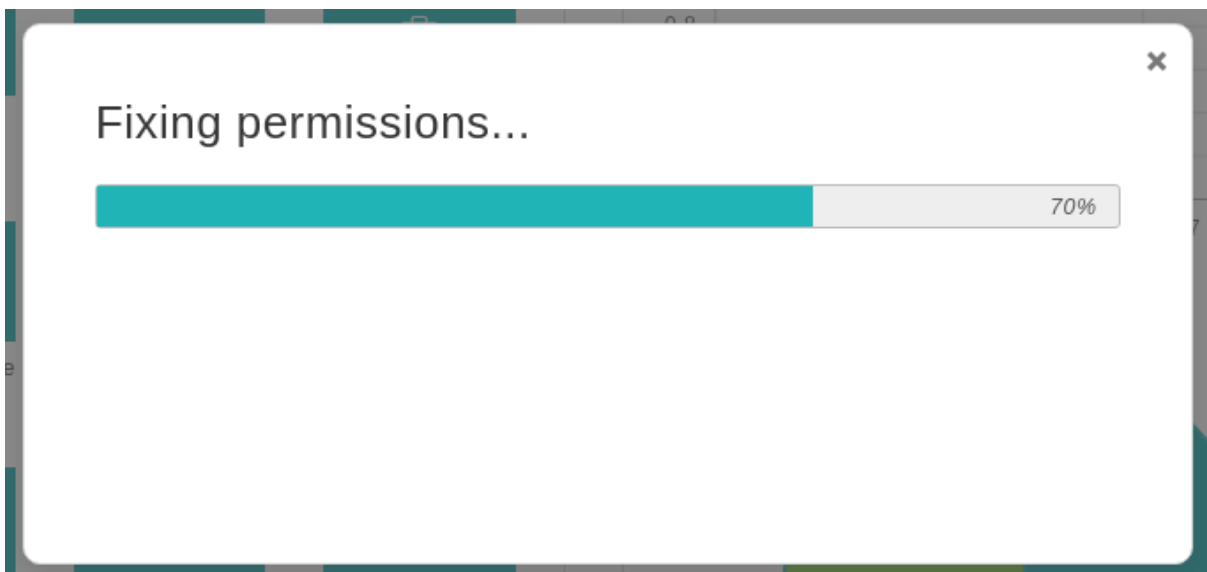
You can customize the permissions per folder and file using the Permissions Configuration page.

Warning

It is possible that —if you select the wrong kind of permissions in the Permissions Configuration page— you will be locked out of your site and will not be able to access it over FTP or your hosting panel's file manager. If this happens, please contact your host and ask them to fix the permissions of your site.

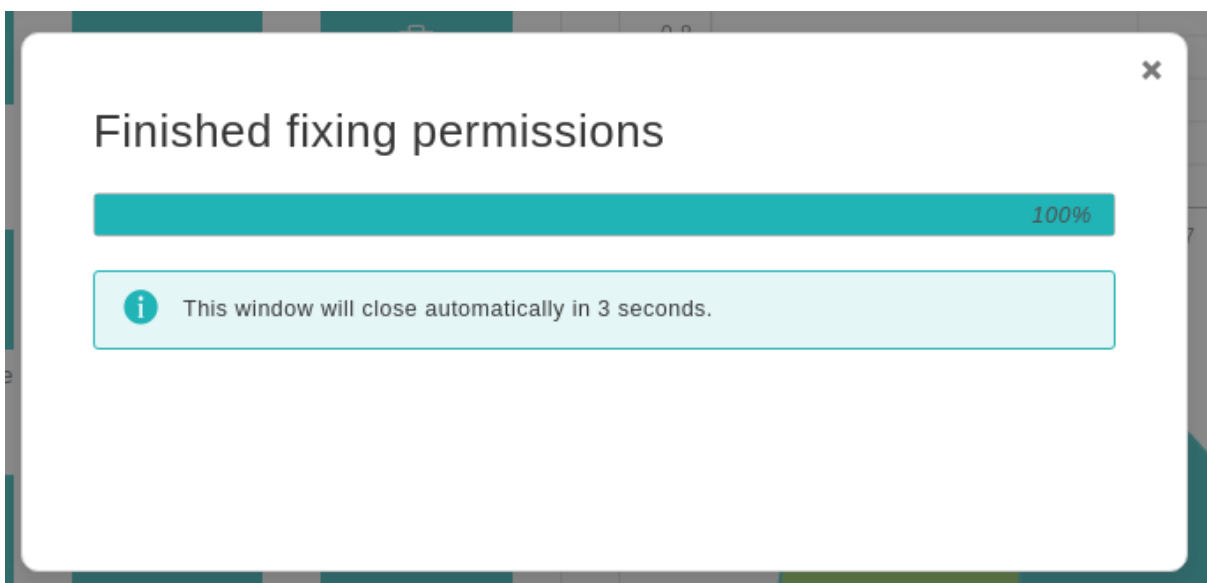
When you click on the Fix Permissions tool you are going to see the "Fixing Permissions..." pop-up window with a progress bar filling up as Admin Tools is changing the permissions of all your directories and files.

Fixing permissions



When it's over the progress bar will fill up and the title of the page changes to "Finished fixing permissions":

Finishing fixing permissions



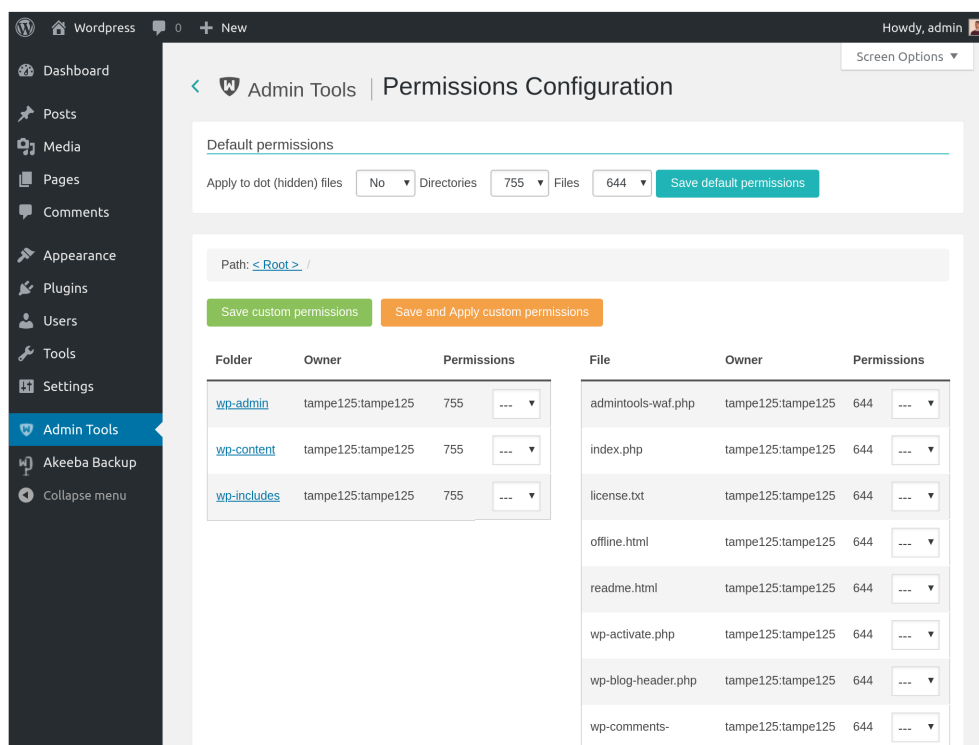
No permissions have been changed on my site. Why?

It's a matter of ownership. If you are on a host which doesn't use suPHP, your files and directories are owned by a different user than the one the web server is running under. In this case the only option is to use an FTP client to manually change the permissions.

3.1. Configuring the permissions of files and directories

By default, Admin Tools will apply 0755 permissions to all of your directories and 0644 permissions to all of your files. However, this isn't always desirable. Sometimes you want to make configuration files read-only (0400 or similar permissions) or give a directory wide-open (0777) permissions. While this is not recommended, it may be the only option on some shared hosts for several extensions to work. Most notably, some extensions need to be able to append to files —e.g. Akeeba Backup needs to append to its log and backup archives— which is impossible to do over FTP and, therefore, requires wider permissions. With Admin Tools you can do that using the Permissions Configuration button in the plugin control panel.

Configuring the permissions



When you launch this feature you see a page split in three sections.

The top section, titled Default permissions, allows you to configure the permissions which will be applied if nothing different is configured. Use the drop-down lists to select the default permissions for directories and files (the default setting is 755 and 644 respectively), then use the Save default permissions button to apply the setting.

The middle section shows the path to the currently selected directory and allows you to quickly navigate through the folders by clicking on their names.

The bottom section is split in two panes, Folders and Files. Each pane lists the folders and files inside the current directory. Clicking on the name of a folder will navigate inside that folder. There are three columns next to each

folder. The first displays the current owner (user:group format). The second displays the current permissions of that directory in the file system. The final column contains is a drop down list. The default setting, represented by dashes, means that there is no specific preference for this folder/file and the default permissions will be applied to it. If you select a customized permissions setting remember to click the Save custom permissions button before navigating to another folder or returning to the control page, otherwise your settings will be lost.

Important

None of these customized permission settings are applied immediately. You will need to launch the Fix Permissions feature for them to be applied. Return to the Control Panel page where you can find this button.

Alternatively, you can click on the Save and Apply custom permissions button to immediately save and apply all custom permissions you see on this page. If you don't see the permission changing, please take a look at the previous section of this user's guide for more information on what you have to do.

4. Emergency Off-Line Mode

Important

This feature uses .htaccess files which are only compatible with Apache, Litespeed and a very few other web servers. Some servers (such as NginX and IIS) are incompatible with .htaccess files. If we detect a known to be incompatible server type this feature will not be shown at all in Admin Tools' interface. It should be noted that even if you do see it in the interface it doesn't necessarily means that it will work on your server. This depends on your server's capabilities. If you are unsure or believe it doesn't work please consult your host.

If you have reasons to believe that your site is under active attack you can use this feature to cut off all access to your site at the web server level. Only your current IP address will have access to the site. The Emergency Off-Line Mode feature carries out the following actions:

- It creates —if it doesn't already exist— a static HTML page named offline.html in your site's root. This page contains the offline message to show to visitors.
- It creates a backup copy of your site's .htaccess file, if there was one, under the name .htaccess.eom.
- Finally, it creates a .htaccess file which will temporarily redirect all access attempts to the offline.html page. It will allow only your IP address to have access to the site.

In order to put your site in Emergency Off-Line Mode, simply click on the Emergency Off-Line button in Admin Tools' Control Panel page. This will get you to the following page:

The Emergency Off-Line Mode page

WordPress Development 1 0 + New Howdy, nicholas

Admin Tools | Emergency Off-Line

Set Offline

Clicking the button above will set your site to the Emergency Off-Line mode. In this mode nobody will be able to access your site except visitors coming from your current IP address. Should your Internet connection drop or your IP change for any reason, the only way to access your site will be removing the .htaccess file from your site's root using FTP. Please read this very carefully and print this page for reference.

In case this automated tools fails to create the .htaccess file on your site's root, please remove your current .htaccess (if any) and create a new .htaccess file with the following contents:

```
RewriteEngine On
RewriteBase /
RewriteCond %{REMOTE_HOST} !127\.0\.0\.1
RewriteCond %{REQUEST_URI} !offline\.html
RewriteCond %{REQUEST_URI} !(\.png|\.jpg|\.gif|\.jpeg|\.bmp|\.swf|\.css|\.js)$
RewriteRule (.*) offline.html [R=307,L]
```

Thank you for creating with [WordPress](#). Version 4.9.4

Clicking the Set Offline button will attempt to perform the steps outlined above. Should any of those steps fail, for example due to insufficient file permissions, you can still put your site in Emergency Off-Line Mode by taking out the following procedure:

1. Keep a copy of your site's .htaccess file, e.g. renaming it to htaccess .bak.
2. Create a new .htaccess file in your site's root with its contents being what displayed in the last part of the Emergency Off-Line Mode page.

If your Internet IP address changes before you disable the Emergency Off-Line Mode —i.e. your connection drops or you switch to another computer which connects to the Internet through a different Internet router— you will be unable to log in to your site. In this case, follow these steps:

1. Using an FTP application of your liking remove the .htaccess file, or upload a blank .htaccess file overwriting the old one.
2. Go to your site's administrator back-end and relaunch Admin Tools' Emergency Off-Line mode. Clicking on the Set Offline button will create a new .htaccess file with your current IP address. Your backup .htaccess .eom file will not be overwritten.

If you want to set your site back on-line, just visit the Emergency Off-Line page and click on the Set Online button. This will replace the off-line .htaccess file with the contents of the .htaccess .eom backup file and remove the backup file. If this doesn't work, follow this manual procedure:

1. Using an FTP application of your liking remove the .htaccess file, or upload a blank .htaccess file overwriting the old one.
2. Rename the .htaccess .eom backup file back to .htaccess

Will I be able to use FTP or my host's control panel file management when I enable this feature?

Of course! This feature only protects web (HTTP/HTTPS) access. It can't and won't touch FTP access or your hosting control panel's file management.

Should I use the emergency off-line mode when I want to temporarily put my site off-line, e.g. for maintenance?

It's not recommended. This feature is designed for emergencies. Also note that when you use it nobody can use permalinks (URLs which do not contain `index.php` in them), not even you.

The `offline.html` page Admin Tools creates is horrid. Can I change it?

Thank you for asking. It's horrid on purpose (we want you to provide a page which better fits your brand and doesn't look like every other site's out there). Of course you can change it. Simply upload an `offline.html` of your liking to your site's root. You can link to JPG, GIF, PNG, BMP, SWF, CSS and JS files —on the same or a different server— from inside the HTML of this file. Do not try to link to other file types, it will not work.

Won't the redirection to `offline.html` screw up my SEO ranking?

No. The redirection to `offline.html` is made using the 307 HTTP status code which tells search engines that this redirection is temporary, they should not index the page now, but come back later when the problem will have been restored.

Help! I have been locked out of my site! Fix it!

Read a few paragraphs above. You just have to remove a file using FTP.

The redirection doesn't work! I test it from another device connected on the same WiFi / network and I can still see my site!

Well, yes, that's the whole point. You are supposed to be able to see your site only from your IP address. Which is shared by all devices on the same network.

If you want to test that this feature really works please try accessing your site from another computer, connected to the Internet from a different router / network connection. One good idea is to use your cellphone, as long as it connects to the Internet over a cellular connection (e.g. 3G or 4G), not over WiFi. If you did that and still don't see the redirection happening, make sure that your server supports `.htaccess` files and that it has `mod_rewrite` enabled. Some servers, like IIS, do not support `.htaccess` files at all. If this is the case, consult your host about taking your site completely off-line.

Help! As soon as I clicked on "Put Offline" I got a white page or Internal Server Error 500 page.

Don't panic! You have a really old version of Apache —1.3 or 2.0— which doesn't support a feature used in the `.htaccess` file generated by Admin Tools. You can easily work around this issue by editing the `.htaccess`

file in your site's root, using an FTP application. Replace [R=307,L] in the last line with [R,L] (that is, remove the =307 part) and save back the file. That's all.

My Internet connection drops all of the time. Will I get continuously locked out of my site if I use this feature?

It depends. If you have a static IP address, no, you will never get locked out. If you have a dynamic IP address, most likely yes. Some ISPs will assign you the same IP address if your connection only dropped for a couple of minutes. Other ISPs will change your IP address every hour, even if your connection never drops. It all depends on how your ISP assigns IP addresses to its clients. The only way to find out is the hard way: trial and error.

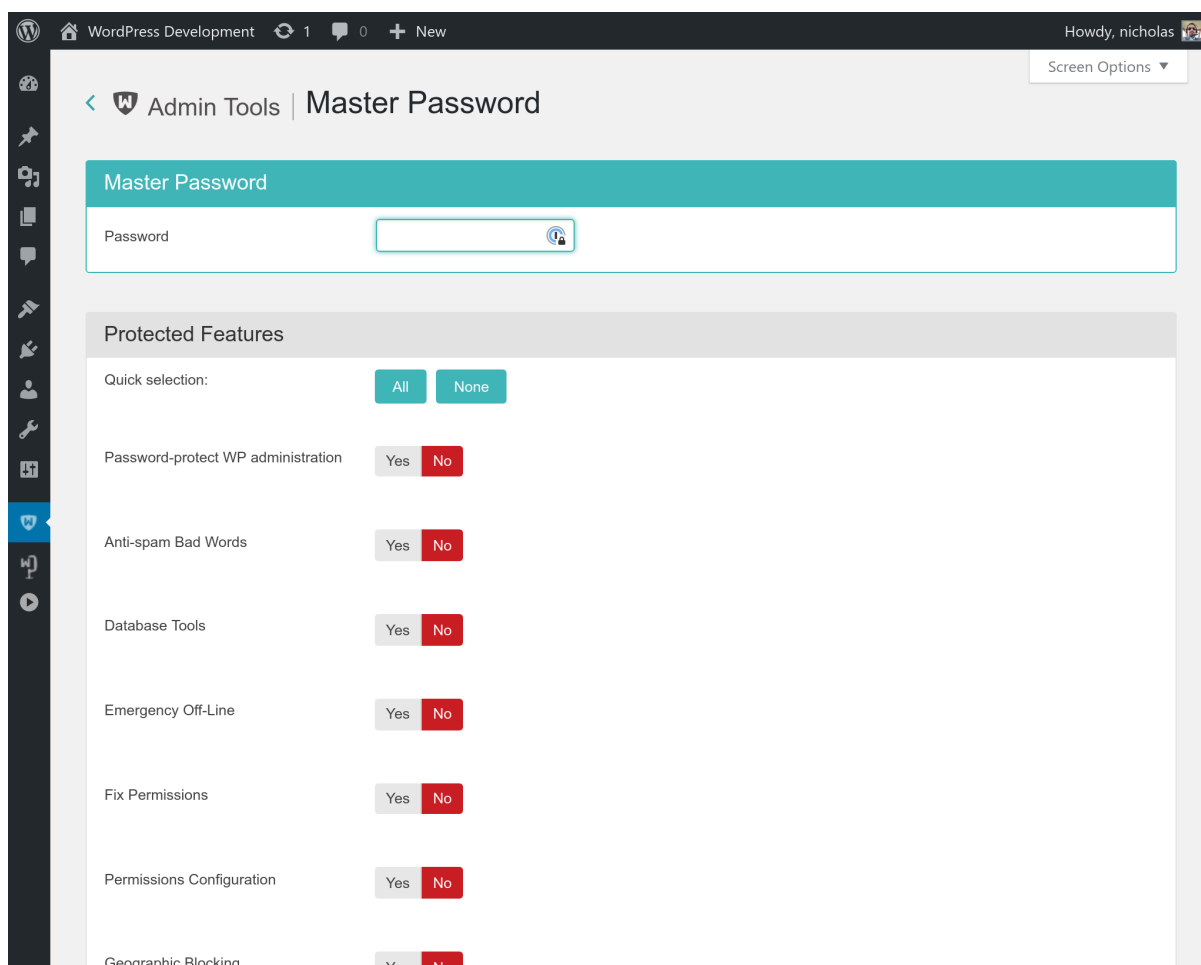
5. Protecting Admin Tools with a password (Master Password)

Warning

THIS IS NOT A SECURITY FEATURE. THE MASTER PASSWORD IS STORED UNENCRYPTED IN THE SITE'S DATABASE. We consider this feature as a simple way for you to prevent your clients from modifying configuration parameters which could break their own site. **THIS FEATURE IS NOT DESIGNED TO PREVENT A MALICIOUS PERSON WHO HAS INFILTRATED YOUR SITE FROM ACCESSING ADMIN TOOLS.**

Sometimes you are not the sole administrator of a website, for example when there is a large administrative team or when you build the website for a client. In such cases you do not need everyone with administrative access to be able to modify Admin Tool's settings. Instead of giving you the traditional "all or nothing" access control implied by WordPress user roles, Admin Tools allows you to control access to any or all of its features using a "master password". The idea is that before any user is able to use one of the protected features, they have to supply the "master password" in Admin Tools' control panel page.

The Master Password page



When you click on the Master Password button in the Control Panel you get to the Master Password page where you can set both the password and select which features to protect.

The top area of the page allows you to set a Master Password. If you want to disable password protection altogether simply leave it blank.

The bottom area of the page lets you select which features will be protected. Set the radio button next to each feature you want to protect to "Yes" before clicking on the Save Changes button. Features marked as "No" will be accessible by all administrator users. Features marked with "Yes" will only be available to users who enter a valid password in the Control Panel page. This means that even Administrators will not be able to access the protected features without supplying a valid password.

If you want to quickly protect all features, click on the All button above the list. Conversely, clicking on the None button will disable Master Password protection on all features.

I have forgotten my password. Now what?

The only way to find out your password is to directly read it from the database. Use your host's database management tool —usually it's phpMyAdmin— to list the contents of your site's `wp_admintools_storage` table (where `wp_` is your site's prefix). Find the only record in the table (the `key` value is "cparams") and take a peek at the contents of the `value` column. It contains a long text. At some point you will see something like "masterpassword" : "mypassword". The `mypassword` part is your master password.

6. Protect your WordPress administration with a password

Important

This feature uses .htaccess files which are only compatible with Apache, Litespeed and a very few other web servers. Some servers (such as NginX and IIS) are incompatible with .htaccess files. If we detect a known to be incompatible server type this feature will not be shown at all in Admin Tools' interface. It should be noted that even if you do see it in the interface it doesn't necessarily mean that it will work on your server. This depends on your server's capabilities. If you are unsure or believe it doesn't work please consult your host.

The Password-protect WP administration tool of Admin Tools is designed to add an extra level of protection to your site's wp-admin, asking for a username and password before accessing the login page or any other file inside the wp-admin directory of your site. It does so by using Apache .htaccess and .htpasswd files, so it won't work on IIS hosts.

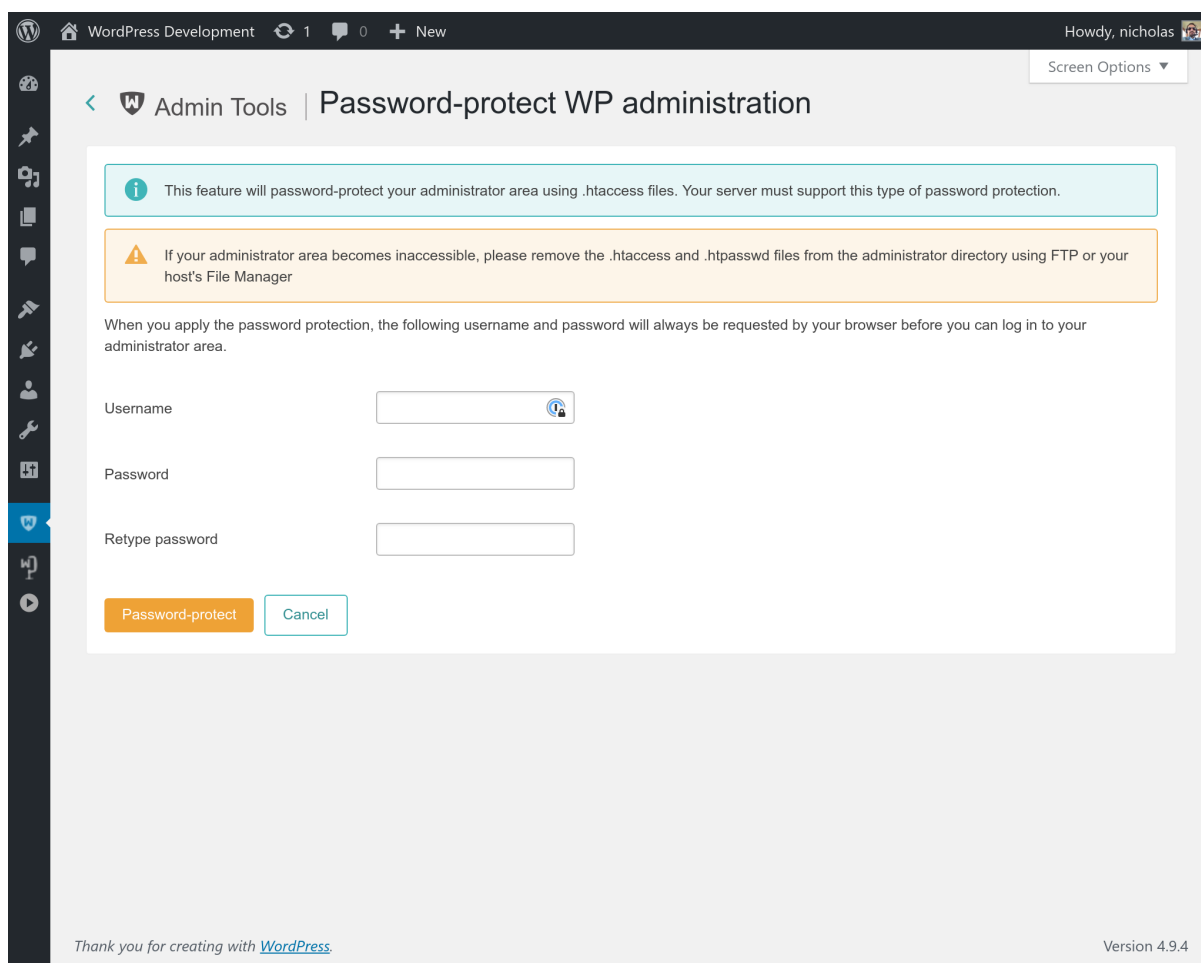
Important

Some prepackaged server bundles, such as Zend Server, and some live hosts do not allow using .htaccess files to password-protect a directory. If it is a local server, edit your httpd.conf file and modify all AllowOverride lines to read:

```
AllowOverride All
```

If you are on a live host, please consult your host about the possibility of them allowing you to use this feature on your site.

Password-protect Administrator



If you are on a server running on Windows™, you are receiving a warning at the top of the page stating that the password will be stored to disk unencrypted. This is done due to the lack of the system-wide crypt function on the Windows platform, which causes Apache to understand password only if they are unencrypted or encrypted with a non-standard encryption scheme which does not exist in PHP.

Warning

If you password your administrator directory on a Linux system and then restore your site on a Windows server (typical live to local site restoration) you will be receiving a blank page or an Internal Server 500 when accessing the site. This is normal and expected. All you have to do is to remove the `.htaccess` and `.htpasswd` files from your wp-admin directory after restoring the site.

In order to apply the password protection, simply enter a desired username and password and click on the Password-protect button. After a few seconds your browser will ask you to supply the username and password you just specified. This will also happen each and every time anybody tries to access the administrator back-end of your site. In other words, you have to share the username and password with all back-end users of your site.

If you wish to remove the password protection you can either remove both the `.htaccess` and `.htpasswd` files from your wp-admin directory, or click on the Remove Password Protection button.

500 Internal Server Error when enabling this feature

If after applying the password protection you immediately receive a blank page or an Internal Server Error 500 instead of a password prompt, your server is not compatible with the password protection scheme.

In this case, the only way to gain access to your site's administrator back-end is to remove the `.htaccess` and `.htpasswd` files from your `wp-admin` directory using an FTP application or the File Manager in your site's hosting control panel. If in doubt, consult your host about how you can do that before trying to apply the password protection.

If those files do not show up in your FTP client, please create two blank files with those names and upload them to your site, overwriting the existing (but invisible) ones. This will remove the password protection so that you can regain entrance to your administrator back-end.

404 Not Found error page or WordPress error page when enabling this feature

Long story cut short: ask your host to disable Apache custom error pages for HTTP status codes 401 and 403.

But why does this happen? (Optional, detailed information; you don't have to read the next paragraphs).

When you enable password protection all you're doing is create a `.htaccess` file. This tells Apache, your web server, that the `wp-admin` directory is password protected. The next time your browser tries to access anything in that directory it has to send an HTTP Basic Authentication header that contains your username and password. If it doesn't, Apache returns an HTTP 401 status which, in turn, instructs the browser to ask you for the username and password (and then store it in its authentication cache for the browsing session). This is how your browser knows it needs to ask you for a username and password.

However, HTTP 401 is technically an HTTP error status. Apache has a feature called custom error pages. Depending on the HTTP error status returned (all 4xx and 5xx codes) you can configure Apache to return a static HTML page with custom content to the browser when it sends the error code. This holds true even for the 401 status described above. **The real cause of the problem you are facing is that the configured custom error page does not exist.** This causes Apache to internally report the file as missing. This breaks the authentication flow and would normally trigger a 404 Not Found error page.

WordPress' `.htaccess` file always asks Apache to redirect missing files to its `index.php` file. That's how permalinks work: the URL is not a real file, Apache hands it over to WordPress and WordPress figures out which post or page to display. If it doesn't know what to do with the URL, like in this unfortunate case, WordPress displays its 404 error page.

When you disable custom error pages for the 401 error code you let Apache communicate that status directly to the browser without WordPress interfering. This lets the password protection work properly. FYI, the aforementioned error will also take place if you use your hosting control panel's directory password protection feature. It is not caused by Admin Tools. It is caused entirely by your server's configuration. Also note that most hosts do let you define and reset custom error pages through the hosting control panel.

I used that and my public site is now asking for a username and password

You have a plugin which has placed its files inside the `wp-admin` folder of your site. This is against WordPress best practices. Check your browser's console to find the offending plugin and report it to the WordPress Plugin Directory.

7. The `.htaccess` maker

Note

This feature is only available in the Professional release

Warning

This feature is only available on servers running the Apache web server. If your server is using IIS or NginX the button to launch this feature will not be shown. If you are using Lighttpd, Litespeed or any

other server software you will see a button to launch this feature but this feature may not have any effect. If unsure please consult with your host about their server's support of .htaccess files.

One of the most important aspects of managing a web site hosted on an Apache server is being able to fine-tune your .htaccess file. This file is responsible for many web server level tweaks, such as enabling the use of permalinks, blocking access to system files which should not be accessible from the web, redirecting between pages based on custom criteria and even optimising the performance of your site. On the downside, learning how to tweak all those settings is akin to learning a foreign language. The .htaccess Maker tool of Admin Tools is designed to help you create such a file by utilizing a point-and-click interface.

Important

Some prepackaged server bundles and some live hosts do not allow using .htaccess files to override server settings. If it is a local server, edit your `httpd.conf` file and modify all `AllowOverride` lines to read:

```
AllowOverride All
```

If you are on a live host, please consult your host about the possibility of them allowing you to use this feature on your site.

Tip

If you ever want to revert to a "safe default", just set all of the options on this page to "Off" and click on "Save and create .htaccess". This will remove our custom code from your .htaccess file.

If you have manually edited the file and remove the special markers used by WordPress and / or Admin Tools to mark their sections of the file please delete the .htaccess file completely. Then go to Settings, Permalinks, choose another option and click on Save. Repeat that, this time selecting the option that was there before and click again on Save. If you are unsure please search "reset WordPress .htaccess" on your favorite search engine. There are hundreds of articles out there explaining how this works.

The bottom part of the .htaccess maker page contains the standard buttons you'd expect:

- Save Changes will save the changes you have made in this page's options without actually updating the .htaccess file. This should be used when you have not decided on some options yet.
- Save and create .htaccess is the logical next step to the previous button. It not only saves the changes you made, but also updates your site's .htaccess file on the server. If you already had a .htaccess file on your site, it will be saved as `.htaccess.admintools` before the file is updated, allowing you to go back to a safe state quickly.
- The Cancel button takes you back to the Control Panel page.

The rest of the page contains several panes with different options, described below. Before you change anything please read and understand the following warning. It is vital to not getting locked out of your site.

Warning

Depending on your web server settings, some of these options may be incompatible with your site. In this case you will get a blank page or an Internal Server Error 500 error page when trying to access any part of your site. If this happens, you have to replace the .htaccess file in your site's root directory using an FTP application or the File Manager feature of your hosting control panel. Remember that your old and working .htaccess file is saved as `.htaccess.admintools` before any changes are applied. You can rename that file back to `.htaccess` to revert to the last known good state. If you are unsure how this works, please consult your host before trying to create a new .htaccess file using this tool.

Some prepackaged server environments, like WAMPserver, do not enable Apache's `mod_rewrite` module by default, which will always result in an Internal Server Error upon applying the .htaccess file. Then again, these do not work with WordPress out of the box, unless you had completely removed the .htaccess

file that ships with WordPress in the first place. If this is the case you are strongly suggested to enable `mod_rewrite` on your installation. On WAMPserver you can click on its tray icon, go to Apache, Modules and make sure `rewrite_module` is checked. On other server environments you have to edit your `httpd.conf` file and make sure that the `LoadModule mod_rewrite` line is not commented out (there is no hash sign in front of it). Once you do either of these changes, *you must restart your server* for the change to become effective.

We strongly suggest that you begin by setting all options to No and then enable them one by one, creating a new `.htaccess` file after you have enabled each one of them. If you bump into a blank or error page you will know that the last option you tried is incompatible with your host. In that case, remove the `.htaccess` file, set the option to No and continue with the next one. Unfortunately, there is no other way than trial and error to deduce which options may be incompatible with your server. **This is exactly what we do on servers we have not set up ourselves.**

7.1. Basic Security

Basic security

Basic security

Disable directory listings (recommended)	<input type="radio"/> Yes <input checked="" type="radio"/> No
Protect against common file injection attacks	<input checked="" type="radio"/> Yes <input type="radio"/> No
Disable PHP Easter Eggs	<input checked="" type="radio"/> Yes <input type="radio"/> No
Block access to <code>wp-config-sample.php</code> and <code>readme.html</code>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Protect against clickjacking	<input type="radio"/> Yes <input checked="" type="radio"/> No
Reduce MIME type security risks	<input type="radio"/> Yes <input checked="" type="radio"/> No
Reflected XSS prevention	<input type="radio"/> Yes <input checked="" type="radio"/> No
Remove Apache and PHP version signature	<input checked="" type="radio"/> Yes <input type="radio"/> No
Prevent content transformation	<input type="radio"/> Yes <input checked="" type="radio"/> No
Block access from specific user agents	<input checked="" type="radio"/> Yes <input type="radio"/> No
User agents to block, one per line	<pre>WebBandit webbandit Acunetix binlar BlackWidow Bolt 0 Bot mailto:craftbot@yahoo.com BOT for JCE casper checkprivacy</pre>

Disable directory listings (recommended)	When disabled, your web server might list the files and subdirectories of any directory on your site if there is no index.html file inside it. This can pose a security risk, so you should always enable this option to avoid this from happening.
Protect against common file injection attacks	Many attackers try to exploit vulnerable extensions on your site by tricking them into including malicious code hosted on the attacker's server. Enabling this option will protect your server against this kind of attacks. This works by preventing any URL which references an http:// or https:// URL in the query string. Sometimes these are legitimate requests. For example, some slideshow plugins use them. In this case you are recommended to use the RFIShield (Remote File Inclusion protection) in the Web Application Firewall and turn this .htaccess Maker option OFF.
Disable PHP Easter Eggs	<p>PHP has a fun and annoying feature known as "Easter Eggs". By passing a special URL parameter, PHP will display a picture instead of the actual page requested. Whereas this is considered fun, it is also widely exploited by attackers to figure out the version of your PHP installation (these images change between different versions of PHP) and launch hacking attacks targeting your specific PHP version. By enabling this option you completely disable access to those Easter Eggs and make it even more difficult for attackers to figure out the details of your server.</p> <p>Note: You are advised to also set <code>expose_php</code> to <code>Off</code> in your <code>php.ini</code> file to prevent accidental leaks of your PHP version.</p>
Block access to wp-config-sample.php readme.html	These two files are left behind after any WordPress installation or upgrade and can be directly accessed from the web. They are used by attackers to tell the WordPress version you are using, so that they can tailor an attack targeting your specific WordPress version. Enabling this option will "hide" those files when accessed from the web (a 404 Not Found page is returned), tricking attackers into believing that these files do not exist and making it slightly more difficult for them to deduce information about your site.
Protect against clickjacking	Turning on this option will protect you against clickjacking [http://en.wikipedia.org/wiki/Clickjacking]. It does so by preventing your site's pages to be loaded in a, Frame, IFrame or Object tag unless this comes from a page inside your own site. Please note that if your site relies on its pages being accessible through frames / iframes displayed on other sites (NOT on your site displaying content from other sites, that's irrelevant!) then you should not enable this option. If unsure, enable it.
Reduce MIME type security risks	Internet Explorer 9 and later, as well as Google Chrome, will try by default to guess the content type of downloaded documents regardless of what the MIME header sent by the server. Let's say a malicious user to upload an executable file, e.g. a .EXE file or a Chrome Extension, under an innocent file extension as .jpg (image file). When a victim tries downloading this file, IE and Chrome will try to guess the file type, identify it as an executable file and under certain circumstances executing it. This means that your site could be unwittingly used to serve malware. Such an event could result in your site being blacklisted by browser makers and cause their browsers to display a warning to users when visiting your site. By enabling this feature you instruct IE and Chrome to respect the file type sent by your server, eliminating this issue. See the relevant MSDN article [https://msdn.microsoft.com/en-us/library/gg622941(v=vs.85).aspx] for more information.
Reflected XSS prevention	<p>When enabled the browser will be instructed to prevent reflected XSS attacks. Reflected XSS attacks occur when the victim is manipulated into visiting a specially crafted URL which contains Javascript code in it. This URL leads to a vulnerable page which outputs this Javascript code verbatim in the page output ("reflects" the malicious code sent in the URL).</p> <p>This is a commonly used method used by attackers to compromise web sites, especially when a zero-day XSS vulnerability is discovered in popular WordPress plugins or WordPress itself. The attacker will try to trick the administrators of websites into visiting a maliciously crafted link. If the victims are logged in to their site at that time the malicious JavaScript will execute, typically giving the attacker privileged information or opening a back door to compromising the site.</p>

Enabling this option in .htaccess Maker will instruct the browser to try preventing this issue. Please note that this only works on compatible browsers (IE8; Chrome; Safari and other WebKit browsers) and only applies to reflected XSS attacks. Stored XSS attacks, where the malicious JavaScript is stored in the database, is **NOT** prevented. You should consider this protection a safety belt. Not wearing a safety belt in the event of an accident pretty much guarantees serious injury or death. Wearing a safety belt minimises the possibility of injury or death but does not always prevent it. This option is your safety belt against the most common type of XSS attacks. You should use it but don't expect it to stop everything thrown your way. Always keep your software up-to-date, especially when a security release is published!

For more information please consult the relevant MSDN article [<http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-iv-the-xss-filter.aspx>].

Remove Apache and PHP version signature

By default Apache and PHP will output HTTP headers advertising their existence and their version numbers. If you are always using the latest and greatest versions this may not be a problem, but the chances are that your host is using an older version of both software. Giving away the version numbers of the server software in every request makes it trivial for an attacker to obtain information about your site which will help them to launch a tailored attack, targeting known security issues in the versions of Apache and PHP you're using. Enabling this option will mitigate this issue. Please note that this is SECURITY THROUGH OBSCURITY which is NEVER, EVER an adequate means of protection. It's just a speed bump in the way of an attacker, not a roadblock.

You are strongly advised to keep your server software up-to-date. If you're not managing your own server, e.g. you're using a shared host, we very strongly recommend choosing a hosting service which follows this rule. As a simple test, if your server is not currently using one of the PHP versions published in the top right corner of <http://php.net> (or at most one version earlier, i.e. the third number of the version on your server is one less than the one listed on php.net) the chances are that your server is using outdated, vulnerable server software. Remember that outdated versions of PHP and Apache, even with *some* security patches backported, CAN NOT be secure. There's a good reason new software versions are published regularly. For example a popular but woefully outdate version of PHP is PHP 5.3.3. It has a MAJOR issue regarding bcrypt encryption, fixed in 5.3.10 and NOT backported by any vendor to an earlier version of PHP. As a result using PHP 5.3.3 makes your site's passwords *insecure*.

Prevent content transformation

Enabling this feature instructs proxy servers and caches to not convert your content. For example, certain proxy servers (typically found in mobile networks, businesses and ISPs in congested areas) will attempt to scale and aggressively compress images, CSS and Javascript to save bandwidth. This can lead to several issues, from displayed images being a bit off to your site breaking down because the compressed CSS/JS introduced errors preventing the browser from parsing it correctly. With this feature enabled the cache and proxy servers will be instructed to not do that by setting an HTTP header. If they respect the HTTP header (they should, it's a web standard) such issues are prevented.

For more information please consult the formal web standard document RFC 2616, section 14.9.5 [<https://tools.ietf.org/html/rfc2616#section-14.9.5>]

Block access from specific user agents

When enabled, it will block any site access attempt if the remote program sends one of the user agent strings in the User agents to block, one per line option. This feature is designed to protect your site against common bandwidth-hogging download bots and otherwise legitimate tools which are more usually used for hacking sites than their benign intended functionality.

User agents to block, one per line

The user agent strings to block from accessing your site. You don't have to enter the whole UA string, just a part of it. The default setting includes several usual suspects. Separate multiple entries by a single newline character (that is a single press of the ENTER key). Do note that some server with mod_security or mod_evasive installed will throw an "Access forbidden" message if you try to save the configuration settings when this field contains the word "WGet". If you come across this issue it is not a bug with Admin Tools or WordPress, it is a server-

level protection feature kicking in. Just avoid including the word Wget and you should be out of harm's way.

Default list of user agents to block

The following is the default list of user agents to block, as of Admin Tools 1.0.0.b1. It is very thorough and seems to be reducing the number of attacks enormously. If you are upgrading from an earlier version you might want to update the list manually (it's not updated automatically). Remember to enable the Block access from specific user agents to enable the feature and then click on Save and create .htaccess to generate the .htaccess file which applies this setting on your site.

```
WebBandit
webbandit
Acunetix
binlar
BlackWidow
Bolt 0
Bot mailto:craftbot@yahoo.com
BOT for JCE
casper
checkprivacy
ChinaClaw
clshttp
cmsworldmap
comodo
Custo
Default Browser 0
diavol
DIIbot
DISCo
dotbot
Download Demon
eCatch
EirGrabber
EmailCollector
EmailSiphon
EmailWolf
Express WebPictures
extract
ExtractorPro
EyeNetIE
feedfinder
FHscan
FlashGet
flicky
GetRight
GetWeb!
Go-Ahead-Got-It
Go!Zilla
grab
GrabNet
Grafula
harvest
HMView
ia_archiver
Image Stripper
Image Sucker
InterGET
```

Internet Ninja
InternetSeer.com
jakarta
Java
JetCar
JOC Web Spider
kmccrew
larbin
LeechFTP
libwww
Mass Downloader
Maxthon\$
microsoft.url
MIDown tool
miner
Mister PiX
NEWT
MSFrontPage
Navroad
NearSite
Net Vampire
NetAnts
NetSpider
NetZIP
nutch
Octopus
Offline Explorer
Offline Navigator
PageGrabber
Papa Foto
pavuk
pcBrowser
PeoplePal
planetnetwork
psbot
purebot
pycurl
RealDownload
ReGet
Rippers 0
SeaMonkey\$
sitecheck.internetseer.com
SiteSnagger
skygrid
SmartDownload
sucker
SuperBot
SuperHTTP
Surfbot
tAkeOut
Teleport Pro
Toata dragostea mea pentru diavola
turnit
vikspider
VoidEYE
Web Image Collector
Web Sucker
WebAuto

WebCopier
WebFetch
WebGo IS
WebLeacher
WebReaper
WebSauger
Website eXtractor
Website Quester
WebStripper
WebWhacker
WebZIP
Widow
WWW-Mechanize
WWWOFFLE
Xaldon WebSpider
Yandex
Zeus
zmeu
CazoodleBot
discobot
ecxi
GT::WWW
heritrix
HTTP::Lite
HTTrack
ia_archiver
id-search
id-search.org
IDBot
Indy Library
IRLbot
ISC Systems iRc Search 2.1
LinksManager.com_bot
linkwalker
lwp-trivial
MFC_Tear_Sample
Microsoft URL Control
Missigua Locator
panscient.com
PECL::HTTP
PHPCrawl
PleaseCrawl
SBIDER
Snoopy
Steeler
URI::Fetch
urllib
Web Sucker
webalta
WebCollage
Wells Search II
WEP Search
zermelo
ZyBorg
Indy Library
libwww-perl
Go!Zilla
TurnitinBot

sqlmap

7.2. Server protection

Server protection

Server protection

Site protection Yes No

File types allowed

jpe
jpg
jpeg
jp2
jpe2
png
gif
bmp
css
js

Exceptions

Allow direct access to these files

wp-activate.php
wp-comments-post.php
wp-cron.php
wp-links-opml.php
wp-mail.php
wp-signup.php
wp-trackback.php
xmlrpc.php
wp-content/plugins/akeebabackupwp/app/remote.php
wp-content/plugins/akeebabackupwp/app/index.php

Allow direct access, except .php files, to these directories

.well-known

Allow direct access, including .php files, to these directories

wp-content/upgrade

This is the product of original research conducted by our company, offering a quite thorough protection against a plethora of known threats when enabled. This feature is based on the tenet that nothing executes on your site unless you allowed it to. By blocking access to site elements (media files, JavaScript, CSS and PHP files) it makes it extremely hard—but not outright impossible—for an attacker to hack your site, even if he manages to exploit a security vulnerability to upload malicious PHP code to your site. Additionally, it will deny direct access to resources not designed to be directly accessible from the web, such as translation files, which are usually used by attackers to find out which version of WordPress you are running on your site to tailor an attack to your site. On the downside, you have to explicitly enable access to some plugins' PHP files which are designed to be called directly from the web and not through WordPress' main file, `index.php`.

Do note that enabling this feature will kill the functionality of some extensions which create arbitrarily named PHP files throughout your site, e.g. in subdirectories of wp-content/plugins. In our humble opinion the security risk of having your site unprotected outweighs the benefits of such solutions.

Before describing what each option does, a small explanation of how the protection works is in order. The protection code in the generated `.htaccess` file blocks direct web access to all files. WordPress's standard "entry point" or "main" file, `index.php`, is automatically exempt from this rule. However, your site also contains images, media, CSS and Javascript files inside certain directories. For each of the back-end and front-end protection we need a set of directories where such files are allowed and the file extensions of those files. These are what those options are all about. The default settings contain the most common file types you'd expect to find on a site and the standard WordPress directories where they should be located. You only have to tweak them if you want to add more file extensions or have such static files in locations other than the default.

Site protection Disables direct access to most resources, except those in the exceptions lists. It is generally recommended to turn it on to enhance the protection of your site.

File extensions allowed The extensions of files which allowed to pass through the server protection filter. Place one file extension per line, without the dot. For example, if you want to allow access to all PDF files you have to type in `pdf` on a new line of this list. Do note that file extensions are case-sensitive. This means that `PDF`, `Pdf`, `pdf` and `pDF` are four different file extensions as far as your web server is concerned. As a rule of thumb, type in the extensions in lowercase and make sure that the extensions of the files you upload are also in lowercase.

File extensions added here are allowed inside WordPress' default directories (`wp-includes` and `wp-content`). Moreover, only files with these extensions are allowed in the directories placed under the "Directories where only files with allowed extensions will be accessible" option (see below).

Disable client-side risky behavior in static content The files with extensions matching "File extensions" are, generally speaking, static files. However, some kinds of static files may contain client-side, dynamic content. For example, `HTML` and `SVG` files can contain JavaScript which executes on your browser. This kind of client-side, dynamic content can pose a security risk. For example, an attacker can upload a malicious `HTML` or `SVG` file which steals your login cookie and sends it to the attacker who can now impersonate you on your site, allowing them to take it over.

When you enable this option the `.htaccess` Maker sends a `Content-Security-Policy` header for these files which prevents them from executing any embedded client-side code in them.

If you do have certain files or folders with static files that absolutely need executable, embedded, client-side code please add them to one of the three Exceptions features described further below. Any explicitly allowed files or folders will be exempt from the "Disable client-side risky behavior in static content".

The following section is Exceptions. This allows specific files or all files in specific directories to pass through the Server Protection filter without further questions. This is required for several reasons. For starters, WordPress' core features depend on direct access to files. Some plugins also need to directly access PHP files, without passing them through WordPress' `index.php`. One such example is Akeeba Backup Professional's `restore.php` used in the integrated restoration feature, as it would be impossible to use the `index.php` of a site which is in a state of flux while the restoration is underway. Finally, you may have a third party script which doesn't install as a WordPress plugin. The Server Protection feature would normally block access to it and you still need a way around this limitation. So here we have those workarounds:

Files which will always be made accessible Place one file per line which should be exempt from filtering, therefore accessible directly from the web. The default settings only include WordPress core files which need to be accessed directly.

You do not need to add anything that is located `wp-admin`. That folder is always allowed direct access. If you want to best protect your site we recommend that you use the Password Protect `wp-admin` feature of Admin Tools to apply a server-level password protection to your `wp-admin` folder. This will very efficiently protect it from hackers.

Directories where only files with allowed extensions will be accessible Place one directory per line. Only files with extensions matching the “File extensions allowed” will be accessible in these directories. Any other file will NOT be allowed to be accessed over the web.
This is useful for folders which have non-executable files such as `wp-content/uploads`.

Directories where all files except .php will be accessible Place one directory per line. All files in these directories, except those with a .php extension, will be allowed to be accessed directly from the web. Please note that this option differs from the one above. Directories in this list allow all file extensions, not just the ones listed in “File extensions allowed”. Only files with .php and similar extensions (such as .phps, .php5 and so on) are blocked.

Directories where all files including .php will be accessible Place one directory per line. This option should be used as sparingly as possible. Each and every directory placed in this list is no longer protected by Server Protection and can be potentially used as an entry point to hacking your site. As far as we know there are only three cases when its use is even marginally justifiable:

- If you have installed another WordPress, Joomla!, phpBB, or any other PHP application in a subdirectory of your site. For example, if you are trying to restore a copy of your site inside a directory named `test` in your site's root you have to add `test` to this list. This is the one and only usage scenario which doesn't compromise your site's security.
- Some themes and theme frameworks may wrap their CSS and JavaScript inside PHP files in order to deliver them compressed to your browser. While this is a valid technique, it's possible that the list of PHP files is too big to track down and include in the first list of the Exceptions section. In this case you may consider putting the template subdirectory containing those files in this list.
- Some plugins generate .php files with arbitrary file names and expect them to be directly accessible from the web. This is insecure because you cannot tell which files are legitimate and which are suspicious just by looking at their filenames. Hackers understand that and know of these plugins, therefore they will try to hide their hacking scripts inside these folders: it's hiding a tree inside a forest.

Please note that this practice is dangerous. If you want to allow it it's your site and your risk assessment. Just don't come back and wonder why Admin Tools didn't protect you when it's you who has decided to cut a hole in the fence :)

In order to figure out which custom exceptions you need to add on your site, take a look at the How to determine which exceptions are required section.

Warning

Windows users beware! *Do not* use Windows' path separator (the backslash - \) to separate directories! We are talking about directories as they appear in URLs, so you should always use the URL path separator (forward slash - /) in those settings. In other words `some/long/path` is correct, `some\long\path` is WRONG.

7.2.1. How to determine which exceptions are required

After applying the Server Protection script you may notice that some of your extensions do no longer work properly or, even worse, at all. Sometimes your site may even look like something's missing or like CSS and Javascript no longer loads. Don't be afraid and don't rush into turning off the Server Protection. Determining which exceptions are required is easy and takes only a few minutes of your time. On the upside, once you determine them on one site you can reuse them on all sites having that plugin installed. You will quickly end up with your "master" exceptions list which you'll be able to apply to all of your sites without a second thought.

In the following example we are going to use Google Chrome to detect access issues on a site. Similar tools are built-in in other major browsers, such as Firefox, Opera, Safari, Edge and Internet Explorer 8 or later.

A typical indication that something went wrong is that CSS has gone missing or an action does not complete.

In order to figure out what is going wrong, we have to find out which of the files referenced by the page are throwing a 404 error (this means that they are filtered out by Server Protection), their naming pattern and location. Provided that you are using Chrome open up the Developer Tools pane by typing CTRL-SHIFT-I while viewing that broken page. Click on the Network tab. Reload the page. A list of files the browser tried to access appears.

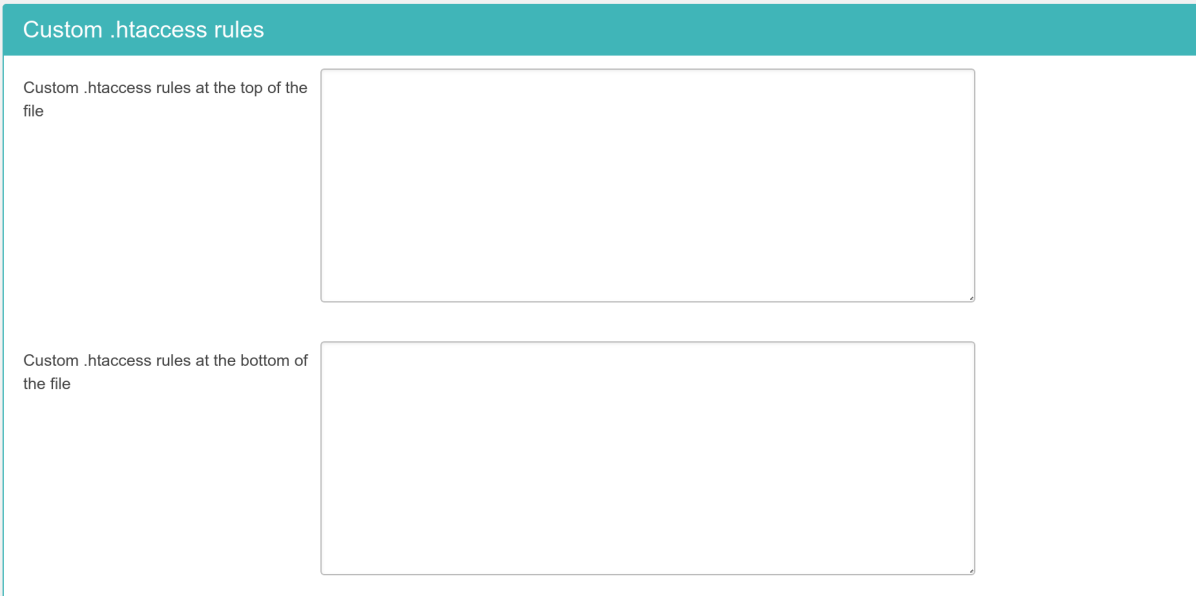
Go through this list and look for items in red. Look at the Status column. If you have a 404 or 403 you have located the files which probably have the problem.

Click on each red file. The right hand part of the window changes to display some debugging info about that file. Make sure the Headers tab is selected. The interesting part is the request URL which tells you where that file came from.

First, make sure these files really do exist. If they don't exist it's a legitimate 404 (not found) error and you can't do much about it. If the files do exist they are being blocked by our .htaccess file. Try adding the file path relative to your site's root (NOT the file URL!) in the Allow direct access to these files list in the .htaccess Maker. Then save and create .htaccess file and reload the page. If you repeat the process you'll see that this file now loads correctly.

7.3. Custom .htaccess rules

Custom .htaccess rules



The screenshot shows a web interface titled "Custom .htaccess rules". It contains two text input areas. The first area is labeled "Custom .htaccess rules at the top of the file" and is empty. The second area is labeled "Custom .htaccess rules at the bottom of the file" and is also empty. The interface has a teal header bar and a light blue border.

Sometimes you just need to add custom .htaccess rules beyond what the .htaccess Maker can offer. Such examples can be special directives your host told you to include in your .htaccess file to enable PHP 7, change the server's default error documents and so on. If you are an advanced user you may also want to write your own advanced rules to further customize the behaviour of the Server Protection. The two options in this section allow you to do that.

The contents of the Custom .htaccess rules at the top of the file text area will be output at the top of the .htaccess section created by Admin Tools, just after the RewriteEngine On directive. You should put custom exception rules and, generally, anything which should run before the protection and security rules in here.

The contents of the Custom .htaccess rules at the bottom of the file text area are appended to the end of the .htaccess section created by Admin Tools. This is the place to put stuff like directives to enable PHP 7 and any optimizations which should run only after the request has passed through the security and server protection rules.

7.4. Optimisation and utility

Optimisation and utility

Optimisation and utility

Force index.php parsing before index.html	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Set default expiration time to 1 hour	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Automatically compress static resources	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Force GZip compression for mangled Accept-Encoding headers	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Redirect index.php to the site's root	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Redirect www and non-www addresses	<input type="text" value="Redirect www to non-www"/>
Redirect this (old) domain name to the new one	<input type="text"/>
Force HTTPS for these URLs (do not include the domain name)	<input type="text"/>
HSTS Header (for HTTPS-only sites)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Disable HTTP methods TRACE and TRACK (protect against XST)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Enable Cross-Origin Resource Sharing (CORS)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Set the UTF-8 character set as the default	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Send ETag	<input type="text" value="Server default"/>

This section contains directives which are of utilitarian value and bound to save you some time:

Force index.php parsing before index.html

Some servers attempt to serve index.html before index.php. This has the implication that trying to access your site's root, e.g. `http://www.example.com`, will attempt to serve an index.html first. If this file doesn't exist, it will try to serve index.php. However, all of our WordPress sites only have the index.php, so this checking slows them down unnecessarily on each page request. This rule works around this problem. Do note that some servers do not allow this and will result in a blank page or Internal Server Error page.

Set default expiration time to 1 hour If your server has `mod_expires` installed and activated, enabling this option will cause all files and pages served from the site to have an expiration time of 1 hour, which means that the browser will not try to load them over the network before one hour elapses. This is a very desirable feature, as it speeds up your site.

Please note that some static files are given a longer expiration time of 1 week.

Automatically compress static resources Enabling this option instructs the server to send plain text, HTML, XML, CSS, XHTML, RSS and Javascript pages and files to the browser after compressing them with GZip. This significantly reduces the amount of data transferred and speeds up the site. On the downside some very old browsers, like Internet Explorer 6, might have trouble loading the site. Is anyone still using IE6? No? Good! Then enable this feature and make your WordPress site faster!

Force GZip compression for mangled Accept-Encoding headers

Note

This feature **REQUIRES** the Automatically compress static resources feature to be enabled.

Up to 15% of visitors to your site may not receive compressed resources when visiting your site, even though you have enabled Automatically compress static resources feature above. The reasoning is explained in detail by Yahoo engineers [<https://developer.yahoo.com/blogs/ydn/pushing-beyond-gzipping-25601.html>]. Enabling the Force GZip compression for mangled Accept-Encoding headers feature will allow clients (browsers) which send mangled Accept headers to be served compressed content, improving the perceived performance of your site for them.

Redirect index.php to the site's root

Normally, accessing your site as `http://www.example.com` and `http://www.example.com/index.php` will result in the same page being loaded. Except for the cosmetic issue of this behaviour it may also be bad for search engine optimization as search engines understand this as two different pages with the same content ("duplicate content"). Enabling this option will redirect requests to `index.php`, without additional parameter, to your site's root overriding this issue.

Redirect www and non-www addresses

Most web servers are designed to treat `www` and non-`www` URLs in the same way. For example, if your site is `http://www.example.com` then most servers will also display it if called as `http://example.com`. This has many adverse effects. For starters, if a user accesses the `www` site, logs in and then visits the non-`www` site he's no longer logged in, causing a functional issue with your site's users. Moreover, the duplicate content rules also apply in this case. That's why we suggest that you enable one of the redirection settings of this option. The different settings are:

- Do not redirect. It does no redirection (turns this feature off)
- Redirect non-`www` to `www`. Requests to the non-`www` site will be redirected to the `www` site, e.g. `http://example.com` will be redirected to `http://www.example.com`.
- Redirect `www` to non-`www`. Requests to the `www` site will be redirected to the non-`www` site, e.g. `http://www.example.com` will be redirected to `http://example.com`.

Redirect this (old) domain name to the new one

Sometimes you have to migrate your site to a new domain. Usually this is done transparently, having both domains attached to the same site on the hosting level. However, while a visitor can access the old domain name, the address bar on his browser will still show the old domain name and search engines will believe that you have set up a duplicate content site, having an adverse impact on your search results. So, you'd better redirect the old domain to the new domain with a 301 redirection to alert both users and search engines about the name change. This is what this option does. You can include several old domains separated by commas. For example:

`example.net, www.example.net`

will redirect all access attempts to example.net and www.example.net to the new domain.

Force HTTPS for these URLs (do not include the domain name)

Sometimes you need to redirect certain pages of your site to a secure (HTTPS) address. For example, your WooCommerce checkout page.

Use one URL per site and do not include http:// and your domain name. For example, if you want to redirect `http://www.example.com/eshop.html` to `https://www.example.com/eshop.html` you have to enter `eshop.html` in a new line of this field.

HSTS Header (for HTTPS-only sites)

Assuming that you have a site which is only supposed to be accessed over HTTPS, your visitor's web browser has no idea that the site should not be ever accessed over HTTP. There are two privacy implications for your users:

- There is a man-in-the-middle attack known as "SSL Stripping". In this case the user will access your site over plain HTTP without having any idea that they should be using HTTPS instead.
- Even if WordPress forwards your user to HTTPS by means of a plugin, the unencrypted (HTTP) request can still be logged by an attacker. With a moderate amount of sophistication on the part of the attacker (basically, some \$200 hardware and widely available information) they can efficiently eavesdrop *at the very least* the URLs visited by your user –undetected but to the most vigilant geeks among your users– and probably infer information about them.

The HSTS header can fix SSL Stripping attacks by instructing the browser to always use HTTPS for this website, even if the protocol used in a URL is HTTP. The browser, having seen this header, will always use HTTPS for your site. An SSL Stripping and other man-in-the-middle attacks are possible only if your user visits your site *for the first time* in a hostile environment. This is usually not the case, therefore the HSTS header can provide real benefits to the privacy of your users.

For more information on what the HSTS header is and how it can protect your site visitors' privacy you can read the Wikipedia entry on HSTS [http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security].

Important

Enabling HSTS will also have the following side effects which are designed to prevent unsafe HTTP redirections and cookie leaking:

- If your site is accessed over HTTP there will be a redirection to the HTTPS domain name, as configured in the .htaccess Maker.
- non-www to www redirection and vice versa will always redirect requests to the HTTPS version of the domain name, even if you access it over HTTP.
- Old to new domain redirection will always redirect to the HTTPS domain name, as configured in the .htaccess Maker.
- The HSTS header is only sent over HTTPS requests, not over HTTP requests, per HSTS header best practices.

Most sites will not notice any difference. If you have a strange setup with different HTTP domain names assigned to the same site but only one HTTPS domain (e.g. a shared SSL setup) you may experience redirection issues. In this case we advise you to disable HSTS. Instead, add the following directive in the "Custom .htaccess rules at the bottom of the file" area:

Header always set Strict-Transport-Security "max-age=31536000"

Disable HTTP methods TRACE and TRACK (protect against XST) Enabling this option will prevent remote clients from using the HTTP methods TRACE and TRACK to connect to your site. These can be used by hackers to perform privilege escalation attacks known as Cross Site Tracing (XST) [https://www.owasp.org/index.php/Cross_Site_Tracing]. To the best of our knowledge there are no side-effects to enabling this feature.

Enable Cross-Origin Resource Sharing (CORS) By default a third party site cannot load content from your site using an AJAX request since your content is in a different domain than the site hosting the JavaScript performing the request. Using CORS you can circumvent this problem, allowing third party sites' JavaScript to load content from your site. When you enable this option the proper Access-Control-Allow-Origin and Timing-Allow-Origin HTTP headers will be set for all requests. For more information on CORS please consult the Enable CORS [<http://enable-cors.org/>] site.

Set the UTF-8 character set as the default Some servers use the legacy ISO-8859-1 character set as the default when serving content. While WordPress pages will appear correctly –WordPress sends a content encoding header– other content such as JSON data, CSV exports and Admin Tools' messages to blocked users may appear incorrectly if they're using international characters. If you're unsure, try enabling this option.

Send ETag Your web server sends an ETag header with each **static** file it serves. Browsers will ask the server in subsequent requests whether the file has a different ETag. If not, they will serve the same file therefore reducing the amount of data they need to transfer from the server (and making the site load faster). By default ETags are calculated based on the file size, last modified date and the inode number. The latter depends on the location of the file inside the filesystem of the server.

When you have a site hosted on a single server this is great. If your static files are, however, hosted on a server farm this may not be a good idea. The reason is that every static file is stored on different server and while the file size and last modified date might be the same the inode number will differ, therefore causing the browser to perform unnecessary file transfers. This is where this option comes in handy.

Important

Do NOT change this option if your site is hosted on just one server. If you are not sure or have no idea what that means then your site **is** hosted on just one server and you **MUST NOT** change this option. Please bear in mind that site speed analysers like YSlow are designed for gigantic sites running off *hundreds or thousands of servers*. Their site speed checklists **DO NOT** work well with the vast majority of sites you are working on, i.e. very small sites running off a single server. Treat these checklists as suggestions: you need to exercise common sense, not blindly follow them. If you disable ETags on a small site you are more likely to do harm than good!

The available options are:

- **Server default.** Use whatever setting the server administrator has chosen. If you are not perfectly sure you know what you're doing choose this option.
- **Full.** Send ETags based on file size, last modification date/time and inode number.
- **Size and Time.** Send ETags based on file size and last modification date/time only.
- **Size only.** Send ETags based on file size only.
- **None (no ETag sent).** Disable ETags completely. Do keep in mind that if you do not also enable the Set default expiration option you will be hurting your site's performance **BIG TIME**.

Referrer Policy Header

While surfing, your browser will send out some information about the previous you were visiting (the Referrer that brought you to the new page). This is useful for analytics, for example you can easily track down how many visitors came from Twitter or any other page.

However, there are security implications about the Referrer header. What if on the private area of your website there are sensible information? Think about a private support area, where there is a ticket with the link `www.example.com/private-support/help-my-site-www-foobar-com-is-hacked` ; you post a reply with a link to a Stack Overflow reply, the user clicks on it and... whops! Now Stack Overflow knows that the site `www.foobar.com` was hacked.

The Referrer Policy header will instruct your browser when to send the Referrer header and how many information you want to share.

- **Do not set any policy** You're not setting any instruction to the browser
- **(Empty)** You do not want to set the Referrer Policy here (as header) and the browser should fallback to other mechanisms, for example using the `<meta>` element or the `referrerpolicy` attribute on `<a>` and `<link>` elements.
- **no-referrer** Never send the referer header
- **no-referrer-when-downgrade** The browser will not send the referrer header when navigating from HTTPS to HTTP, but will always send the full URL in the referrer header when navigating from HTTP to any origin. It doesn't matter whether the source and destination are the same site or not, only the scheme.

Source	Destination	Referrer
<code>https://www.yoursite.com/url1</code>	<code>http://www.yoursite.com/url2</code>	NULL
<code>https://www.yoursite.com/url1</code>	<code>https://www.yoursite.com/url2</code>	<code>https://www.yoursite.com/url1</code>
<code>http://www.yoursite.com/url1</code>	<code>http://www.yoursite.com/url2</code>	<code>http://www.yoursite.com/url1</code>
<code>http://www.yoursite.com/url1</code>	<code>http://www.example.com</code>	<code>http://www.yoursite.com/url1</code>
<code>http://www.yoursite.com/url1</code>	<code>https://www.example.com</code>	<code>http://www.yoursite.com/url1</code>
<code>https://www.yoursite.com/url1</code>	<code>http://www.example.com</code>	NULL

- **same-origin** The browser will only set the referrer header on requests to the same origin. If the destination is another origin then no referrer information will be sent.

Source	Destination	Referrer
<code>https://www.yoursite.com/url1</code>	<code>https://www.yoursite.com/url2</code>	<code>https://www.yoursite.com/url1</code>
<code>https://www.yoursite.com/url1</code>	<code>http://www.yoursite.com/url2</code>	NULL
<code>https://www.yoursite.com/url1</code>	<code>http://www.example.com</code>	NULL
<code>https://www.yoursite.com/url1</code>	<code>https://www.example.com</code>	NULL

- **origin** The browser will always set the referrer header to the origin from which the request was made. This will strip any path information from the referrer information.

Source	Destination	Referrer
https://www.yoursite.com/ url1	https://www.yoursite.com/ url2	https://www.yoursite.com/
https://www.yoursite.com/ url1	http://www.yoursite.com/ url2	https://www.yoursite.com/
https://www.yoursite.com/ url1	http://www.example.com	https://www.yoursite.com/

Warning

Navigating from HTTPS to HTTP will disclose the secure origin in the HTTP request.

- **strict-origin** This value is similar to `origin` above but will not allow the secure origin to be sent on a HTTP request, only HTTPS.

Source	Destination	Referrer
https://www.yoursite.com/ url1	https://www.yoursite.com/ url2	https://www.yoursite.com/
https://www.yoursite.com/ url1	http://www.yoursite.com/ url2	NULL
https://www.yoursite.com/ url1	http://www.example.com	NULL
http://www.yoursite.com/ url1	https://www.yoursite.com/ url2	http://www.yoursite.com/
http://www.yoursite.com/ url1	http://www.yoursite.com/ url2	http://www.yoursite.com/
http://www.yoursite.com/ url1	http://www.example.com	http://www.yoursite.com/

- **origin-when-cross-origin** The browser will send the full URL to requests to the same origin but only send the origin when requests are cross-origin.

Source	Destination	Referrer
https://www.yoursite.com/ url1	https://www.yoursite.com/ url2	https://www.yoursite.com/ url1
https://www.yoursite.com/ url1	https://www.example.com	https://www.yoursite.com/
https://www.yoursite.com/ url1	http://www.yoursite.com/ url2	https://www.yoursite.com/
https://www.yoursite.com/ url1	http://www.example.com	https://www.yoursite.com/
http://www.yoursite.com/ url1	https://www.yoursite.com/ url2	http://www.yoursite.com/

Warning

Navigating from HTTPS to HTTP will disclose the secure URL or origin in the HTTP request.

- **strict-origin-when-cross-origin** Similar to `origin-when-cross-origin` above but will not allow any information to be sent when a scheme downgrade happens (the user is navigating from HTTPS to HTTP).

Source	Destination	Referrer
<code>https://www.yoursite.com/url1</code>	<code>https://www.yoursite.com/url2</code>	<code>https://www.yoursite.com/url1</code>
<code>https://www.yoursite.com/url1</code>	<code>https://www.example.com</code>	<code>https://www.yoursite.com/url1</code>
<code>https://www.yoursite.com/url1</code>	<code>http://www.yoursite.com/url2</code>	NULL
<code>https://www.yoursite.com/url1</code>	<code>http://www.example.com</code>	NULL

- **unsafe-url** The browser will always send the full URL with any request to any origin.

7.5. System configuration

Warning

If you backup and restore your site on a new host you **MUST** change these configuration parameters to reflect your new server configuration manually. In fact, you must remove your `.htaccess` file, let WordPress regenerate a new `.htaccess` files, then let Admin Tools create a new `.htaccess` file before you can use your site's front-end.

Optimisation and utility

System configuration

Host name for HTTPS requests (without `https://`)

Host name for HTTP requests (without `http://`)

Follow symlinks (may cause a blank page or 500 Internal Server Error)

Base directory of your site (/ for domain's root)

This final section contains all the options which let the `.htaccess` maker know some of the most basic information pertaining your site and which are used to create the rules for some of the options in the previous section.

Host name for HTTPS requests (without `https://`) Enter the site's domain name for secure (HTTPS) connections. By default, Admin Tools assumes it is the same as your site's domain, but you have to verify it as it may be different on some hosts, especially on shared hosts. Do not use the `https://` prefix, just the domain name without the path to your site. For example, if the address is `https://www.example.com/wordpress` then type in `www.example.com`.

Host name for HTTP requests (without `http://`) Enter the site's domain name for regular (HTTP) connections. By default, Admin Tools assumes it is the same as the address you are connected to right now, but you have to verify it. Do not use the `http://` prefix, just the domain name without the path to your site. For example, if the address to your site's root is `http://www.example.com/wordpress` then type in `www.example.com`.

Follow Symlinks WordPress normally does not create symlinks and does not need symlinks. At the same time, hackers who have infiltrated a site do use symlinks to get read access to files that are normally outside the reach of the web site they have hacked. This is why this option exists. You can set it to:

- **Default.** It's up to your host to determine if symlinks will be followed. Use this if the other options cause problems to your site.
- **Yes, always.** This is the insecure option. If you use it keep in mind that in the event of a hack all world-readable files on the server may be compromised. Really, it's a horrid idea. Don't use it.
- **Only if owner matches.** That's the safe approach to enabling symlinks. They will be followed only if the owner of the symlink matches the owner of the file/directory it links to.

If you have no idea what that means, first try setting this option to "Only if owner matches". If this results in a blank page or an Internal Server Error 500 then set this to "Default". For more information please consult Apache's documentation.

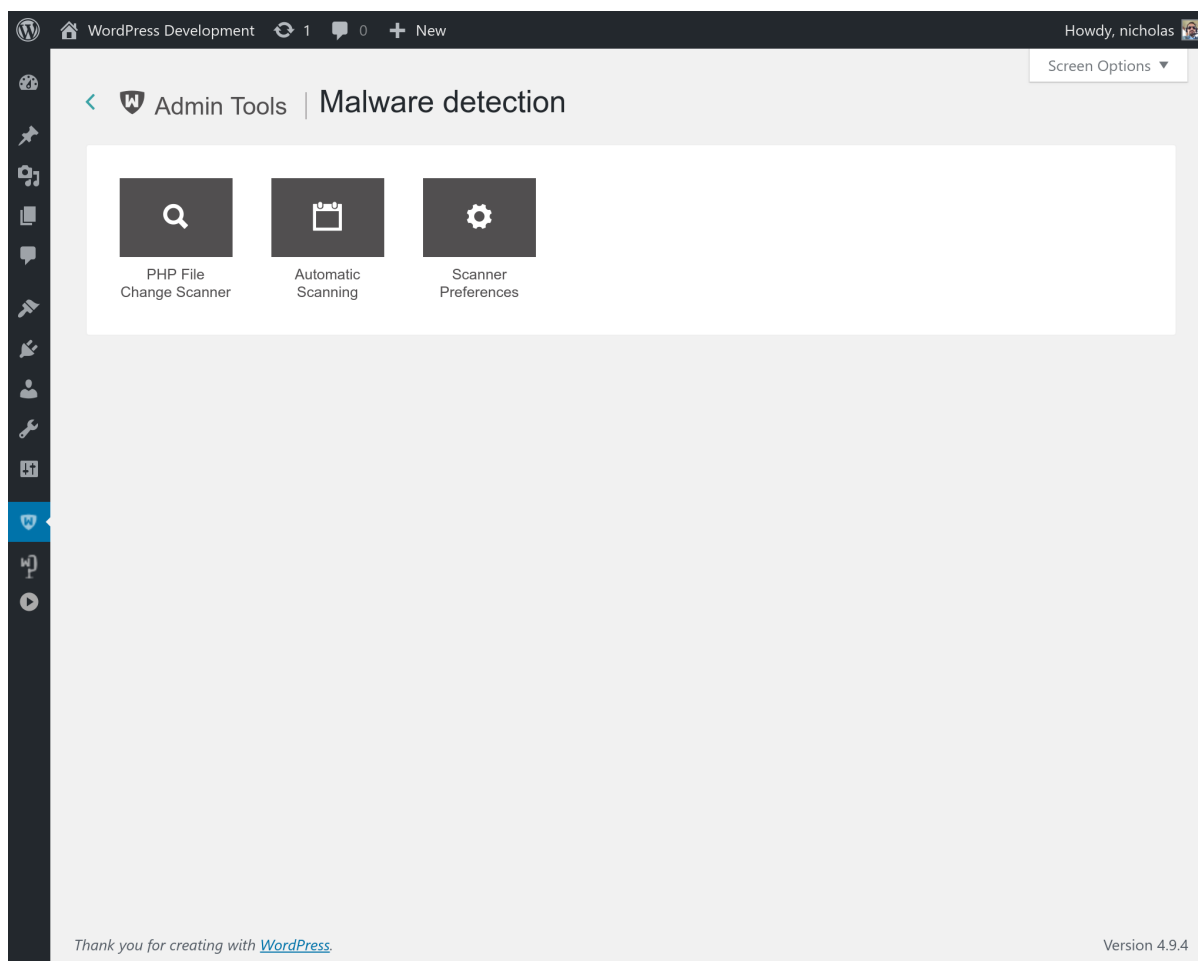
Base directory of your site This is the directory where your site is installed. For example, if it is installed in a directory named `wordpress` and you access it on a URL similar to `http://www.example.com/wordpress` you have to type in `/wordpress` in here. If your site is installed on the root of your domain, please use a single forward slash for this field: `/`

8. Malware Detection (the PHP File Scanner)

Note

This feature is only available in the for-a-fee Professional release of our software.

Malware detection



Admin Tools has a very powerful feature called PHP File Change Scanner. This feature can be used to perform a security scan of the PHP files included anywhere under your site's root directory, as well as detect any modified or added files in subsequent runs. The file scanning engine is built on top of Akeeba Engine, the engine powering our acclaimed Akeeba Backup site backup software, ensuring rock solid operation. Each scanned file also comes with a preliminary automatic security assessment ("threat score") which can give you a quick idea of how possible it is that the file in question could be suspicious (malware / hacked file).

The PHP File Change Scanner has more handy features. For example the ability to produce DIFF's (a synopsis of how modified files differ from the previous known copy), print and export the scan reports as well as the interactive report viewer which allows you to peek at the contents of each file. This feature can allow power users to detect and eliminate hacks much faster than using a purely manual method. You can also automate the run of the scanner engine using a CLI CRON job, making sure that you always know what's going on with your site.

Warning

By default, only files with a lowercase `.php`, `.phps`, `.php3` and `.inc` extension are scanned. Non-PHP files or PHP files whose extension is different (e.g. `.PHP` in capitals, `.php4`, `.php5`, `.php7` and so on) will not be scanned unless you configure it so. The idea of this feature is to scan only PHP files, because the modification or addition thereof could signify a potential problem or hack of your site. We only use a subset of lowercase extensions because these are the extensions of virtually all PHP files you will encounter on the overwhelming majority of sites. Other extensions are host-specific and not universal enough to guarantee that they do contain PHP code.

Moreover, not all hacking scripts are written in PHP. Some of them may be written in PERL, Python, Ruby, shell script (e.g. Bash) or they could be executable binaries. Some hackers may also place infected PDFs, PNGs, Word documents etc which will infect your computer if you open them. None of those

files will be scanned by Admin Tools's PHP File Change Scanner. These files can only be detected by using a traditional antivirus.

8.1. How does it work and what should I know?

The PHP File Change Scanner is a hybrid between a backup engine and a file scanner. It works by "sweeping" your WordPress site for PHP files and comparing them to their last known state saved in the database. It will then report any changes, i.e. files which have been modified or added since the previous scan. The following paragraphs will explain how some aspects of the file scanning and reporting engine work.

Scope of the scan. Only files inside your WordPress site's root are scanned. If you have placed PHP files outside of your site's root, they will not be scanned. Moreover, any readable directory under your site's root will be scanned, even if it does not belong to the current WordPress installation. For example, if you have additional sites or subdomains stored in subdirectories of your site's root, they will be scanned nonetheless.

Only PHP files are scanned. Only files with the extensions defined in the Scanner Preferences page are scanned. By default this is .php, .phps, .php3 and .inc files. Non-PHP files or PHP files whose extension is different will not be scanned. The idea of this feature is to scan only PHP files, because the modification or addition thereof could signify a potential problem or hack of your site. We only use the lowercase .php extension because this is the extension of virtually all PHP files and the other extensions are host-specific and not universal enough to guarantee that they do contain PHP code.

File comparison terms. In order to determine if a file is modified, Admin Tools will compare its size, last modification time and md5 sum. If any of these do not match the previous scan's results, the file is considered modified. If there is no record of that file in a previous scan, the file is considered as new.

When a file change is detected. A file change is detected only if the file is added or modified since the immediately previous scan. This means that if you scan now, modify a PHP file and scan again, it will show up as modified. If you perform a third scan right after the second one, the file will NOT be reported as changed (unless it has a non-zero Threat Score and it's not Marked as Safe). This is normal. The file was changed between the first and second scan, but not between the second and third scan.

Threat score calculation. Whenever Admin Tools Professional encounters a new or modified file, it calculates a "threat score". This is a weighed sum of potential security "red flags". Essentially, Admin Tools Professional runs a few heuristics against the PHP file in question, looking for code patterns which are commonly (but *NOT NECESSARILY*) used in hacking scripts and hacked files. Each of those patterns is assigned a "weight". The weight is multiplied by the number of occurrences of the pattern to give a score. The sum of these scores is what we call a "threat score". How to interpret it: the higher the threat score, the more probable it is that this could be a nefarious file and its contents should be *manually assessed*.

Please note that a high threat score does not necessarily mean that the file is hacked or malware. Likewise, a low but non-zero threat score (1-10) does not necessarily mean that the file in question is necessarily safe. Please take a look at the next few sections for more information.

Removing old scans has some consequences. When you remove an old scan, Admin Tools also removes all associated file alert records. If you have defined some files with a non-zero Threat Score as "Marked Safe" in this scan's report, then this information is lost when you delete this scan. As a result, subsequent scans will, again, report the file as "Suspicious".

Heavy database usage. In order for this feature to work, Admin Tools Professional needs to perform very heavy use of your database. There will be at least one database query for each and every PHP file on your site. The average site contains over 1,000 such files. Moreover, there will be one database query for each and every new or modified file.

Heavy resource usage. Scanning your site is a very CPU and memory intensive procedure. Admin Tools Professional has to scan your entire site, find the PHP files, read them, calculate an MD5 sum (very CPU and memory intensive process!), read data from the database, compare it with those in memory, write data to the database and repeat that for each file. This does put a big strain on your server, similar to what you get when you're backing up your site.

Potential problems. As stated above, the file scan operation is very database, CPU and memory intensive. This can cause failure of the scan process due to one of several reasons, especially on lower-end hosts (usually: cheap or low quality shared hosts):

- **Memory exhaustion.** Getting an out-of-memory error is not at all unlikely. We strongly recommend having *at the very least* 32Mb of available PHP memory. We recommend 64Mb to 128Mb for trouble-free operation. If you only have 16Mb or less of available PHP memory, the scan will most likely fail.
- **Exhausting your MySQL query limit.** Some hosts have a limit on how many queries you can run per minute or per hour. Because the file scan is very database-intensive, you may exhaust this limit, causing the scan to crash.
- **MySQL server has gone away.** Likewise, some hosts have set up MySQL (the database server) to forcibly close the connection if it doesn't receive data for a short time period, usually anything between 0.5 and 3 seconds. This could cause the infamous "MySQL server has gone away" error message, killing your scan.
- **Timeout.** Calculating MD5 and diffs for large files is a very time consuming process. It is possible that PHP times out during that operation, especially on slow, low-end hosts.
- **Hitting the CPU usage limit.** Many hosts enforce a CPU usage limit. Given that the file scan is a very CPU-intensive process, it is possible that you hit that limit. What usually happens is that the host kills the script causing the "excessive" CPU usage (our file scan operation).

All of the above manifest themselves as a 500 Internal Server Error message or a never ending scan process when trying to scan your site. Unfortunately, these are all server limitations and we can not work around them, while maintaining the usefulness of the PHP File Change Scanner feature. If you hit on those limitations, our recommendation is to switch to a better performing / higher-quality host.

8.2. Configuration

You can configure the PHP File Change Scanner from the Malware Detection page, clicking on the Scanner Preferences button.

WordPress Development 1 0 + New Howdy, nicholas Screen Options

Admin Tools | Scanner Preferences

File Scanner

Calculate diffs when scanning Yes No

When this option is enabled, Admin Tools will calculate a diff (compact form of file differences) for each modified file detected by the PHP File Scanner feature. WARNING: This consumes A LOT of database space, about 20-40Mb for a typical site!

Send results to this email

The scan results will be automatically sent to this email address. If you leave it blank no email will be sent.

Email only on actionable items Yes No

When enabled (default) the PHP File Change Scanner will send you an email with the scan results summary only when actionable items (added, modified or suspicious files) are detected.

File types to be scanned

```
php
phps
php3
inc
```

Excluded folders not to be scanned

Excluded files not to be scanned

Frontend Yes No

When enabled it allows you to the PHP File Change Scanner without logging in to the backend.

Secret word

Protects the frontend scheduling feature from DoS attacks by requiring you to pass this secret word in the frontend scheduling URL. Please use long, complex passwords. Consult the documentation for more information.

Thank you for creating with [WordPress](#). Version 4.9.4

Calculate diffs when scanning	<p>When this option is enabled, Admin Tools will calculate a diff (compact form of file differences) for each modified file detected by the PHP File Scanner feature. This is useful if you want to pinpoint the changes made to a file.</p> <p>Please note that this consumes a lot of database space, about 20-40Mb for a typical site.</p>
Send results to this email	<p>The scan results will be automatically sent to this email address. If you leave it blank no email will be sent.</p>
Email only on actionable items	<p>When enabled (default) the PHP File Change Scanner will send you an email with the scan results summary only when actionable items (added, modified or suspicious files) are detected.</p>
File types to be scanned	<p>Enter file extensions to be scanned by the PHP File Change Scanner. One extension per line, without the leading dot. Please only include extensions of file types you expect to contain PHP executable code. Don't add non-PHP files such as .exe or .docx; that would slow down the scanner without increasing your security. Remember that the PHP File Change Scanner is designed to scan PHP files; it's not a generic antivirus, it's useless against malicious macros, traditional viruses in EXE files etc.</p>
Excluded folders not to be scanned	<p>List of folders which are going to be ignored while the PHP File Change Scanner is scanning your site. One directory per line. Always use forward slashes, even on Windows. Paths must be relative to your site's root folder. Example:</p> <pre>wp-content/plugins/myplugin/somefolder</pre>
Excluded files not to be scanned	<p>List of files which are going to be ignored while the PHP File Change Scanner is scanning your site. One file per line. Always use forward slashes, even on Windows. Paths must be relative to your site's root folder. Example:</p> <pre>wp-content/plugins/someplugin/file.php</pre>
Frontend	<p>Set to Yes to enable scheduling this feature with the Scheduling URL method.</p>
Secret Word	<p>The Secret Word to control access to the Scheduling URL method. Only applies when the Frontend option above is set to Yes.</p>

8.3. Scanning and administering scans

Performing a new scan

Performing a scan is a very simple process. Just go to Admin Tools and click on Malware Detection, PHP File Change Scanner. On that page, simply click on Scan Now to initiate the scan. The scanning status is displayed below the list of scans.

The scan process is split in many steps in order to avoid server timeouts. Take a look at the Last server response label. It tells you for how long the current step is running. If this figure goes over 120 seconds, you can be sure that the scan is stuck. In case the scan is stuck or throws an error, please read the "How does it work?" section.

Please note that the first time you run this feature, all scanned PHP files will be reported as Added. This is normal. Since there was no previous scan, all PHP files are new as far as Admin Tools is concerned. A positive side-effect of this behaviour is that all PHP files go through the "Threat score" determination engine which will typically result in a list of 30-100 files you should check. In other words, even if you run this feature for the first time after a site is hacked, it will narrow down the list of files you should check.

Managing scans

PHP File Scanner: Managing scans

The screenshot displays the 'Security Exceptions Log' in the Admin Tools plugin. At the top, there are navigation links for 'Admin Tools' and 'Security Exceptions Log'. Below the title, there is a toolbar with 'Bulk Actions', 'Apply', 'Scan Now', and 'Purge file cache' buttons. A pagination indicator shows '1 item' of '1'. The main content is a table with the following columns: '#', 'Scan Date', 'Total Files', 'Modified', 'Possible Threats', 'Added', and 'Actions & Reports'. One scan entry is listed with ID '1', a scan date of '2018-03-20 16:54:54', 743 total files, 0 modified files, 14 possible threats, and 738 added files. A 'View Report' button is present in the 'Actions & Reports' column for this entry. The footer of the page includes a WordPress thank-you message and the version number 'Version 4.9.4'.

The main page of the PHP File Change Scanner feature gives you an overview of the scan operations. From left to right, you see the following columns on each row:

- **A checkbox** which is used to select the row(s) you want to delete, by pressing the Delete button on the toolbar.
- **The scan ID** (a number) is a monotonically increasing number, i.e. each new scan has an ID which is equal to the previous scan's ID plus one.
- **Scan date** is the date and time this scan was performed. The date and time are shown in GMT (UTC) timezone.
- **Total files** is the total number of PHP files which Admin Tools detected
- **Modified** is the total number of PHP files which Admin Tools detected that are modified since the last scan or have a threat score greater than 0 and not marked by you as safe.
- **Possible threats** is the total number of PHP files, new, added or modified, with a non-zero threat score.
- **Added** is the total number of PHP files which were added since the last scan.
- **Actions & Reports** contains a link titled View Report when modified or added files are detected on your site.

8.4. Reading the reports

PHP File Scanner: Reading the reports

File path	Status	Threat score	Marked safe
wp-includes/rest-api/endpoints/class-wp-rest-comments-controller.php	New	5	MARK SAFE
wp-admin/includes/class-ftp.php	New	5	MARK SAFE
wp-admin/includes/file.php	New	4	MARK SAFE
wp-includes/ms-functions.php	New	3	MARK SAFE
wp-includes/ID3/getid3.php	New	3	MARK SAFE
wp-admin/includes/class-wp-community-events.php	New	3	MARK SAFE
wp-content/plugins/akismet/class.akismet.php	New	3	MARK SAFE
wp-includes/comment.php	New	2	MARK SAFE
wp-includes/class-wp-session-tokens.php	New	2	MARK SAFE
wp-admin/network.php	New	1	MARK SAFE
wp-includes/load.php	New	1	MARK SAFE
wp-includes/SimplePie/Sanitize.php	New	1	MARK SAFE
wp-includes/SimplePie/Parse/Date.php	New	1	MARK SAFE

The report view of the PHP File Change Scanner allows you to navigate through the results of a file scan operation, enabling you to review any suspicious files. Each row contains the following columns:

- **File path** is the path and name of the file, relative to your site's root directory. Clicking on it will open the Examine File view for that file.
- **Status** can be one of:

New A file which was added since the last file scan. When you scan a site for the first time, all files will have this status. This could be a file created by your installed extensions, a file you uploaded yourself, a file added during an extension upgrade or a hacking script.

Modified A file which was modified since the last file scan. A file can be modified because you edited it, an extension update replaced it or because the site was hacked.

Suspicious A suspicious file is a file which did exist during the previous scan, has not been modified and has a non-zero Threat Score. This does not necessarily mean that the file is hacked or that it has a nefarious purpose. Please see the discussion regarding the Threat Score below.

If a file has a non-zero threat score (therefore potentially dangerous, see below) the status will appear in bold letters.

- **Threat Score.** The higher this number is, the most likely it is that the file is hacked or nefarious. Please note that a high threat score does not necessarily mean that the file is hacked or a hacking script. Likewise, a low but

non-zero threat score (1-10) does not necessarily mean that the file in question is necessarily safe. The number is merely A PROBABILITY INDICATOR. Admin Tools prefers to err on the side of caution. This means that false positives (high threat scores for perfectly safe, not hacked files) are all too common. For instance, Admin Tools' own file, Akeeba Backup Professional's files, a few WordPress core files and some third party plugin files have high Threat Scores. None of these files is hacked or nefarious. In order to understand why that happens, let's take a look at what the Threat Score is and how it's calculated.

Whenever Admin Tools Professional encounters a new or modified file, it calculates a "threat score". This is a weighed sum of potential security "red flags". Essentially, Admin Tools Professional runs a few heuristics against the PHP file in question, looking for code patterns which are commonly (but NOT NECESSARILY) used in hacking scripts and hacked files. Each of those patterns is assigned a "weight". The weight is multiplied by the number of occurrences of the pattern to give a score. The sum of these scores is what we call a "threat score". How to interpret it: the higher the threat score, the more probable it is that this could be a nefarious file and its contents should be manually assessed.

The first thing you should do is to compare the file you have with the same file from a fresh installation of WordPress and the plugin this file belongs to. For example, let's say that you get a high threat score for the `wp-content/plugins/foobar/example.php` file. From the file path you can understand that it's part of a plugin called Foobar. Install a new WordPress site on a local server and install Foobar on it. Find the `wp-content/plugins/foobar/example.php` file on the new site and compare it with the one from your regular site you are using the PHP file comparison on. A very handy tool to compare files is WinMerge [<http://winmerge.org/>]. If you're not on Windows or Linux (the platforms supported by WinMerge) you can search for graphical diff or file comparison tools for your platform. In any case, if the files match then the file is safe. In this case you can click on the icon in the Marked Safe column so that it turns into a green checkmark. When you do that, future scans will not report the file *unless* it is changed.

A simple way to get started is running the file scanner on a pristine copy of your site, i.e. you know it's not hacked. By definition you can mark all suspicious files as safe. See below.

- **Marked Safe.** All files with a non-zero threat score will appear on each and every scan as Suspicious. Obviously, you don't want to go through the tedious task of manually verifying files as described above for each and every scan. Marking a file as safe tells Admin Tools that this particular file, in its current state, is not suspicious and should not be reported again as suspicious unless it's modified. Unmarking the file (default) will report this file as suspicious during the next scan.

Tip

If someone hacks your site, he could run a scan, mark the hacked files as safe and then run yet another scan in an attempt to hide his tracks. If in doubt, just delete all of the scans and run a new scan. This effectively resets the "Marked Safe" status of all files and will reassess the threat score of all files on your site, just like the very first scan you did on that site.

You can print the report by clicking on the Print button on the toolbar. The Print button will print out all of the files on the report, not just the ones you currently see on your screen. It is advisable to print out the result in landscape (not portrait) orientation. Moreover, the Export CSV button will export the entire report in a comma separated values (CSV) file which you can then import in Microsoft Office Excel, Apple Numbers, OpenOffice.org/LibreOffice Calc, Google Docs spreadsheet or any other desktop or on-line spreadsheet application.

The button Mark All as Safe will mark all files with a non-zero threat score on the current report as Safe. It is advisable to do that only in the following case. Take a new scan, make sure it has no new or suspicious files. Run any updates on your site. Take a new scan; the update files appear as new, modified and / or suspicious. Use the Mark All as Safe button to mark these files as Safe. These files were installed during the update and are trusted (as far as you can trust the developers which supplied them). Please note that if you do NOT trust the source of a particular update you should not use this button. A good reason to not necessarily trust the update is if the software you are updating has recently (e.g. in the last 12 months) been taken over by a new developer. There are many cases where legitimate software was bought out by shady people who waited for a few months before ultimately publishing an update with malware hidden in it. Therefore we strongly recommend that you exercise abundant caution with code coming from a new developer who has recently taken over established, legitimate software.

The Examine File view

When you click on a file name, the Examine File view opens. In this view you can view detailed information about the file, as well as the file itself.

In the File Information pane you can see the generic file information you would see in the Report view.

Below that you can find the Current file source pane. Please note that this pane shows you the contents of the file *as it is right now*. This may or may not be equal to the contents of the file which was scanned. If the file has since been deleted, you will see an empty pane. The places where suspicious code patterns have been found will be highlighted in yellow background.

If you have enabled the diff feature in the component's configuration page and this is a Modified file, you will also see the Diff to the previous version pane. On this pane you will see the consolidated differences between the scanned file and its previous state.

8.5. Automating the scans (CRON jobs)

Tip

Consult the Automatic Scanning page of the plugin for detailed information, tailored to your site, without having to read this documentation page.

When you install Admin Tools, it copied a file named `admintools-filescanner.php` into your site's `wp-content/plugins/admintoolswp/cli` directory. When you run it, it will execute a new scan. If you have access to the command-line version of PHP (most hosts do), you can use that script to schedule your file scans.

In order to schedule a file scan, you will have to use the following command line to your host's CRON interface:

```
/usr/local/bin/php /home/USER/webroot/wp-content/plugins/admintoolswp/app/cli/admintool
```

where `/usr/local/bin/php` is the path to your PHP CLI executable and `/home/USER/webroot` is the absolute path to your web site's root. You can get this information from your host.

Special considerations:

- Most hosts do not impose a time limit on scripts running from the command-line. If your host does and the limit is less than the required time to scan your site, the scan will fail.
- This script is not meant to run from a web interface. If your host only provides access to the CGI or FastCGI PHP binaries, this script will not work with them. The solution to this issue is tied to the time constraint above.
- Some servers do not fully support this scan method. The usual symptoms will be a scan which starts but is intermittently or consistently aborted in mid-process without any further error messages and no indication of something going wrong. In such a case, trying running the scan from the back-end of your site will work properly. If you witness similar symptoms, you can most likely not automate your site's scan.

8.6. Automating the scans (scheduling URL)

Tip

Consult the Automatic Scanning page of the plugin for detailed information, tailored to your site, without having to read this documentation page.

The front-end scheduling URL feature is intended to let you perform an unattended, scheduled scan of your site. This is not the recommended method to do it, though. You should only use this method if the regular command line CRON jobs are not supported by your server.

The front-end backup URL performs a single scan step and sends a redirection (HTTP 302) header to force the client to advance to the next page, which performs the next step and so forth. You will only see a message upon completion, should it be successful or not. There are a few limitations, though:

- **It is not designed to be run from a normal web browser**, but from an unattended cron script, utilizing **wget** or **curl** as a means of accessing the function.
- The script is not capable of showing progress messages.
- Normal web browsers tend to be "impatient". If a web page returns a bunch of redirection headers, the web browser thinks that the web server has had some sort of malfunction and stop loading the page. It will also show some kind of "destination unreachable" message. Remember, these browsers are meant to be used on web pages which are supposed to show some content to a human. This behaviour is normal. Most browsers will quit after they encounter the twentieth page redirect response, which is bound to happen. Do not come to tell us that Firefox, Internet Explorer, Chrome, Safari, Opera or another browser doesn't work with the front-end backup feature. It was NOT meant to work by the browser's design.
- Command line utilities, by default, will also give up loading a page after it has been redirected a number of times. For example, **wget** gives up after 20 redirects, **curl** does so after 50 redirects. Since Admin Tools redirects once for every of the several dozens of scan steps it is advisable to configure your command line utility with a large number of redirects; about 10000 should be more than enough for virtually all sites.

Tip

Do you want to automate your scans despite your host not supporting CRON? Webcron.org [<http://webcron.org/>] fully supports Admin Tools' front-end scan scheduling feature and is dirt cheap - you need to spend about 1 Euro for a year of daily site scan runs. Just make sure you set up your Webcron CRON job time limit to be at least 10% more than the time it takes for Admin Tools to perform a scan of your site.

Before beginning to use this feature, you must set up Admin Tools to support the front-end scan scheduling option. First, go to Admin Tools' main page and click on the Malware Detection, Scanner Settings button. Find the option titled Frontend and set it to **Yes**. Below it, you will find the option named Secret key. In that box you have to enter a password which will allow your CRON job to convince Admin Tools that it has the right to request a backup to be taken. Think of it as the password required to enter the VIP area of a night club. After you're done, click the Save button on top to save the settings and close the dialog.

Tip

Try entering a complex password here. Do note that special characters and non-latin letters need to be "URL escaped" (written as something like %20, i.e. percent sign followed by two hexadecimal digits) in the scheduling URL. The easiest way to get the correct URL is using the PHP File Scanner Scheduling button in Admin Tools' main page.

Most hosts offer a CPanel of some kind. There has to be a section for something like "CRON Jobs", "scheduled tasks" and the like. The help screen in there describes how to set up a scheduled job. One missing part for you would be the command to issue. Simply putting the URL in there is not going to work.

Warning

If your host only supports entering a URL in their "CRON" feature, this will most likely not work with Admin Tools. There is no workaround. It is a hard limitation imposed by your host. We would like to help you, but we can't. As always, the only barrier to the different ways we can help you is server configuration. You can, however, use a third party service such as WebCron.org.

If you are on a UNIX-style OS host (usually, a Linux host) you most probably have access to a command line utility called **wget**. It's almost trivial to use:

```
wget --max-redirect=10000 "http://www.yoursite.com/wp-content/plugins  
/admintoolswp/filescanner.php?key=YourSecretKey"
```

Of course, the line breaks are included for formatting clarity only. You should not have a line break in your command line!

Important

Do not miss the **--max-redirect=10000** part of the **wget** command! If you fail to include it, the backup will not work with **wget** complaining that the maximum number of redirections has been reached. This is normal behavior, it is not a bug.

Important

YourSecretKey must be URL-encoded. You can use an online tool like <http://www.url-encode-decode.com> or simply consult the PHP File Change Scanner Scheduling page.

Warning

Do not forget to surround the URL in double quotes. If you don't the scan will fail to execute! The reason is that the ampersand is also used to separate multiple commands in a single command line. If you don't use the double quotes at the start and end of the scheduling URL, your host will think that you tried to run multiple commands and load your site's homepage instead of the front-end scheduling URL.

If you're unsure, check with your host. Sometimes you have to get from them the full path to **wget** in order for CRON to work, thus turning the above command line to something like:

```
/usr/bin/wget --max-redirect=10000 "http://www.yoursite.com/wp-content/plugins  
/admintoolswp/filescanner.php?key=YourSecretKey"
```

Contact your host; they usually have a nifty help page for all this stuff. Read also the section on CRON jobs below.

wget is multi-platform command line utility program which is not included with all operating systems. If your system does not include the **wget** command, it can be downloaded at this address: <http://wget.addictivecode.org/FrequentlyAskedQuestions#download>. The **wget** homepage is here: <http://www.gnu.org/software/wget/wget.html>. Please note that the option **--max-redirect** is available on **wget** version 1.11 and above.

Important

Using a web browser (Internet Explorer, Google Chrome, ...) or **wget** version 1.10 and earlier will most probably result into an error message concerning the maximum redirections limit being exceeded. This is *not* a bug. Most network software will stop dealing with a web site after it has redirected the request more than 20 times. This is a safety feature to avoid consuming network resources on misconfigured web sites which have entered an infinite redirection loop. Admin Tools uses redirections creatively, to force the continuation of the scan process without the need for client-side scripting. It is possible, depending on site size, Admin Tools configuration and server setup, that it will exceed the limit of 20 redirections while performing a site scan operation.

Warning

The ampersands above should be written as a single ampersand, not as an HTML entity (&);. Failure to do so will result in a 403: Forbidden error message and no backup will occur. This is not a bug, it's the way **wget** works.

9. Web Application Firewall

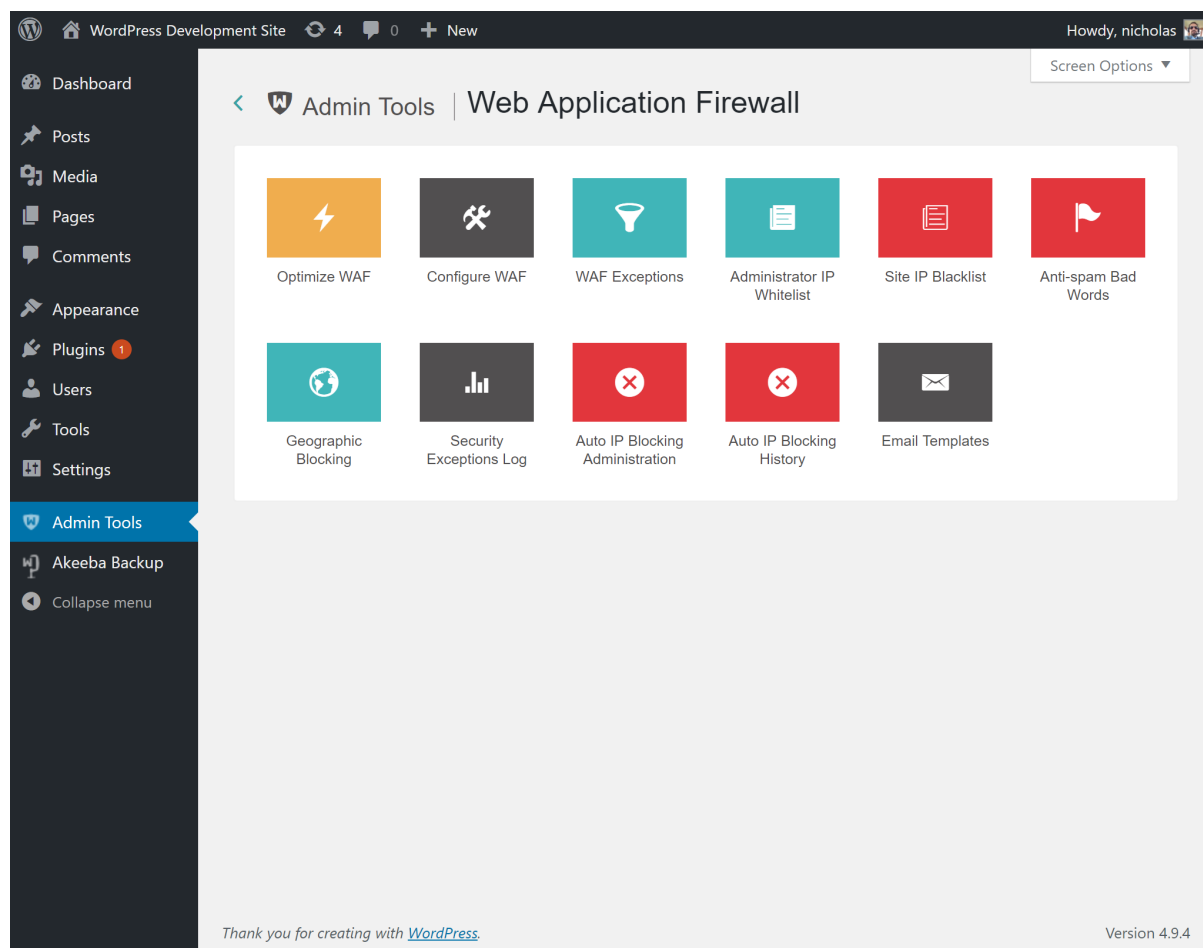
Note

Some of the features described below are only available in the Professional release

The Web Application Firewall feature of Admin Tools is designed to offer real-time protection against the most common attacks, including the fingerprinting attacks used by attackers to deduce information about your site in order to tailor an attack to it.

When you launch the Web Application Firewall feature of Admin Tools you are presented with its control panel page:

The Web Application Firewall page



Clicking on any icon will take you to the respective page.

Help! I used WAF and now I am locked out of my site

Open your site with an FTP programme or using your hosting provider's File Manager feature. Go to the web root of your site, typically called `public_html` or `htdocs`. If you're not sure please ask your host.

Navigate into the folder `wp-content/plugins/admintoolswp/app/plugins/waf/admintools`

There's only one file called `main.php` Rename it to `main.php.bak`

Now you have regained access to your site.

Go to Admin Tools, Web Application Firewall and fix the issue that caused you to get locked out (see the "How do I unblock myself" section below).

After you're done rename the `main.php.bak` file back to `main.php` for WAF to be active again and protect your site.

How do I unblock myself

See the section above for regaining access to your site.

In most cases the easiest way to unblock yourself is simply going to Admin Tools and click the big Unblock My IP button. If this doesn't work, or the button is not visible, follow the instructions below.

Do remember to rename back main.php -or run Optimize WAF again- after you're done unblocking yourself!

Automatically banned IP address

Go to Web Application Firewall and click the Security Exceptions Log button. Delete all records with your own IP address.

Then, go back to Web Application Firewall and click on the Auto IP Blocking Administration button. Select the record showing your IP address and click on the Delete button to delete the block.

Tip

Don't know what your IP address is? Just visit whatismyipaddress.com [<http://whatismyipaddress.com>] to find out!

If this problem keeps happening without you doing anything and the IP blocked is NOT the same as the one reported by whatismyipaddress.com [<http://whatismyipaddress.com>] you will have to do one more thing. Go to Admin Tools, Web Application Firewall and click on the WAF Configuration button. In the first tab set Enable IP workarounds to Yes.

If that was not the case, you have two options. The first is to troubleshoot the reason of the ban. Go to Admin Tools, Web Application Firewall, Security Exceptions Log and check the Reason and Target URL for the entries which have your IP address in the IP address field. Find the reason in the "List of blocking reasons" documentation page to find out why you're being blocked. If you are not sure what that means, please file a support ticket remembering to copy the information from the Security Exceptions Log. Kindly note that you need to have an active subscription to receive support.

The second option at your disposal is adding your IP address to either of the IP whitelists, as follows.

The first approach is to add your IP address to the Administrator IP Whitelist. Using this option will limit access to the administrator section of your site only to the IPs listed in the whitelist. We strongly recommend you to not use it unless you and all of your back-end users have static IP addresses. In all other cases you may get blocked out of your site. Go to Admin Tools, Web Application Firewall and click the Administrator IP Whitelist button. Add your own IP address.

The second approach is to use the Safe IP List. All IPs in that list will not be automatically banned. In order to do that, go to Admin Tools, Web Application Firewall and click on the WAF Configuration button. Inside the Auto-ban Repeat Offenders area find the Never block these IPs field. This is a comma-separated list. Add the IPs you want to never be automatically blocked separated by commas on that list.

Administrator IP white-listing

If you have enabled administrator IP white-listing, you have to make sure that your IP address is included in the white-list in order to be able to access your site. Go to Admin Tools, Web Application Firewall and click the Administrator IP Whitelist button. Add your own IP address.

Warning

Don't use the Administrator IP Whitelist if your ISP assigns an IP address dynamically. This is the default unless you are paying them extra for a "static IP".

Please note that having a dynamic DNS solution, such as what is offered by Dyn.com, and having a static IP address are two exactly opposite things. The former regularly updates a DNS entry (domain name) to point to your ever changing IP address. The latter means that your IP address never, ever changes. Using the IP whitelisting requires a static IP address which never, ever changes. If all you got is a dynamic DNS solution then this feature is NOT for you and you should not use it.

Also bear in mind that using dynamic DNS for IP whitelisting would not only make your site very slow (as you'd have to resolve the dynamic domain on every page load) but you'd also have a security risk e.g. by having an attacker forcibly disconnect you from the ISP, hijacking your dynamic DNS account etc.

IP black-listing

If you have enabled IP black-listing, you have to make sure that your IP address is not included in the blacklist in order to be able to access your site. Go to Admin Tools, Web Application Firewall and click the Site IP Blacklist button. Remove your own IP address.

Administrator Secret URL parameter

The immediate symptom to that is that you cannot access `/wp-admin` on your site.

If you have forgotten your Administrator Secret URL parameter go to Admin Tools, Web Application Firewall, Configure WAF, click on the Basic Protection Features tab and find the Administrator secret URL parameter option. Change or remove all of the text in that box to reset or unset, respectively, this feature.

Please remember that you should only use lowercase and uppercase letters A-Z without accents or diacritics, numbers 0-9, underscores and dashes only in your secret URL parameter. If you are using any different character you will need to URL-encode it or your browser will NOT be able to communicate it correctly to your server, therefore leading to your inability to access your site.

Please keep in mind that on most servers the secret URL parameter is case sensitive, i.e. `abc`, `ABC` and `Abc` are three *different* parameters.

Finally, please note that on some servers you may have to access your site's wp-admin as `https://www.example.com/wp-admin/index.php?secret` where `https://www.example.com` is the URL to your site and `secret` is your administrator secret URL parameter. Pay attention to the `/index.php?` part (including the slash and the question mark) in that URL. Some servers really do require that bit.

9.1. How WAF works and optimization

Note

Some of the features described below are only available in the Professional release

The Web Application Firewall is a series of individual protection features which run at various stages of WordPress preparing a page for display.

These features can be loaded by either of two ways.

- **Regular WordPress plugin.** This is the simplest and recommended method for most users. Admin Tools installs the file `wp-content/mu-plugins/admintoolswp.php` (relative to your site's root directory). This file runs every time WordPress is processing a page. It uses WordPress hooks to trigger the relevant features when something interesting happens. While this is the simplest method to run Admin Tools, it only protects code running inside WordPress itself. If you have a plugin with directly web accessible .php files which do not load WordPress they are left unprotected. As a result they can be used to hack your site.

PROS: Easier to implement. Less likely to interfere with third party software running outside WordPress.

CONS: Does not protect against vulnerabilities in web accessible .php files which don't go through WordPress.

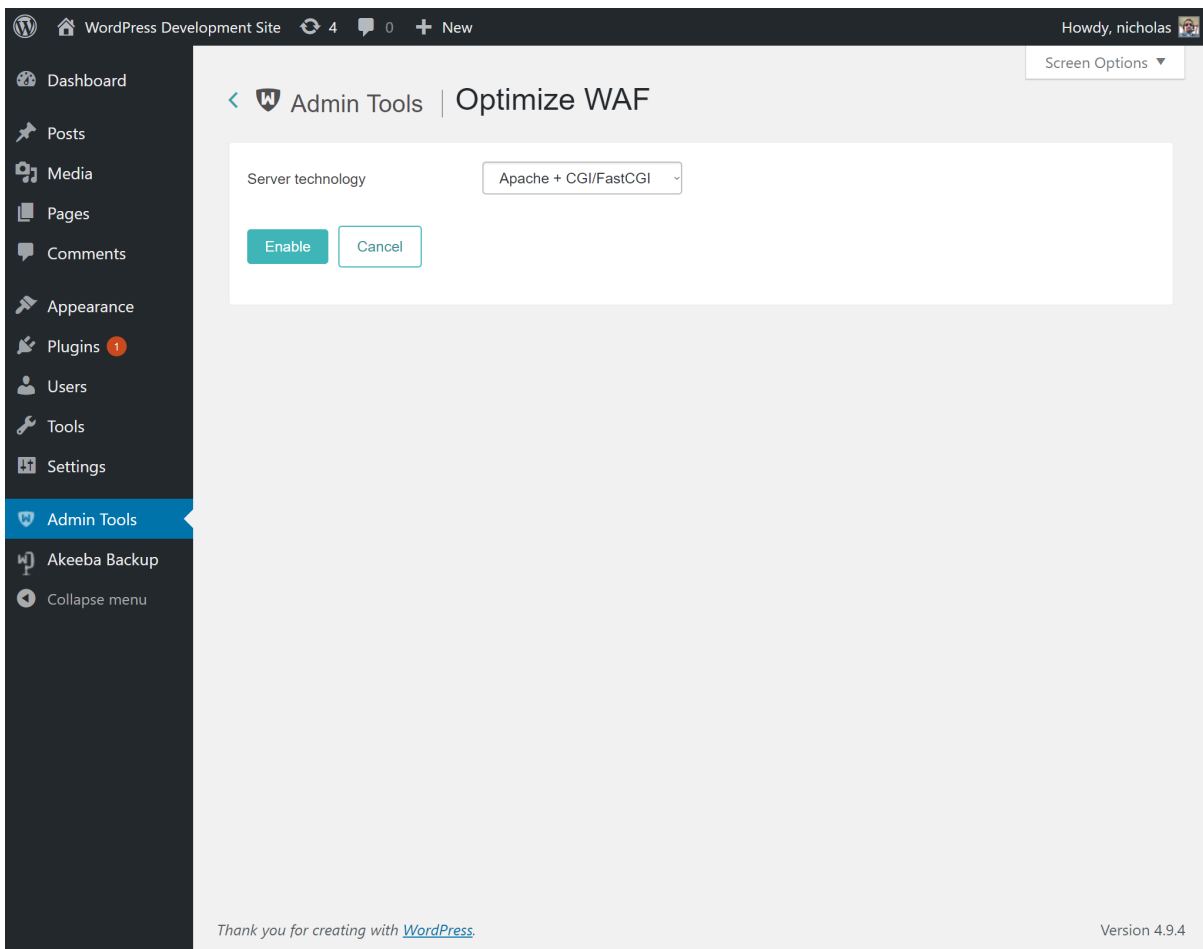
- **Auto-prepend script.** In this mode you tell your web server to load Admin Tools' Web Application Firewall every time it tries to process a .php file, be it one of WordPress' files or any directly web accessible script. While this is the most powerful method it has two disadvantages. First, you need to know the exact server technology you are using so that the correct .htaccess code can be generated. Second, it only works on Apache and LiteSpeed web servers which understand .php files (otherwise you'd have to modify your PHP configuration).

PROS: Offers more complete protection.

CONS: Harder to implement. More likely to interfere with third party software running outside WordPress.

The Optimize WAF page allows you to apply the Auto-prepend Script mode. You will need to select the technology used by your web server:

The Optimize WAF page



If you are not sure which server technology is used by your site's server please ask your host. They know and they can tell you very easily which one of the options applies to you. It is, however, impossible for you, us or any third party which hasn't set up the server to tell which technology is being used without a lot of trial and error.

I tried using this feature and my site broke. Help!

Open your .htaccess file over FTP or through your hosting provider's File Manager feature. It's located in the web root of your site, typically called public_html or htdocs. If you're not sure please ask your host.

Find the lines

```
# +++OptimizeWaf+++
```

and

```
# ---OptimizeWaf---
```

in that file. Delete everything between them, including these two lines.

Save the file.

Note

The next steps may not apply to you. Under some server technologies there is no `.user.ini` file created.

Next up, open the file `.user.ini` (note the leading dot!) in your site's root. If you do not see that file please make sure that your FTP client or your hosting provider's file manager are configured to show hidden files. All files whose name starts with a dot are hidden on most servers.

Find the lines

```
; AdminTools WAF
```

and

```
; END AdminTools WAF
```

in that file. Delete everything between them, including these two lines.

Save the file.

On some hosts you may have to wait a few minutes for the changes in these two files to take effect.

I have an NginX or IIS server

It should be possible by using the `Apache + CGI/FastCGI` option on this page. This creates a `.user.ini` file in your site's root to load the auto prepend file `admintools-waf.php` created in your site's root. This is something which works with all FastCGI implementations, including the ones used by NginX and IIS.

If you have a *really* old IIS server which uses PHP as a SAPI filter you're out of luck. Also, you're running an obsolete version of PHP with known security vulnerabilities. The only reasonable thing to do is upgrade PHP to a modern version. By doing so you *have* to use PHP in CGI or FastCGI mode, therefore you can use the Optimize WAF feature.

I am using the FastCGI option but it keeps telling me that the changes have not taken effect

This feature creates a `.user.ini` file in the root of your site (the same folder where your site's main `index.php` file is located in). The contents of these files are cached. By default, the cache time is 5 minutes. Some hosts increase the cache time up to an hour. So the first thing you should do is wait for up to an hour.

If nothing happens after more than an hour it's possible that you have a problem with `.user.ini` files not cascading properly. On most servers the settings of `.user.ini` files *cascade*, i.e. they are applied when accessing PHP files inside any subdirectory of the main directory where the `.user.ini` file is located. However, if you are on Windows or using a thread pool for your FastCGI implementation it's possible that the `.user.ini` files do NOT cascade. In this case please copy the `.user.ini` file into all subdirectories of your site. Alternatively, copy its contents into your site's PHP configuration (`php.ini` file) if possible. Finally, there's another alternative: convert its contents into `.htaccess` code and place that code into your site's `.htaccess` file.

If you are unsure what any of this means please do ask your host and show them this documentation page. They know how their server is set up and they can guide you on which steps are necessary.

9.2. Configure

Note

Some of the features described below are only available in the Professional release

This page is where all the configuration fine-tuning of the firewall takes place. By default, only very basic features are enabled during installation. You will have to enable more advanced features manually. Once you are content with your options click on Save to save the changes and return to the WAF panel page, or Back to return without saving.

Important

If you do something wrong and you inadvertently lock yourself out of the administrator area of your site, do not panic! Read this page [<https://www.akeeba.com/documentation/troubleshooter/atwpwafissues.html>] about regaining entrance.

The Configure WAF page is split into several tabs (or option groups, if you enabled the Long Configure WAF Page parameter in the component's Options page) to make it easier for you to locate the correct option. The documentation of this page is organized as one section per tab to help you locate the option you are looking for.

9.2.1. Basic Protection Features

WAF: Basic Protection Features

WordPress Development Site 4 0 + New Howdy, nicholas

Admin Tools | Configure WAF

Basic features Request Filtering Hardening Options Cloaking Project Honeypot Exceptions Auto-ban Logging & Reporting Customisation

Enable IP workarounds Yes No

If your server is behind a reverse proxy, a cache (e.g. Varnish) or a CDN you may need to enable this option. Do NOT enable sites not using such a setup because it will degrade your security. If you are unsure look below: Admin Tools will ask your browser to detect the recommended setting for this option.

The recommended setting for your site is: Yes

Allow access to Administrators that are in the WhiteList IP only Yes No

When enabled, only Administrators in the IPs in the Whitelist (see the [Administrator IP Whitelist](#) feature) will be allowed to access the site. All other attempts to access the administrator pages will be redirected to the site's home page. Be careful when using this feature! If you haven't added your own IP to the Whitelist you will get locked out of your site!

This will affect only Administrator roles, lower roles (ie Subscribers) will be able to login normally.

Disallow site access to IPs in Blacklist Yes No

When enabled, if the visitor's IP is in the Blacklist (see the [IP Blacklist](#) feature) they will immediately get a 403 Forbidden error message upon trying to access your site.

Administrator secret URL parameter

For example, if you enter "test", then you will only be able to access your administrator area by typing the URL <http://www.example.com/wp-admin/?test>. **WARNING! IT MUST START WITH A LETTER, NOT A NUMBER.** For better compatibility across servers, please use lowercase ASCII characters and numbers only (a-z, 0-9).

Change admin URL

Hides the login pages (`wp-Login.php`, `wp-admin`, `Login`, `admin`). Please use only alphanumeric character, underscore (`_`) and dash (`-`). The following words can not be used since they have a special meaning in WordPress: `dashboard`, `admin`, `Login`, `wp-Login.php`.

Define a custom slug for user registration, for example `new_account`

Defend against plugin deactivation Yes No

When enabled, Admin Tools will prevent users from trying to deactivate the plugin. This means that you will also be unable to deactivate the plugin until you disable this option! Moreover please note that this has no effect against someone renaming or deleting the files of the Admin Tools plugin.

Away Schedule from (hh:mm) to (hh:mm)

i Current server time is 08:49. Please double check it and change the timezone in Wordpress settings if required.

Save Changes Cancel

Thank you for creating with [WordPress](#). Version 4.9.4

The Basic Protection Features section contains the very basic options which allow you to control who can access your site.

Enable IP workarounds

When this option is disabled (default on new installations) Admin Tools will get the visitor's IP only from the REMOTE_ADDR environment variable sent by your server to PHP. This is the most secure option but may cause a problem on certain sites which have a load balancer, reverse proxy, cache or CDN in front of the web server. In these cases the REMOTE_ADDR contains the IP address of the load balancer, reverse proxy, cache or CDN in front of the web server, NOT the IP address of the visitor. As a result all attacks will appear to be coming from the same IP address. Automatically or manually blocking this IP will disable your site for everyone. Moreover, features like IP whitelist, IP blacklist and so on will not work properly or at all.

On these setups Admin Tools you can set the Enable IP Workarounds option to Yes. This way Admin Tools can use the X-Forwarded-For HTTP header which is sent by the load balancer, reverse proxy, cache or CDN in front of the web server instead of REMOTE_ADDR. This HTTP header contains the real IP address of the visitor and Admin Tools' IP-based features will work properly.

This option must NOT be enabled on sites which are not behind a load balancer, reverse proxy, cache or CDN. If you do that then an attacker can send a X-Forwarded-For HTTP header to mask their IP address or perform a targeted denial of service attack.

If you are unsure about your setup there is a failsafe ways to figure out if you need to enable this feature. First, set it to No. Then wait until there is an attack on your site. Did your site become inaccessible **for everyone** after the last time Admin Tools detected an attack? Do you always see the same IP or variations of the same in the Security Exceptions Log? If the answer to both questions is "yes" then you must set the "Enable IP workarounds" option to Yes.

Allow administrator access only to IPs in Whitelist

When enabled, only IPs in the Whitelist (see the following sections of this documentation about configuring it) will be allowed to access the administrator area of the site. All other attempts to access the administrator pages will be redirected to the site's home page. Be careful when using this feature! If you haven't added your own IP to the Whitelist you will get locked out of your administrator area!

Please look into the IP Whitelist documentation section for more information.

Important

IPs added to the administrator IP whitelist are fully white-listed as far as Admin Tools is concerned. This means that no security measure will be applied against them. Please place only very well trusted IPs in this list! If an attack is launched from this IP, it will not be blocked by Admin Tools!

Disallow site access to IPs in Blacklist

When enabled, if the visitor's IP is in the Blacklist (see the following sections of this documentation about configuring it) they will immediately get a 403 Forbidden error message upon trying to access your site.

We recommend that you do not routinely add IPs which get automatically blocked to the Blacklist. Let Admin Tools manage IP blocking. Attackers usually employ dynamically assigned IPs which change over time or use compromised third party computers to launch their attacks from for a limited amount of time. If you blacklist these IPs you may end up permanently blacklisting legitimate traffic by accident, when these IPs are assigned to a different person. Likewise, if someone gets blocked by accident and you blacklist their IP you are actually blocking a legitimate user from your site. Admin Tools is very capable of managing IP blocking automatically, with a rolling time window, making it harder for attackers to attack your site while making sure that legitimate visitors are unlikely to be permanently banned by accident.

Administrator
secret URL
parameter

Normally, you can access your site's administrator area using a URL similar to `http://www.example.com/wp-admin`. Potential hackers already know that and will try to access your site's administrator area the same way. From that point they can try to brute force their way in (guess your username and password) or simply use the fact that a WordPress administrator area exists to deduce that your site is running WordPress and attack it using WordPress-specific attacks. Whatever you enter here you are required to include as a URL parameter in order to access your administrator area. For instance, if you enter the word *test* here you will only be able to access your site's administrator area with a URL similar to `http://www.example.com/administrator?test`. All other attempts to access the administrator area will be redirected to the site's home page. If you do not wish to use this feature, leave this field blank.

Important

The secret URL parameter *must* start with a letter. If it starts with a number, you will immediately get a "Illegal variable `_files` or `_env` or `_get` or `_post` or `_cookie` or `_server` or `_session` or globals passed to script" error when trying to access your site's administrator back-end. It should also contain only lowercase and uppercase ASCII characters and numbers (a-z, A-Z, 0-9), dashes and underscores in order to ensure the widest compatibility with all possible browser and server combinations.

Any other characters you use (such as: punctuation; special characters; Latin letters with accents or diacritics; Greek, Cyrillic, Chinese, Japanese and other ethnic script characters) will have to be URL-encoded. This makes it difficult and tricky to use, hence our recommendation not to use it.

Moreover note that some extended Unicode characters such as certain Traditional Chinese characters and Emoji cannot be used. They will be either rejected by the server or trigger a server protection which will lock you out from your site at the hosting level (you'll have to contact your host to unblock you).

Finally note that on most servers this is case sensitive, i.e. `abc`, `ABC` and `Abc` are three different secret words.

Tip

Some servers do not work when trying to access the protected administration area of your site with a URL in the format `http://www.example.com/wp-admin?test` (where `http://www.example.com` is the URL to your site and `test` is your administrator secret URL parameter) due to their configuration. You may want to try using `http://www.example.com/wp-admin/?test` (add a slash right before the question mark) or `http://www.example.com/wp-admin/index.php?test` (add `/index.php` right before the question mark). One of them is bound to work on your server. Unfortunately, there is no way to know which ones will work on your server except for trying them out. The first format (`http://www.example.com/wp-admin?test`) works on 95% of servers and that's what we recommend trying out first.

Change admin
URL

As explained in the option above, you can normally access your site's administrator area using a URL similar to `http://www.example.com/wp-admin` which is known to hackers with potentially negative consequences. This Admin Tools feature allows you to "cloak" the administrator login URL.

It's easier to explain this with an example. Let's say you use the setting `cupcake` in this Admin Tools option. When someone who is not already logged in to the administrator back-end tries to access `http://www.example.com/wp-admin` they will be redirected to the home page of your site and a security exception will be logged. When they try to access `http://www.example.com/cupcake` they will see the WordPress administration login page.

A few important notices regarding this feature:

- WordPress allows you to log into your site from its public area. If you are already logged into the public area as a user with a role that allows access to wp-admin you will be able to access your site's administration area as wp-admin. **This is not a bug, it is by design and makes perfect sense.** The objective of this feature is to cloak the administration login page. Once you are logged in with a user with an administrative role you have access to the administration area by definition.
- It **REQUIRES** a server setup which can use permalinks without index.php in them. Typically this means an Apache or LiteSpeed server which can understand .htaccess files. Alternatively, it can be an NginX, IIS, etc server as long as you have configured it properly per the instructions in the WordPress Codex for your particular server technology.
- You **MUST NOT** have any page or other route which is the same as or a subset of what you enter in this option. If you do you will lose access to that page / route the public area of your site.
- By using this option you are **NOT** renaming the wp-admin directory on the server. Doing so is not supported by WordPress and would break your site. This feature is a URL manipulation trick, a sort of smoke and mirrors to confuse hackers trying to brute force your administrator login. Even though it's a trick it is a very effective one!
- You **CAN** combine it with the Administrator secret URL parameter feature. In this case you need to access the login page as something like `http://www.example.com/cupcake?test` where "cupcake" is the setting of Change administrator login directory to and "test" is the setting of Administrator secret URL parameter.

Unlike using the Administrator secret URL parameter on its own you **MUST NOT** put a slash or /index.php before the question mark *even if your server required it before enabling the change administrator login directory option*. Remember that what you are accessing is not a real directory on your server, it is merely a URL manipulation trick.

- You **CAN** combine it with the Password-protect Administrator feature (assuming that you are using Apache or another server compatible with .htaccess and .htpasswd files). In fact, it is recommended.

Defend
against plugin
deactivation

Enabling this option will prevent any other Administrator / Super Administrator user from deactivating the Admin Tools plugin in WordPress' Plugins page. Use it in conjunction with the Master Password feature to avoid having other administrators of the site disable Admin Tools either on accident or on purpose.

Important

If you need to disable the Admin Tools plugin you must first disable this feature in the Configure WAF page and save your changes.

Away Schedule

By default, WordPress allows users with back-end access to log in to the site any time of the day. On smaller sites which have only a handful, or even just one, administrators on the same zone this means that someone can try to log in with a stolen username / password while you are fast asleep and unable to respond to the unexpected login. This where the Away Schedule comes into play. If a user with a role granting administration privileges tries to log into the public or administration area of your site between the "from" and "to" hour of the day they will be denied login. Moreover, if someone tries to access the administration area's login page during that time they will be redirected to the public area of the site – even if the have used the correct Administrator secret URL parameter.

Please note that this feature does not affect your regular users logging in to the front-end of your site. It only prevents users with a role which allows them to display the administration interface of WordPress.

The From and To time has to be entered in 24-hour format with trailing zeros, e.g. 09:15 for a quarter past 9 a.m. and 21:30 for half past 9 p.m. The time is entered in your server's timezone which may be different than the timezone you live in. For your convenience, the server's time at the time of the page load (in 24 hour format) is shown to you right below the Away Schedule.

9.2.2. Request Filtering

WAF: Request Filtering

WordPress Development Site 4 0 + New Howdy, nicholas

Admin Tools | Configure WAF

Basic features **Request Filtering** Hardening Options Cloaking Project Honeypot Exceptions Auto-ban Logging & Reporting Customisation

SQLiShield protection against SQL injection attacks Yes No
When enabled, Admin Tools will try to detect common SQL injection attacks against your site and block them.

Remote File Inclusion block (RFiShield) Yes No
Some hackers will try to force a vulnerable extension into loading PHP code directly from their server. This is done by passing an http(s):// or ftp:// URL in their request, pointing to their malicious site. When this option is enabled, Admin Tools will look for such cases, try to fetch the remote URL and scan its contents. If it is found to contain PHP code, it will block the request.

Remote PHP protocol block (PHPSHield) Yes No
Some hackers will try to read the files of your site using the php:// wrapper and some advanced PHP filters. When this option is enabled, Admin Tools will block every request that contains the php:// string

Direct File Inclusion shield (DFiSHield) Yes No
When this option is enabled, Admin Tools will search the request parameters for anything which looks like a file path. If one is found, it will be scanned. If it is found to contain PHP code, the request will be rejected.

Uploads scanner (UploadShield) Yes No
When this option is enabled, Admin Tools will proactively scan all files which are uploaded. If any of these files is found to contain even a single line of PHP code, the request is blocked. Do note that not all servers support this feature. If the uploaded files directory is blocked by open_basedir restrictions, no scanning will take place.

Anti-spam filtering based on Bad Words list Yes No
When enabled, all requests containing at least one word in the [Bad Words](#) list will be blocked.

Thank you for creating with [WordPress](#). Version 4.9.4

The Request Filtering section contains the essential defenses of the Web Application Firewall feature. Admin Tools will monitor incoming requests and the data that is submitted to your site, filter them using these options and decide which requests seem to be nefarious, blocking them.

SQLiShield protection against SQL injection attacks When enabled, Admin Tools will try to detect common SQL injection attacks against your site and block them. This solves one of the most common attacks against WordPress plugins so we recommend that you always leave it enabled.

But what is a SQLi attack? Quite a lot of WordPress plugin developers are hobbyists, without experience and / or security training; or mistakes do happen, as WooCommerce famously found out the hard way in early 2017. One of the common mistakes they do is to make assumptions about the nature or the content of user-submitted data, interpolating them into database queries as-is. Database queries are also called SQL queries (SQL, pronounced "sequel", is the shorthand for Structured Query Language, the programming language the database queries are written in). An attacker can exploit this mistake by sending data which have the effect of terminating the developer's database query and starting a new one which either dumps privileged data -such as usernames and passwords- or modifies data into the database - such as adding a new administrator user under the control of the attacker. This class of attacks is called an SQL Injection, or SQLi for short, since the attacker "injects" his own code into a SQL query running on the site.

Remote File
Inclusion block
(RFIShield)

Some hackers will try to coerce a vulnerable plugin into loading PHP code directly from their server. This is done by passing an http(s):// or ftp:// URL in their request, pointing to their malicious site. When this option is enabled, Admin Tools will look for such requests, try to fetch the remote URL and scan its contents. If it is found to contain PHP code, it will block the request.

Important

If your site starts throwing white pages when submitting a URL in your site's front-end, please disable this option. The white page means that your server is not susceptible to this kind of attack and doesn't properly advertise this to Admin Tools when requested. In this case, Admin Tools crashes while trying to scan the contents of the remote location, causing the white page error. Disabling this option in such a case poses no security risk.

The best way to deal with this issue is at the PHP level, by adding `allow_url_include = 0` in a new line inside your server's `php.ini` file or the `.user.ini` file in your site's root (if the latter file doesn't exist you can create it). In this case you can disable this Admin Tools option.

Remote PHP
protocol block
(PHPShield)

Some hackers will try to pass a request parameter beginning with the `php://` wrapper and specially crafted filters to coerce the server into executing malicious code. This is an advanced attack which can be easily blocked by Admin Tools when you enable this option. We recommend that you always enable this option.

Uploads scanner
(UploadShield)

When this option is enabled, Admin Tools will proactively scan all files which are uploaded through WordPress. If any of these files is found to contain PHP code the request is blocked. This can prevent some kinds of very tricky attacks, like uploading malicious PHP code wrapped inside avatar images. Do note that not all servers support this feature. If the uploaded files directory is blocked by `open_basedir` restrictions, no scanning will take place. If unsure, ask your host if they have put `open_basedir` restrictions which block access to the PHP uploads directory. If they answer affirmatively, this Admin Tools feature will not work unless this restriction is lifted.

Warning

NOT ALL PLUGINS ALLOW ADMIN TOOLS TO SCAN THEIR UPLOADS! Some components do not use WordPress' `index.php` entry point file. Instead, they use their own. Since these uploads do not pass through the WordPress application, Admin Tools' code doesn't run and these uploaded files are not scanned UNLESS you have used the Optimize WAF feature. In this case and if you have not enabled the Optimize WAF feature, if a plugin is found vulnerable your site will still be at risk. We suggest using the Optimize WAF feature for maximum protection of your site.

Anti-spam filtering based on Bad Words list

When enabled, all requests containing at least one word in the Bad Words list (configured separately, see the next sessions) will be blocked. By default the Bad Words list is empty; you have to configure it to match your site's needs. One good idea is to include pharmaceutical, luxury watches and shoes brand names, as this makes up the majority of comment and contact spam received on web sites.

9.2.3. Hardening Options

WAF: Hardening Options

The screenshot shows the 'Configure WAF' interface in the Admin Tools. The 'Hardening Options' tab is selected. The settings include:

- Login error message:** A text input field. Description: *WordPress leaks user information when the access credentials are wrong (ie "Wrong password for user..." or "Invalid username"). Changing the error message to something more obscure and generic will prevent attackers to gain such info.*
- Remove RSS links:** A toggle switch set to 'Yes'. Description: *This option will remove RSS links from your WordPress site header*
- Remove blog client links:** A toggle switch set to 'Yes'. Description: *This option will remove blog client links (such as Weblog and Windows Live Writer) from your WordPress site header*
- Change session duration:** Two input fields for 'regular login' and '"Remember me" login'. Description: *By default WordPress sets session duration to 48 hours or 2 weeks if the option "Remember me" is checked. Here you can tweak those settings and customize session duration. Leave the fields empty to use the default values.*
- Disable editing users' properties:** A toggle switch set to 'Yes'. Description: *When enabled, trying to modify the settings of an existing or create a new Administrator will fail.*
- Treat failed logins as security exceptions:** A toggle switch set to 'Yes'. Description: *When enabled, failed login attempts of any kind of user (even simple Subscribers users) count as security exceptions and are being logged in Admin Tools' Security Exceptions Log. There is a very useful implication to that. Since they count as security exceptions, they count towards the exceptions limit you set up in the automatic IP blocking. Therefore, after a number of failed login attempts, the user's IP will be automatically blocked for the duration you have set up.*
- Blocked email domains:** A large text area. Description: *Enter one domain for each line. Registration will be blocked if the user tries to use a domain contain in this list*

At the bottom of the main content area, there are 'Save Changes' and 'Cancel' buttons.

Footer text: *Thank you for creating with [WordPress](#).* Version 4.9.4

With the Hardening Options section you are able to harden the way some basic WordPress features work. These are advanced settings, so please make sure you understand what each option does before you enable it.

Login error message	<p>WordPress is very verbose when a user fails to login. It tells the user if the username is not found or the password is wrong. While this is useful for forgetful users, it's like striking gold for hackers. They can abuse these messages to figure out which usernames are used on your site and then launch a brute force attack (try many different common passwords until they're in).</p> <p>By setting some text in this option you will be replacing the login failure message with what you've entered, no matter if it's the username or the password which is wrong. We recommend setting it to something along the lines of "You have entered the wrong username, the wrong password or you don't have an account on our site".</p>
Remove RSS links	<p>Removes the RSS (feed) links from your site's pages. If someone knows, or guesses, the feed URL they can still access the RSS feed.</p>
Remove blog client links	<p>Removes the special links normally present on your site's pages which allow you to use third party blog editor applications. Obviously you should only enable this option if you're not using any such software.</p>
Change session duration	<p>WordPress keeps a user logged in for 48 hours or, if they have used the Remember Me feature, for 2 weeks. You can use this option to change the duration of the login session. It's recommended that you keep the regular login short, around 30 minutes, to contain the damage of any cookie stealing attacks against your device.</p>
Disable editing users' properties	<p>When enabled, trying to modify the settings of an existing or create a new user from WordPress' Users page will fail. You will need to disable this feature to create or edit WordPress users.</p>
Treat failed logins as security exceptions	<p>When enabled, failed login attempts of any kind of user (even simple users only allowed to comment on posts) count as security exceptions and are being logged in Admin Tools' Security Exceptions Log. There is a very useful implication to that. Since they count as security exceptions, they count towards the exceptions limit you set up in the automatic IP blocking. Therefore, after a number of failed login attempts, the user's IP will be automatically blocked for the duration you have set up. This will catch and block brute force attacks i.e. hackers trying different combinations of usernames and password against your site, in case they can guess a combination which lets them in.</p>
Disable XML-RPC	<p>WordPress 3.5 and later come with the XML-RPC services turned on by default, without any user controls to disable them. The XML-RPC services are used for remote control of your WordPress installation such as JetPack, the WordPress desktop and mobile apps, WP-CLI and remote blogging clients (think of something like Windows Live Writer or MarsEdit). They can also be extended by third party plugins to provide additional functionality which can be used to control aspects of your site remotely.</p> <p>XML-RPC services have been long linked to security issues. They accept XML-formatted content which has its challenges with regards to parsing it in a safe manner. Moreover, there is a very common attack due to the very nature of the XML-RPC services which is still in use: password brute forcing. The XML-RPC services run much faster than your site, bypassing your theme and other parts of your site which take a long time to process. Moreover, they accept a plain text username and password. If the username and password combination is incorrect they quickly respond with an error. If it's correct they provide meaningful output. This is used by attackers to try tons of different passwords in an effort to guess the one you are using. This is called brute forcing. Since XML-RPC is really fast, bypasses any two factor authentication plugin you may have installed and most other kind of account protection they provide a viable and practical way to perform brute-forcing on your site. This attack is mostly dealt with by using the "Treat failed logins as security exceptions" feature explained above. However, if you do not <i>absolutely need</i> remote access to your site it's advisable to disable</p>

XML-RPC services altogether to close every small loophole which could be abused by an attacker to gain a foothold on your site.

Please note that activating this feature does NOT completely block access to the xmlrpc.php file on your site (the XML-RPC services endpoint). It does, however, cause it to always reply with error code 405 even if the username and password is correct. Since the XML-RPC services always fail without trying to parse the data sent in the request they can no longer be abused by attackers for any of the attacks which would otherwise be possible with the XML-RPC services enabled.

We need to clarify that XML-RPC services are not a security threat by themselves. They can be a security threat if you or any of your privileged users do not follow security best practices. If you are using only plugins with good quality code and the passwords of your privileged (Author and above) users are secure you are safe, within reason. Secure passwords in this context mean truly random passwords consisting of at least 32 characters which are a mix of lowercase and uppercase letters, digits and symbols. As a rule of thumb, if you can memorize the password and you do not have an eidetic memory then your password is not secure. Always use random, long passwords stored in a password manager application such as 1Password, KeePass, LastPass etc.

As a final point, no, just because you have an obscure blog with a handful of visitors per month does not mean hackers will leave you alone. Hackers typically take over sites to send spam, host malware or attack other high-value sites. The more obscure your site the least likely they are to get caught. Therefore your site's obscurity makes it a desirable target.

Blocked email domains

Enter one domain per line, without the at sign.

If a user tries to register an account with an email address that uses one of these email domains they will be blocked. This is useful to block free mail services from certain countries which are commonly used by comment spammers.

9.2.4. Cloaking

WAF: Cloaking

The screenshot displays the 'Configure WAF' interface in the WordPress Admin Tools. The 'Cloaking' tab is active, showing the following configuration options:

- Hide/customise generator meta tag:** A toggle switch is set to 'Yes'.
- Generator tag:** A text input field contains the value 'MYOB'.

Below the input field, a note reads: "Enter a custom generator meta tag value, or leave blank to completely remove the tag". At the bottom of the configuration panel are 'Save Changes' and 'Cancel' buttons. The interface also includes a sidebar with navigation icons, a top navigation bar with 'Admin Tools | Configure WAF', and a 'Screen Options' dropdown.

The next section is called Cloaking and lets you change the way that certain WordPress features work. These features are commonly used by attackers to identify which sites run on WordPress (discovery phase of the attack). By cloaking your site against these methods of discovery you are less likely to be attacked. This doesn't mean nobody will attack you; it means that *fewer* hackers will end up attacking *you* compared to the next person running a WordPress site.

Hide/customise generator meta tag

All WordPress installations set the meta generator tag, a piece of HTML in the header of all pages, to advertise the fact that your site is running on WordPress. This information is cached

by search engines and is exploited by attackers who are looking for potential WordPress sites to target. Enable this option and enter a custom value for the generator tag in the next option to change the reported generator.

Generator tag When the previous option is enabled, this is what the generator meta tag's value will be.

9.2.5. Project Honeypot

WAF: Project Honeypot

WordPress Development Site | 4 | 0 | + New | Howdy, nicholas

Admin Tools | Configure WAF

Basic features | Request Filtering | Hardening Options | Cloaking | **Project Honeypot** | Exceptions | Auto-ban | Logging & Reporting | Customisation

Enable HTTP:BL filtering Yes No

*Enables the integration with [Project Honeypot](#). **IMPORTANT:** You need to register to Project Honeypot, get a key and enter it in the next option for this feature to work.*

[Project Honeypot](#) HTTP:BL Key

Enter your HTTP:BL key. You can sign up for Project Honeypot and get your key at http://www.projecthoneypot.org/httpbl_configure.php.

Minimum Threat Rating to block (0-255, default 25)

Project Honeypot uses a logarithmic "threat rating" to rank the possibility of a specific IP being a spammer. This options defines the minimum threat level an IP must have before it's blocked. A value of 25 means that this IP has submitted 100 spam messages on Project Honeypot's spam catching honeypots and is usually a safe indication that it belongs to a spammer. Do note that the rating is logarithmic. A value of 50 means 1,000 spam messages and a value of 75 means one million spam messages. Do not set it to values over 50, as you will most likely never block any spammer at all.

Maximum age of accepted HTTP:BL results

Project Honeypot reports when was the last time this IP was caught sending spam messages. The older this is (the higher the age is), the less likely is that this IP is still used by a spammer. You can chose here what will be the maximum reported age that will be blocked. The default value of 30 means that IPs which have submitted a spam message in the last 30 days will be blocked.

Also block suspicious IPs, not just confirmed spammers Yes No

Sometimes Project Honeypot is not sure if an IP belongs to a spammer or it's a hapless chap who clicked on the wrong link. In this case the IP is marked as "suspicious". The default behaviour is to not block these IPs. However, if you are receiving a lot of spam it's a good idea to enable this feature and block even "suspicious" IPs. Ultimately, some unfortunate users will be inadvertently blocked, so use this option with caution!

Thank you for creating with [WordPress](#). Version 4.9.4

Project Honeypot allows you to integrate with Project Honeypot's spam fighting services. Project Honeypot is a collective effort to detect spammers, email harvester and crackers. Its HTTP:BL service allows participants to

query the IP addresses of their visitors and figure out if it is a malicious user behind it. If you enable this feature, Admin Tools will check the IP address of each visitor and, if it is a malicious user, it will block them.

Important

Enabling Project Honeypot integration helps you fight spam but it's not a silver bullet against spammers! Some spammers will get past it. We recommend also using Akismet or any similar spam prevention service for best protection.

Finally note that Project Honeypot only blocks spammers coming to *your* site. If you are using a third party comments service such as Disqus or Facebook this protection will NOT apply to your spams in most cases (if they are managed through an IFRAME or third party JavaScript) for the simple reasons that the spammers do not interact with *your* site to post comments, they interact with the third party service *outside* of your site. This should be fairly obvious.

Enable HTTP:BL filtering	Turns the entire feature on and off
Project Honeypot HTTP:BL key	Enter your HTTP:BL key. You can sign up for Project Honeypot and get your key at http://www.projecthoneypot.org/httpbl_configure.php .
Minimum Threat Rating to block (0-255, default 25)	Project Honeypot uses a logarithmic "threat rating" to rank the possibility of a specific IP being a spammer. This options defines the minimum threat level an IP must have before it's blocked. A value of 25 means that this IP has submitted 100 spam messages on Project Honeypot's spam catching honeypots and is usually a safe indication that it belongs to a spammer. Do note that the rating is logarithmic. A value of 50 means 1,000 spam messages and a value of 75 means one million spam messages. Do not set it to values over 50, as you will most likely never block any spammer at all.
Maximum age of accepted HTTP:BL results	Project Honeypot reports when was the last time this IP was caught sending spam messages. The older this is (the higher the age is), the less likely is that this IP is still used by a spammer. You can chose here what will be the maximum reported age that will be blocked. The default value of 30 means that IPs which have submitted a spam message in the last 30 days will be blocked.
Also block suspicious IPs, not just confirmed spammers	Sometimes Project Honeypot is not sure if an IP belongs to a spammer or it's a hapless chap who clicked on the wrong link. In this case the IP is marked as "suspicious". The default behaviour is to not block these IPs. However, if you are receiving a lot of spam it's a good idea to enable this feature and block even "suspicious" IPs. Ultimately, some unfortunate users will be inadvertently blocked, so use this option with caution!

9.2.6. Exceptions

WAF: Exceptions

WordPress Development Site | 4 | 0 | + New | Howdy, nicholas

Admin Tools | Configure WAF

Basic features | Request Filtering | Hardening Options | Cloaking | Project Honeypot | **Exceptions** | Auto-ban | Logging & Reporting | Customisation

Never block these IPs

Enter a comma-separated list of IPs which should never be automatically blocked. For example, such a list can be 127.0.0.1, 123.124.125.126 Moreover you can use IP ranges (e.g. 127.0.0.1-127.0.0.10), implied IP range notation (127.0.0 for the entire 127.0.0.1 to 127.0.0.255 block) and CIDR block notation (e.g. 127.0.0/8) on top of plain old IP addresses.

Whitelisted domains

If the IP address of the visitor who raised a security exception resolves to a domain name ending in what you enter here they will not be blocked. Effectively, these domain names have a free pass on your site. Please note that a long list will cause a big performance impact. Enter a comma separated list of the domain names you want to whitelist. The default value is .googlebot.com, search.msn.com which whitelists the search engine indexers Google Bot (used by Google Search) and MSN Bot (used by Bing).

Save Changes | Cancel

Thank you for creating with [WordPress](#). | Version 4.9.4

Sometimes you do not want to block certain IPs or domain names. For example, you don't want to block Google Bot, MSN (Bing) Bot, a third party site management service, a third party CDN service you are using and so on. You can easily add Exceptions from blocking. You can set the following options to prevent Admin Tools from blocking certain IPs and domain names:

Never block these IPs	Enter a comma-separated list of IPs which should never be automatically blocked. For example, such a list can be 127.0.0.1, 123.124.125.126 Moreover, since Admin Tools 2.2.a3 you can use IP ranges (e.g. 127.0.0.1-127.0.0.10), implied IP range
-----------------------	--

notation (127.0.0. for the entire 127.0.0.1 to 127.0.0.255 block) and CIDR block notation (e.g. 127.0.0.0/8) on top of plain old IP addresses.

This field fully supports both IPv4 and IPv6 addresses.

You may enter a dynamic IP domain name prefixed by the at-sign (for IPv4) or hash-sign (for IPv6). This only applies if you are using a dynamic IP address domain provider (e.g. DynDNS). For example, if you are using DynDNS and your dynamic IP address domain name is example.dyndns.info and resolves to an IPv4 address you can enter @example.dyndns.info to whitelist your dynamic IPv4 address. Conversely, if your dynamic hostname resolves to an IPv6 address you can enter #example.dyndns.info to whitelist your dynamic IPv4 address. Be careful to enter the correct domain name or you may have a delay of up to 30" processing security exceptions.

Tip

If you are using the whitelist feature to allow access to the administrator section of your site only to specific IPs, these IPs are automatically added to the safe list of IPs which should never be automatically blocked.

Important

IPs added to this list are fully white-listed. This means that no security measure will be applied against them. Please place only very well trusted IPs in this list! If an attack is launched from this IP, it will not be blocked by Admin Tools!

Whitelisted domains

If the IP address of the visitor who raised a security exception resolves to a domain name *ending* in what you enter here they will not be blocked. Effectively, these domain names have a free pass on your site.

Warning

Malicious URLs from these domain names WILL be blocked but a. this will not be logged and b. their IP address will not be automatically blocked by the "Auto-ban Repeat Offenders" feature below. This is done to protect your site against reflected search engine attacks. Let us explain this.

Some hackers try to exploit search engines' eagerness to scan URLs, crafting malicious URLs to your site and putting them on their own sites. Search engines will see them and try to visit them on your site. You are whitelisting these search engines as you don't want to lock them out of your site. If the malicious URL wasn't blocked just because the request comes from a seemingly innocent source your site would be instantly hacked. That's why the malicious URLs are still blocked, just not logged or cause IP addresses to be automatically banned.

Enter a comma separated list of the domain names you want to whitelist. The default value is .googlebot.com, .search.msn.com which whitelists the search engine indexers Google Bot (used by Google Search) and MSN Bot (used by Bing).

9.2.7. Auto-ban

WAF: Auto-ban

The screenshot shows the 'Configure WAF' interface for the 'Auto-ban' tab. The interface includes a navigation menu on the left and a main configuration area with several settings:

- IP blocking of repeat offenders:** A toggle switch is set to 'Yes'. Below it, a note states: "When set to yes, the IP address of repeat offenders will be automatically banned based on the rest of the settings".
- Email this address after an automatic IP ban:** A text input field contains 'nicholas@akeebabackup.com'. A note below explains: "Admin Tools can optionally send you an email when an IP is automatically banned, to the email address entered in this field. Leave this field empty (default) to disable this feature."
- Block after:** Two input fields are set to '3' and '1', followed by a dropdown menu set to 'minutes'. A note states: "Chose how many attacks have to happen within how much time. For example, if you set it to 3 attacks in 1 hour, Admin Tools will ban a IP address from which at least 3 attacks have been blocked within the last hour."
- Block for this long:** An input field is set to '15' and a dropdown menu is set to 'minutes'. A note states: "How long the block will last. For example, setting it to 1 day will block all access from this IP address for a whole day."
- IP blacklisting of persistent offenders:** A toggle switch is set to 'Yes'. A note below explains: "If an IP triggers this many auto-bans it will be permanently banned (added to the IP blacklist) if they are about to be auto-banned again. Make sure that you turn on the IP blacklisting by setting Disallow site access to IPs in Blacklist to Yes, otherwise the permanent blacklisting will have no effect."
- Permanently blacklist IP after:** An input field is set to '3' followed by the text 'automatic IP blocks'. A note states: "When the previous option is enabled, after how many auto-bans an IP will be permanently banned (added to the IP blacklist)."
- Show this message to blocked IPs:** A text input field contains 'You are a spammer, hacker or an otherwise bad pers'. A note below explains: "Allows you to show a specific message to blocked IP addresses. You may want to explain to the user that his IP was blocked because suspicious activity was detected as originating from his IP address. You can use the special text [IP] in all capital letters, without spaces between the brackets and IP, to display the user's IP in the message. This may be useful if someone gets accidentally blocked and asks you to help them."

At the bottom of the configuration area, there are two buttons: 'Save Changes' and 'Cancel'. The footer of the page includes the text "Thank you for creating with [WordPress](#)." and "Version 4.9.4".

You can easily Auto-ban IP addresses which repeatedly attack your site.

IP blocking of repeat offenders

When set to yes, the IP address of repeat offenders will be automatically banned based on the rest of the settings. This lets Admin Tools manage IP blocking automatically and is the recommended way to handle it. You **MUST** enable logging of security exceptions for this feature to work.

Email this address if an IP is auto banned	<p>Admin Tools can optionally send you an email when an IP is automatically banned, to the email address entered in this field. This will allow you, for example, to determine if some IP is being regularly blocked, in which case it may be a good idea to place it in the permanent IP black list. Leave this field empty (default) to disable this feature.</p> <p>The contents of the e-mails can be configured using the Email Templates feature in the Web Application Firewall page.</p>
Block after	<p>Chose how many attacks have to happen within how much time. For example, if you set it to 3 attacks in 1 hour, Admin Tools will ban a IP address from which at least 3 attacks have been blocked within the last hour.</p>
Block for this long	<p>How long the block will last. For example, setting it to 1 day will block all access from this IP address for a whole day.</p>
IP blacklisting of persistent offenders	<p>If an IP triggers many auto-bans over a period of time it will be permanently banned (added to the IP blacklist) next time they are about to be auto-banned again. Make sure that you turn on the IP blacklisting in the Basic features tab by setting Disallow site access to IPs in Blacklist to Yes, otherwise the permanent blacklisting will have no effect.</p>
Permanently blacklist IP after	<p>If an IP triggers this many auto-bans it will be permanently banned (added to the IP blacklist) when they are about to be auto-banned again. Make sure that you turn on the IP blacklisting by setting "Disallow site access to IPs in Blacklist" to Yes, otherwise the permanent blacklisting will have no effect.</p>
Show this message to blocked IPs	<p>Allows you to show a specific message to blocked IP addresses. You may want to explain to the user that his IP was blocked because suspicious activity was detected as originating from his IP address.</p> <p>You can use the special text [IP] in all capital letters, without spaces between the brackets and IP, to display the user's IP in the message. This may be useful if someone gets accidentally blocked and asks you to help them.</p>

9.2.8. Logging and reporting

WAF: Logging and reporting

WordPress Development Site 4 0 + New Howdy, nicholas

Admin Tools | Configure WAF

Basic features Request Filtering Hardening Options Cloaking Project Honeypot Exceptions Auto-ban **Logging & Reporting** Customisation

Save user sign-up IP in User Notes Yes No

When enabled, the IP new users signed up from will be stored inside User Profile. Users created through the administration area will not have their IP saved as because it makes no sense to do so (it's an administrator registering the user account on their behalf). Third party components creating new user accounts may also not trigger the plugin event.

Log security exceptions Yes No

It is suggested to keep this option enabled. When enabled, all potential security breaches —blocked by Admin Tools— will be logged in the database and made available under the Security Exceptions Log tool.

IP Lookup Service

Link to an IP lookup service. {ip} will be substituted with the IP address. Default: http://ip-lookup.net/index.php?ip={ip}

Email this address on security exceptions

Enter an email address to be notified upon any security exception detected on your site. Leave blank to not be sent a notification. Make sure your site can send out emails first!

Email this address on successful backend login

Enter an email address to be notified upon a successful login of anyone in your site's administrator backend. Leave blank to not be sent a notification. Make sure your site can send out emails first!

Include password in failed login email Yes No

Should the incorrect password be included in the mail you receive when someone triggers a failed login? This only applies when Treat failed logins as security exceptions is enabled.

Do not log these reasons

Security exceptions caused by these blocking reasons will not be logged. As a result, IPs triggering this exception repeatedly will not be automatically banned from your site. Moreover, as there is no log, it will be impossible to tell why someone is being blocked from accessing your site when they trigger one of those reasons.

Do not send email notifications for these reasons

Security exceptions caused by these blocking reasons will not result in an email being sent to the email address specified in Email this address on security exceptions

Enable security exception email throttling Yes No

When enabled the frequency of emails sent by Admin Tools can be throttled down. See the Email Templates for the maximum email frequency settings.

Save Changes Cancel

Thank you for creating with [WordPress](#). Version 4.9.4

In the Logging and reporting section you can change the way Admin Tools logs and reports various activity items and security exceptions happening on your site.

Save user sign-up IP in the user profile When enabled, the IP from which new users signed up will be stored as a note in the user profile.

Important

This feature is guaranteed to work only when a user registers to your site using the public user registration form provided by WordPress. Users created through the Users page of the administration interface will not have their IP saved as a note because it makes no sense to do so (it's an administrator registering the user account on their behalf). Third party plugins creating new user accounts may also not trigger the hook we are using to be notified of user account creation..

Log security exceptions It is suggested to keep this option enabled. When enabled, all potential security issues — blocked by Admin Tools— will be logged in the database and made available under the Security Exceptions Log tool.

Turning on this option will also create a file named `admintools_security_issues.log` in your site's `wp-content/plugins/admintoolspw/app/log` directory. This contains all the debugging details of what Admin Tools detected whenever it issues a 403 error. When asking for support, please include this log or at least the portion relevant to the 403 error page you are receiving in order for us to better serve you. Do note that your logs directory **MUST** be writeable for the log file to be produced.

Important

When this option is turned off the automatic IP blocking of repeat offenders, automatic blacklisting of IPs and most email notification features will be deactivated.

Important

By default we are using a `.htaccess` file to prevent direct web access to the log file. This works on Apache and LiteSpeed web servers. If you are using a different server, such as NginX or IIS, you need to prevent direct web access to this directory. If you are not sure how to do that please ask your host.

IP Lookup Service Admin Tools will provide you with a link to look up the owner of an IP address in the emails it sends you, as well as the Security Exceptions Log and Auto IP Blocking Administrator pages. By default, it uses the `ip-lookup.net` service. This option allows you to use a different IP lookup service if you so wish.

Enter the URL of the IP lookup service you want to use in this text box. The `{ip}` part of the URL will be replaced with the IP address to look up. For example, the default URL (for `ip-lookup.net`) is `http://ip-lookup.net/index.php?ip={ip}`

Email this address on security exceptions Enter one or more email addresses (separated by commas) which will get notified whenever a security exception happens on your site. For example `alice@example.com` for one recipient only or `bob@example.com, charlie@example.net, diane@example.org` for multiple recipients. The email addresses need not be in the same domain name and don't even need to be users of the site itself. Any email address will do.

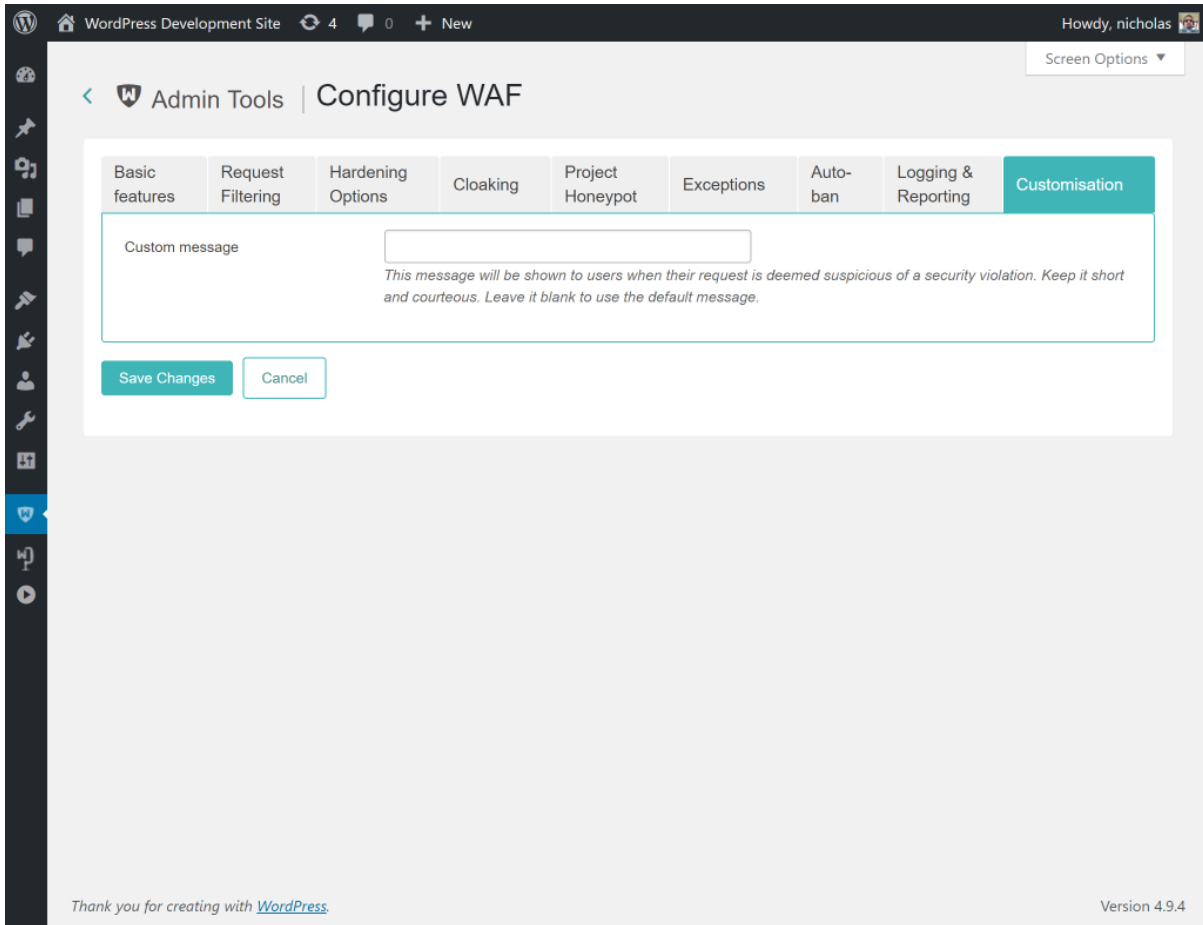
A "security exception" is anything which triggers Web Application Firewall. This is useful to get an ahead warning in the event of a bot trying to perform a series of attacks on your site.

The contents of the e-mails can be configured using the Email Templates feature in the Web Application Firewall page.

Email this address on successful administration login	<p>Enter an email address which will get notified whenever someone successfully logs in to your site's administration area (wp-admin). If you do not wish to use this feature, leave this field blank. If you enter an email address, every time someone logs in to the administration area an email will be sent out to this email address stating the username and site name. If you want to send a notification to multiple email addresses separate them with commas, e.g. <code>alice@example.com, bob@example.net</code>. The email addresses do not need to be in the same domain and they don't even have to be linked to users of your site.</p> <p>This allows you to get instant notification of unexpected administrator area logins which are a tell-tale sign of a hacked site. In that unlikely event, immediately log in to your site's back-end area, go to Admin Tools and click on the Emergency Off-Line Mode button. This will cut off the attacker's access to the entirety of your site and gives you ample time to upgrade your site and its extensions, as well as change the password (and maybe the username) of the compromised administrator account. For maximum security, after taking your site back on-line, log out, clear your browser's cookies and cache and log in again.</p> <p>The contents of the e-mails can be configured using the Email Templates feature in the Web Application Firewall page.</p>
Do not log these reasons	<p>Security exceptions caused by these blocking reasons will not be logged. As a result, IPs triggering this exception repeatedly will not be automatically banned from your site. Moreover, as there is no log, it will be impossible to tell why someone is being blocked from accessing your site when they trigger one of those reasons.</p> <p>For a list of what each reason means please consult the list of WAF log reasons. You can start typing or click on on the field to show the list of reasons.</p>
Do not send email notifications for these reasons	<p>Security exceptions caused by these blocking reasons will not result in an email being sent to the email address specified in "Email this address on security exceptions".</p> <p>For a list of what each reason means please consult the list of WAF log reasons. You can start typing or click on on the field to show the list of reasons.</p>
Enable security exception email throttling	<p>When this feature is set to Yes the email throttling options in the Email Templates feature in the Web Application Firewall page will be taken into account before sending an email to the email address specified in "Email this address on security exceptions". By default, Admin Tools will not send more than 5 emails in 1 hour. When this option is set to No there will be no limit on the amount of emails Admin Tools will send you. Disabling this can be a bad idea because it will slow down your server and fill up your inbox in the case of a bot performing a massive attack against your site.</p>

9.2.9. Customisation

WAF: Customisation



The Customisation section allows you to change the way Admin Tools presents the error message to people who are denied access to the site.

Customise
Security
Exceptions
message

This message will be shown to users when their request is deemed suspicious of a security violation. Keep it short and courteous. Leave it blank to use the default message.

9.3. WAF Exceptions

WAF Exceptions

The screenshot shows the WordPress Admin Tools interface for WAF Exceptions. The page title is "Admin Tools | WAF Exceptions". There are search filters for "Excluded URL" and "Description" with a "Search" button. Below the filters, there are "Bulk Actions" (Apply), "Add new", and "2 items" with pagination controls. The table contains the following data:

<input type="checkbox"/>	Excluded URL	Description	Exception type	Published
<input type="checkbox"/>	2018/*?/26/test-waf-exceptions	WAF Exception based on Regular Expression	RegEx	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2018/02/26/test-waf-exception	Exclude a specific URL	Exact	<input type="checkbox"/>

At the bottom of the page, there is a footer that says "Thank you for creating with WordPress." and "Version 4.9.4".

This page allows you to configure exceptions to the WAF filtering rules. Why you need that? Some plugins are designed to properly and safely parse and use data which triggers WAF protection rules. Most usually, a plugin accepts an absolute path to files on your server or can parse complex data which normally trigger WAF's filters. Without any exceptions set, these plugins would be blocked and you wouldn't be able to properly use your site. The workaround was to disable WAF's filters, but this ended up in degrading the security of your site. Using the WAF Exceptions view you can fine tune which URLs are in the "safe list" and should never be blocked.

Note

WAF Exceptions is a very useful and powerful tool. It's also possible that you apply too many exceptions, opening potential security wholes in the firewall. Be very cautious when using it. Please keep in mind that when you add an exception, WAF is COMPLETELY TURNED OFF for all requests matching the exception. If you apply a too broad exception you will be deteriorating your site's security to the level it was before installing Admin Tools for WordPress.

WAF Exception

The screenshot displays the 'Edit a WAF Exception' page in the WordPress Admin Tools. The left sidebar contains navigation links: Dashboard, Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, Settings, Admin Tools (highlighted), Akeeba Backup, and Collapse menu. The main content area shows the following form fields:

- Excluded URL:** 2018/02/26/test-waf-exception
- Description:** Exclude a specific URL
- Exception type:** Exact (selected), RegEx
- Published:** Yes (selected), No

At the bottom of the form are 'Save Changes' and 'Cancel' buttons. The footer of the page reads 'Thank you for creating with [WordPress.](#)' and 'Version 4.9.4'.

WAF Exceptions are defined by specifying the target URL: you can either specify an **Exact** match or a **RegEx** (Regular Exception) one.

- *Exact.* Using this matching option, you instruct Admin Tools to ignore any security exception coming from a specific URL
- *Regular Expression.* If you have several URLs that are triggering false positives, you can create a regular expression to exclude them all.

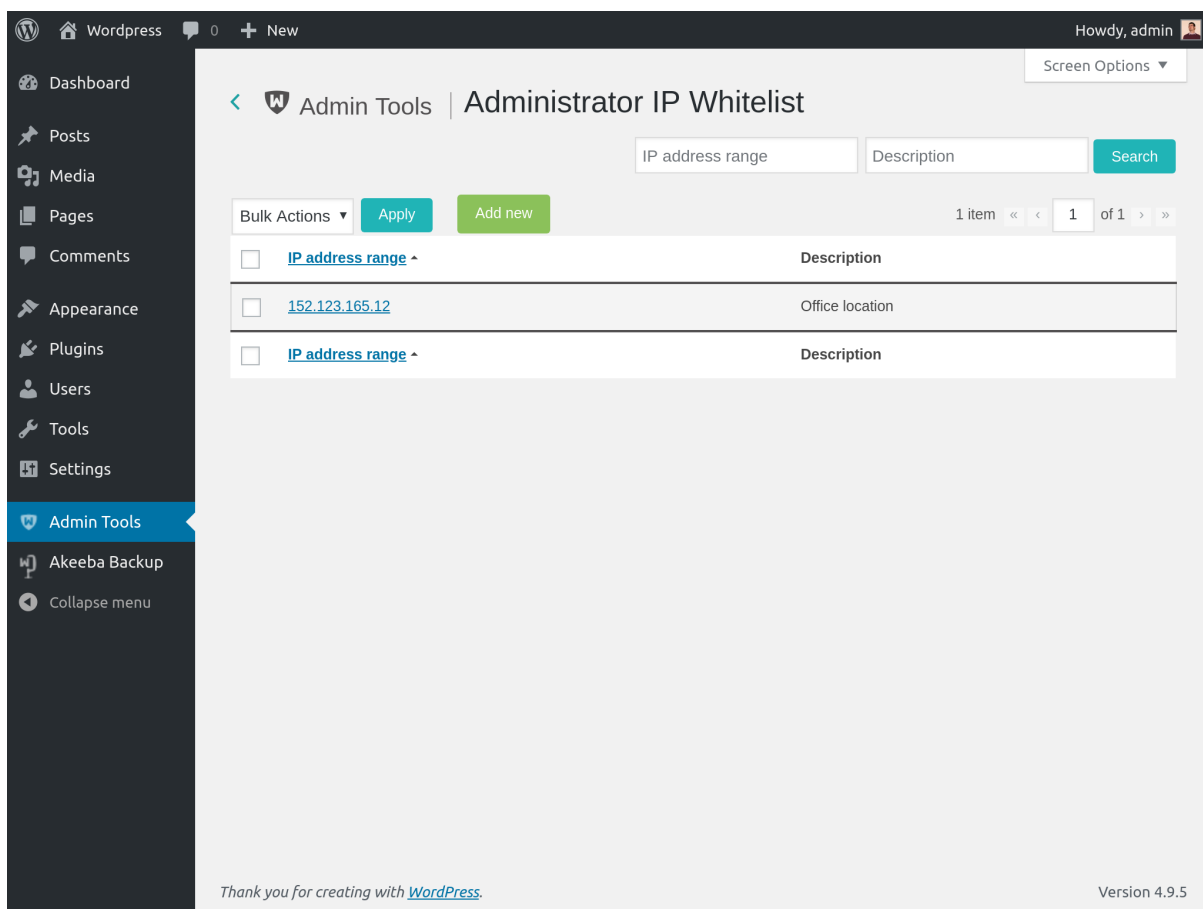
Important

Please note that when using a regular expression, you have to escape any regular expression character, by adding a leading backslash `\`. The most common character that should be escaped is the dash - here the full list:

```
\ ^ $ . | ? * + ( ) [ ] { }
```

9.4. Administrator IP Whitelist

The Whitelist management page



The screenshot shows the WordPress Admin Tools interface for the Administrator IP Whitelist. The top navigation bar includes the WordPress logo, 'Wordpress', a notification icon with '0', a '+ New' button, and a user profile 'Howdy, admin'. The main header shows 'Admin Tools | Administrator IP Whitelist' with a 'Screen Options' dropdown. Below the header are search filters for 'IP address range' and 'Description', and a 'Search' button. A 'Bulk Actions' dropdown is set to 'Apply', with an 'Add new' button. A pagination indicator shows '1 item' of '1'. The main content area contains a table with the following data:

<input type="checkbox"/>	IP address range ^	Description
<input type="checkbox"/>	152.123.165.12	Office location
<input type="checkbox"/>	IP address range ^	Description

At the bottom of the page, there is a footer with the text 'Thank you for creating with WordPress.' and 'Version 4.9.5'.

This page allows you to manage the IP Whitelist, defining the list of IPs or IP blocks which have access to your site's administrator area.

The Edit/Add page looks like this:

The Whitelist editor page

Tip

Your current IP address is displayed right above the edit box. Make sure that is the first to include so that you do not lock yourself out of your site's administrator area!

In the IP Address Range box you can enter an IP or IP range in one of the following ways:

- A single IP, e.g. 192.168.1.1
- A human readable block of IPs, e.g. 192.168.1.1-192.168.1.10
- An implied IP range, e.g. 192.168.1. for all IPs between 192.168.1.1 and 192.168.1.255, or 192.168. for all IPs between 192.168.0.1 through 192.168.255.255.
- A CIDR block [http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing], e.g. 192.168.1.1/8. If you don't know what this is, forget about it as you don't need it.
- A Subnet Mask [<http://en.wikipedia.org/wiki/Subnetwork>] notation, e.g. 192.168.1.1/255.255.255.0
- A dynamic IPv4 domain name prefixed by the at-sign. This only applies if you are using a dynamic IP address domain provider (e.g. DynDNS). For example, if you are using DynDNS and your dynamic IP address domain name is example.dyndns.info and resolves to an IPv4 address you can enter @example.dyndns.info to whitelist your dynamic IPv4 address. Be careful to enter the correct domain name or you may have a delay of up to 30" processing backend login requests and security exceptions. Please note that using the at-sign method ONLY works with IPv4 addresses. This is a limitation of PHP itself.
- A dynamic IPv6 domain name prefixed by the hash-sign. This only applies if you are using a dynamic IP address domain provider (e.g. DynDNS). For example, if you are using DynDNS and your dynamic IP address domain

name is `example.dyndns.info` and resolves to an IPv6 address you can enter `#example.dyndns.info` to whitelist your dynamic IPv6 address. Be careful to enter the correct domain name or you may have a delay of up to 30" processing backend login requests and security exceptions. Please note that using the hash-sign method **ONLY** works with IPv6 addresses. This is a limitation of PHP itself.

Do note that Admin Tools supports IPv4 and IPv6 (if your server supports IPv6) for any form of IP you enter yourself (single IP, human readable block, implied IP range, CIDR block and subnet mask notation).

Please pay attention to the differences between the at-sign and hash-sign notations' meanings. `@something` is IPv4 (e.g. `192.168.1.4`) whereas `#something` is IPv6 (e.g. `ffff::5678:90ab`). Do not use the at-sign for domains resolving to an IPv6 address or the hash-sign for domains resolving to an IPv4 address. Mixing this up can lead to long delays in page loads and / or being unable to access your site. Please keep in mind that the two different methods are required due to the way PHP works. They cannot be merged into a single method because that would considerably slow down every page load of your site.

Notes about using Dynamic IP Address Domain Names

Ideally, you should only use this feature if the IP address you are using to connect to the Internet never, ever changes. This is called a "static IP address" and it's usually an optional, extra cost, feature with most Internet service providers. Please note that having a dynamic DNS service, such as those provided by Dyn.com, is the exact opposite from having a static IP address: dynamic DNS services frequently update a domain name to point to your ever changing IP address.

While Admin Tools makes it possible to use a dynamic DNS for IP whitelisting it may be problematic for two reasons. First, it's terrible for performance as a DNS resolution must be done for every page load of your site where the IP whitelist must be read. This is any attempt to login as a user with administrative / editing privileges and every time there is a security exception raised. If your server does not cache IP resolution locally this can slow your site down considerably.

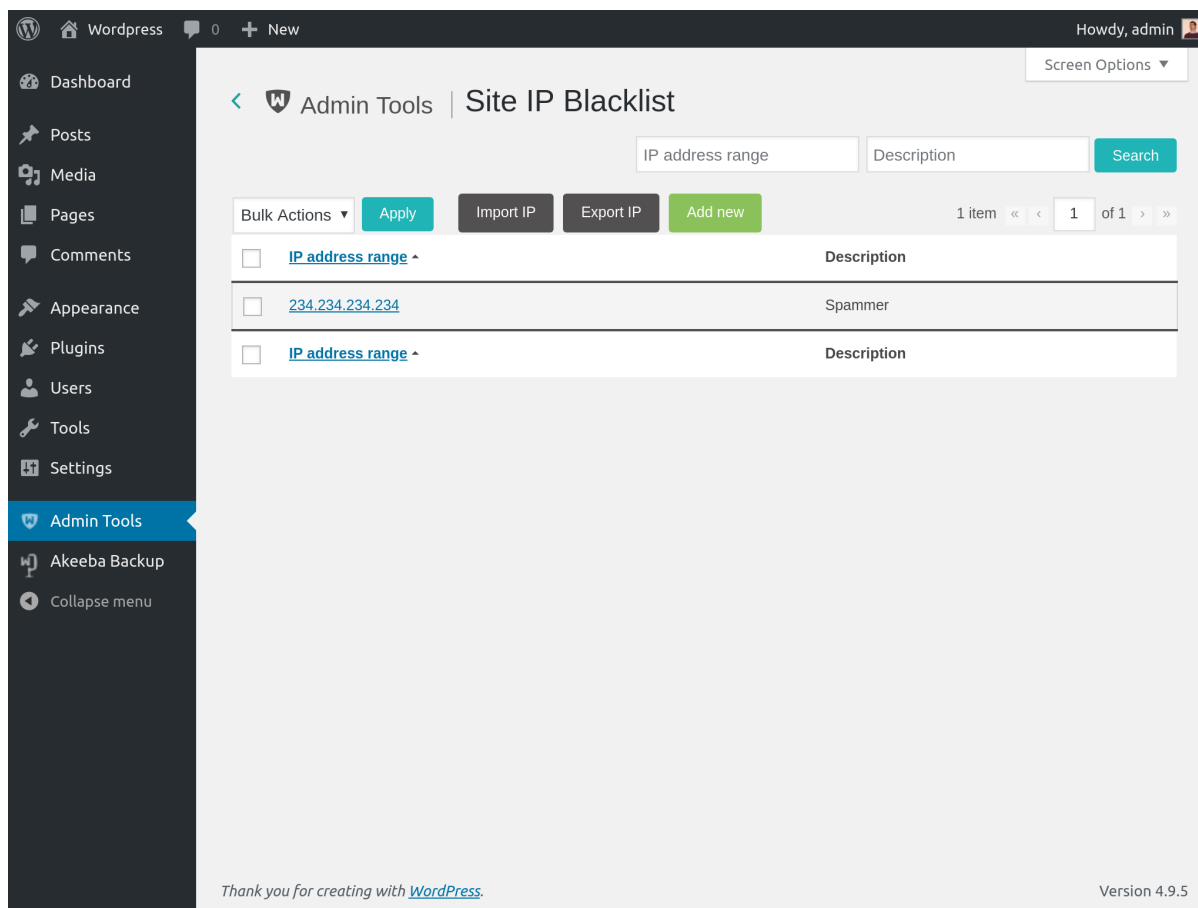
Furthermore, all dynamic IP providers have a default timeout for the dynamic DNS entries varying from 1 minute to 1 hour. If your IP changes within that period your server might be "blind" to the change. The same thing can happen if your dynamic IP updater (typically running in your router or NAS firmware) fails to update the dynamic DNS provider with your new IP address. At best this will be an inconvenience because you cannot access your site's administration until your dynamic DNS provider is updaters and your server "sees" the new IP address for that DNS entry. At worst, this can be initiated by a targeted attack to lock you out of your site while the attacker exploits a different path to gain access to your site, leaving you helpless.

Finally, bear in mind that you should never use this feature if you expect to need to log into your site as a user with editing / administrative privileges from an Internet connection with an unpredictable IP such as a public WiFi hotspot, a satellite Internet connection (e.g. those used in ships, airplanes and remote research stations) or a mobile broadband connection (including mobile-network-assisted Internet routers, even if your ISP is assigning a static IP address to your main, wired, Internet connection). **DO NOT, EVER, WHITELIST THE IP ADDRESS OF A PUBLIC, SHARED CONNECTION! YOU WILL GET HACKED!**

For the observant reader, we listed mobile broadband connections together with shared connections. This is not an oversight. Mobile Internet connections tend to recycle IP addresses far faster than their fixed (landline, fiber, cable, ...) counterparts. This is largely because of the ephemeral nature of the connection and the frequent hopping between areas of coverage and areas of non-coverage. Because of the fast rate of IP address recycling, using them for whitelisting ranges from very impractical to potentially dangerous (e.g. if an advanced attacker uses a malicious femptocell to launch a man-in-the-middle attack).

9.5. Site IP Blacklist

The Blacklist management page



This page allows you to manage the IP Blacklist, defining the list of IPs or IP blocks which do not have access to your site.

Do not overdo it with IP blacklisting!

Contrary to popular belief, you should not manually blacklist every single IP which appears to be attacking your site. This will have unintended consequences which work against your site and offer no additional protection.

First of all, not all detected attacks are actual attacks. Keep in mind that Admin Tools' Web Application Firewall, like every other WAF solution out there, is using a set of rules to determine the probability of a request being part of an attack and block it if it crosses a certain threshold. This means that there are a few cases of legitimate requests being mistakenly treated as attacks (false positives). This can happen when, for example, a user's browser keeps inserting the wrong password in the login form and the user not noticing and keep retrying to log in until they get blocked. You don't want to permanently blacklist that client of yours, now, do you?

Furthermore and most importantly the IP an attack to your site seems to come from is most likely not the IP address of the attacker himself. Even a semi-decent, wanna-be hacker would never use his home's Internet connection to launch an attack. That would be the equivalent of a burglar leaving his driver's license in the house he robbed. Instead, hackers use hacked devices (from a PC to a smart lightbulb and everything in between) of innocent people to launch their attacks from. Therefore the IPs you see attacking you and are tempted to block are innocent people. These are your potential clients. You don't want to block them.

Moreover, IPs are seldom static. They are dynamic. Most ISPs own a bunch of IP addresses. When your router connects to the Internet it is assigned a random address from that bunch. Many ISPs push that further, allocating

an IP address for a short time period (usually 1 to 12 hours) and assign you a different, random IP when that allocation expires. This is done for several performance and business reasons, but what you should remember is that the IP that attacks you today will most likely be assigned tomorrow to your potential client. You do not want to block them!

Finally, there's the performance aspect of IP blocking. Every time someone connects to your site, on every single page load, Admin Tools has to check their IP address against each and every entry of the blacklist. Every entry of the blacklist adds a bit of processing time on every page load. In most cases 50 to 100 blocked IPs will not have a severe impact on your page loading speed. Anything above that threshold has a measurable impact on your site's performance. Your site loads slower for everybody. Search engines pick that up and penalize your slow site by burying it dozens of spots lower in search rankings.

Essentially, the more blacklisted IPs you add the more potential clients you lose.

This leaves us with the question of why this feature exists and how you should deal with IP blacklisting.

There is a small, but large enough to be annoying, percentage of attacks originating from wanna-be hackers who use the same IP address to attack you over and over again. Usually they're running a dumb script with no error handling. Therefore even when Admin Tools blocks them automatically they keep trying and trying. The best thing you can do is, of course, blacklist their IP. Luckily, Admin Tools can do that for you! Just make sure that you enable the automatic IP banning and the permanent IP banning of repeat offenders in the Configure WAF page. Admin Tools will first issue a temporary ban against IPs which seem to be attacking your site. If they are persistent it will add them to the blacklist. This automatic management yields the best results for both performance and security.

So why do we have the IP blacklisting feature, again? Mostly to manage the automatically blacklisted IP addresses and to allow power users to add their own IPs which they do not want to access the site for reasons beyond security. So do yourself a favor and **do not manually blacklist IP addresses!** Managing blacklisted IPs manually is a *Terribly Bad Idea*.

Using the site IP blacklist

The Edit/Add page looks like this:

The Blacklist editor page

Tip

Your current IP address is displayed right above the edit box. Make sure that you do not include it so that you do not lock yourself out of your site's administrator area!

In the IP Address Range box you can enter an IP or IP range in one of the following ways:

- A single IP, e.g. 192.168.1.1
- A human readable block of IPs, e.g. 192.168.1.1-192.168.1.10
- An implied IP range, e.g. 192.168.1. for all IPs between 192.168.1.1 and 192.168.1.255, or 192.168. for all IPs between 192.168.0.1 through 192.168.255.255.
- A CIDR block [http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing], e.g. 192.168.1.1/8. If you don't know what this is, forget about it as you don't need it.
- A Subnet Mask [<http://en.wikipedia.org/wiki/Subnetwork>] notation, e.g. 192.168.1.1/255.255.255.0

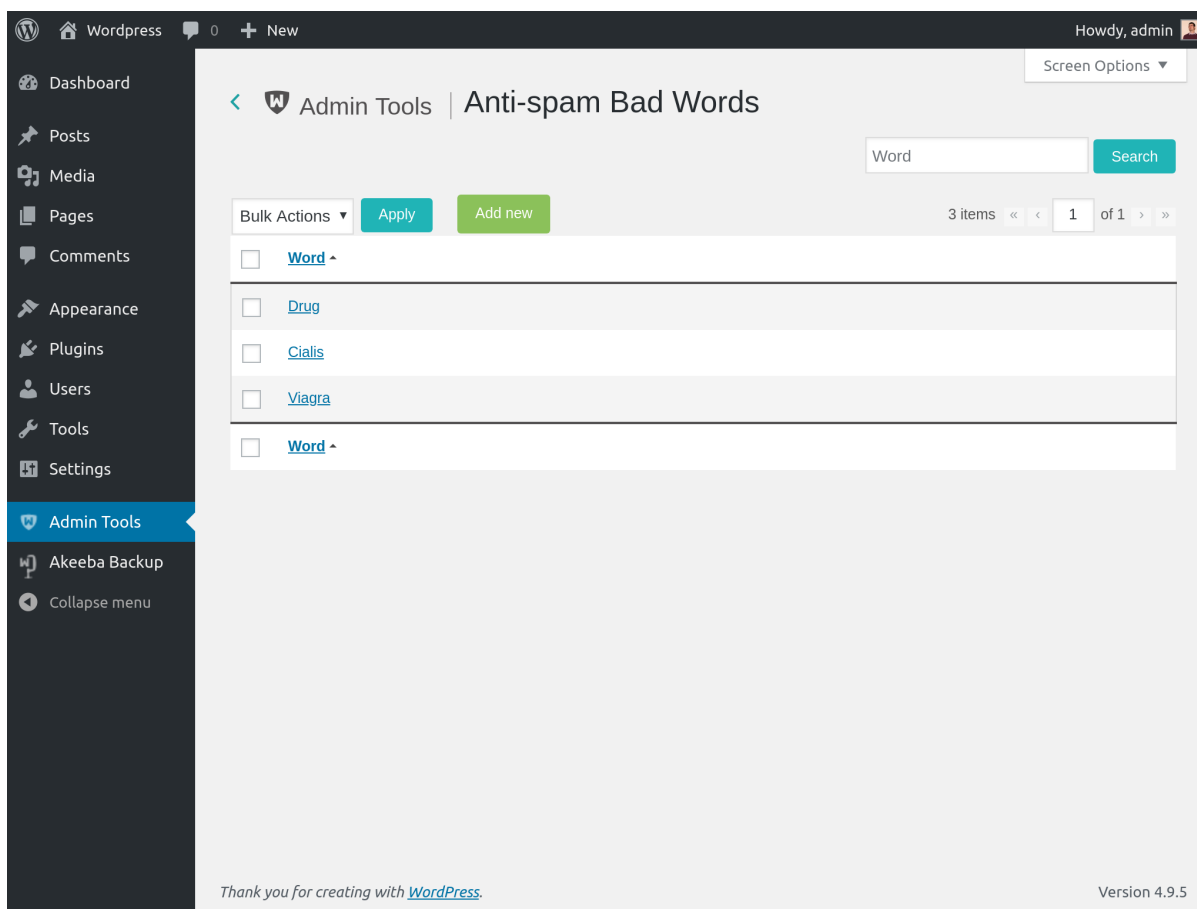
Do note that Admin Tools supports IPv4 and IPv6 (if your server supports IPv6).

Note

If you want to unblock someone who got their IP inadvertently blocked you will have to remove all records belonging to their IP address in FOUR (4) places: Site IP blacklist, Security Exceptions Log, Auto IP Blocking Administration and Auto IP Blocking History.

9.6. Anti-spam Bad Words

The Bad Words management page



This page allows you to manage the list of Bad Words. Their use will be forbidden on the site. If a query contains one of those words, it will result in a 403 error and it will optionally be logged in your Security Exceptions Log. All words are case insensitive, which means that they will be filtered no matter if they appear in lowercase, uppercase or mixed case in the request.

Note

Some servers already include a server-side filter to avoid common spam words. If you receive an error—usually a 403 error or an error noting that you have an invalid request—while trying to save a word, do not panic. It's your server's filter kicking in. Just omit including the word you just tried to include, as it is already filtered very effectively by your server!

9.7. Security Exceptions Log

The Security Exceptions Log viewer page

The screenshot displays the 'Security Exceptions Log' interface within the WordPress Admin Tools. It features a search bar at the top with a dropdown for '- Select a reason', input fields for 'IP Address' and 'Target URL', and a 'Search' button. Below the search bar is a table with the following data:

Date	IP Address	Reason	Target URL
2018-04-04 13:10:28	::1	Admin IP Whitelist	http://localhost/wordpress/wp-login.php
2018-04-04 13:09:20	::1	Login failure	http://localhost/wordpress/wp-login.php
2018-04-03 09:20:20	::1	Admin Query String	http://localhost/wordpress/wp-admin/
2018-04-03 09:19:24	::1	Admin Query String	http://localhost/wordpress/wp-admin/
2018-03-08 15:27:56	::1	Admin Query String	http://localhost/wordpress/wp-admin/

The interface also includes a 'Bulk Actions' dropdown, an 'Apply' button, and pagination controls showing '11 items of 3'. The sidebar on the left contains various WordPress management options, and the footer includes a version number '4.9.5'.

A firewall is worth nothing if it can't log the attempts to override it. Most usually you will see that the same kind of attacks are coming from the same IP addresses over and over again. Using this log viewer facility you can dive into the log, spot those IPs and note them down so that you can ban them (put them in the Blacklist).

Below each IP there is a link reading Add to Black List or Remove from Black List. Clicking the former will add the IP address of the relevant record to the IP Black List and that IP will be denied access to your site. The latter removes the IP address from the black list.

Note

If you want to unblock someone who got their IP inadvertently blocked you will have to remove all records belonging to their IP address in FOUR (4) places: Site IP blacklist, Security Exceptions Log, Auto IP Blocking Administration and Auto IP Blocking History.

9.7.1. List of blocking reasons

The block reasons, listed in the log and optionally sent to you by email are the following. The "Code" is what you need to enter in the "Do not log these reasons" or "Do not send email notifications for these reasons" options in WAF configuration to prevent these security exceptions from being logged or trigger an email respectively.

Admin Query String Code: `ipw1`

Someone tried to access your site's administrator section but he didn't provide the secret URL parameter. Admin Tools blocked him and prevented him from seeing the login page at all.

Admin IP Whitelist	Code: adminpw	Someone tried to access your site's administrator section but his IP was not in the Administrator IP Whitelist. Admin Tools blocked him and prevented him from seeing the login page at all.
Site IP Blacklist	Code: not applicable	Someone tried accessing the front- or back-end of your site but his IP is in the IP Blacklist. Admin Tools blocked him and didn't allow him to see the content of your site.
SQLi Shield	Code: sqlishield	See the Configure WAF page, SQLiShield protection against SQL injection attacks. The attack was blocked by Admin Tools.
Bad Words Filtering	Code: antispam	The request contains one of the Bad Words you have defined and was blocked by Admin Tools.
RFIShield	Code: rfishield	See the Configure WAF page, Remote File Inclusion block (RFIShield). The attack was blocked by Admin Tools.
DFIShield	Code: dfishield	See the Configure WAF page, Direct File Inclusion shield (DFIShield). The attack was blocked by Admin Tools.
UploadShield	Code: uploadshield	See the Configure WAF page, Uploads scanner (UploadShield). The attack was blocked by Admin Tools.
Spammer (via HTTP:BL)	Code: httpbl	See the Configure WAF page, Project HoneyPot. The attack was blocked by Admin Tools.
Login failure	Code: loginfailure	Someone tried to log in in the front- or back-end of your site with the wrong username and/or password.
Admin Directory	Code: adminidir	See the Configure WAF page, Change admin URL. The request was blocked by Admin Tools.
Edit Admin User	Code: nonewadmins	Someone tried to create or edit an administrator user from the backend of your site. In this context "administrator user" means any user who has the "administrator" role or has the capacity to activate plugins.
PHPShield	Code: phpshield	See the Configure WAF page, Remote PHP protocol block. The request was blocked by Admin Tools.

9.8. Auto IP Blocking Administration

Auto IP Blocking Administration

The screenshot shows the WordPress Admin Tools interface. The top navigation bar includes 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Appearance', 'Plugins', 'Users', 'Tools', 'Settings', 'Admin Tools', 'Akeeba Backup', and 'Collapse menu'. The 'Admin Tools' menu is currently selected. The main content area is titled 'Admin Tools | Auto IP Blocking Administration'. It features a search bar labeled 'IP Address' with a 'Search' button. Below the search bar is a 'Bulk Actions' dropdown menu with an 'Apply' button. The table below has 0 items and 1 page. The table has three columns: 'IP Address', 'Latest block reason', and 'Blocked until'. The table currently shows 'No records found'.

This page lists the automatic banning of repeat offenders. You will only see any records here if you have turned on the "IP blocking of repeat offenders" option in the Configure WAF page and there have been repeat offenders. For each auto-banned IP you can see the IP address being banned, the latest security exception this IP triggered and until when (GMT timezone!) this auto-ban will be in effect.

Please remember that this page only lists the automatic bans currently in effect. For a list of automatic IP bans which have been lifted please consult the "Auto IP Blocking History" page.

Note

If you want to unblock someone who got their IP inadvertently blocked you will have to remove all records belonging to their IP address in FOUR (4) places: Site IP blacklist, Security Exceptions Log, Auto IP Blocking Administration and Auto IP Blocking History.

9.9. Auto IP Blocking History

Auto IP Blocking History

The screenshot displays the 'Auto IP Blocking History' page within the WordPress Admin Tools. The page features a search bar for 'IP Address' and a 'Search' button. Below the search bar is a table with columns for 'IP Address', 'Latest block reason', and 'Blocked until'. The table is currently empty, showing 'No records found'. The interface includes a sidebar with navigation options like Dashboard, Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, Settings, Admin Tools, Akeeba Backup, and Collapse menu. The top right shows the user 'Howdy, admin' and a 'Screen Options' dropdown. The bottom of the page has a 'Thank you for creating with WordPress' message and 'Version 4.9.5'.

This page shows the history of the automatic IP bans imposed on repeat offenders. You will only see any records here if you have turned on the "IP blocking of repeat offenders" option in the Configure WAF page and there have been repeat offenders in the past whose automatic ban has now been lifted. For each old auto-banned IP record you can see the IP address which was banned, the latest security exception this IP triggered before it got banned and until when (GMT timezone!) this auto-ban was in effect.

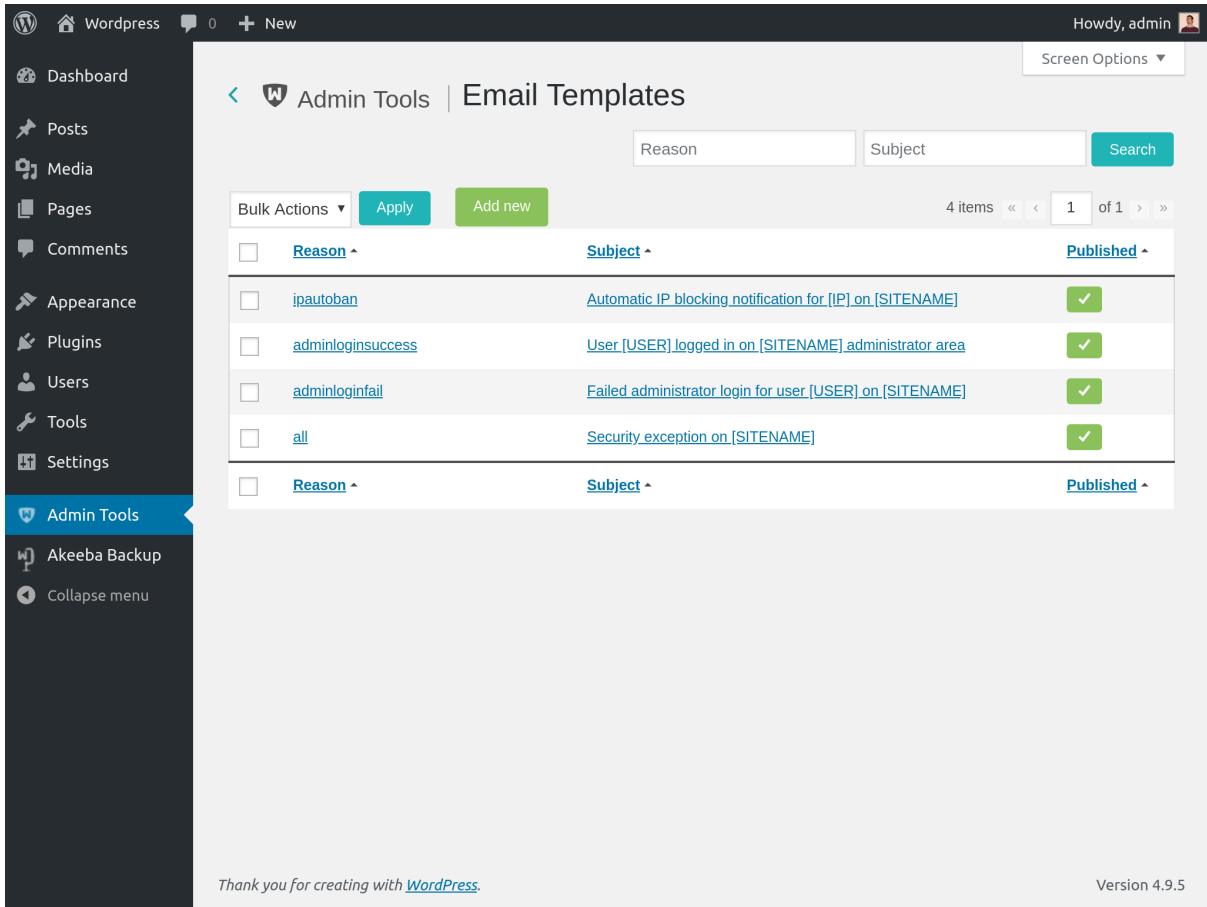
The contents of this page are used by Admin Tools together with the "IP blacklisting of persistent offenders" option in the Configure WAF page to determine which IPs of repeat offenders should be automatically added in the permanent IP blacklist.

Note

If you want to unblock someone who got their IP inadvertently blocked you will have to remove all records belonging to their IP address in FOUR (4) places: Site IP blacklist, Security Exceptions Log, Auto IP Blocking Administration and Auto IP Blocking History.

9.10. Email templates

Email templates



The screenshot shows the WordPress Admin Tools interface for managing email templates. The left sidebar contains navigation options: Dashboard, Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, Settings, Admin Tools (highlighted), Akeeba Backup, and Collapse menu. The main content area is titled "Admin Tools | Email Templates" and includes search filters for "Reason" and "Subject". Below the filters, there are buttons for "Bulk Actions", "Apply", and "Add new", along with a pagination indicator showing "4 items" and "1 of 1". A table lists the email templates with columns for "Reason", "Subject", and "Published".

<input type="checkbox"/>	Reason ^	Subject ^	Published ^
<input type="checkbox"/>	ipautoban	Automatic IP blocking notification for [IP] on [SITENAME]	<input checked="" type="checkbox"/>
<input type="checkbox"/>	adminloginsuccess	User [USER] logged in on [SITENAME] administrator area	<input checked="" type="checkbox"/>
<input type="checkbox"/>	adminloginfail	Failed administrator login for user [USER] on [SITENAME]	<input checked="" type="checkbox"/>
<input type="checkbox"/>	all	Security exception on [SITENAME]	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Reason ^	Subject ^	Published ^

Thank you for creating with [WordPress](#). Version 4.9.5

Admin Tools can be configured (in the Configure WAF page) to send out emails when an attack is blocked. You can configure the contents and layout of these email messages using this page.

Editing an email template

WordPress 0 + New Howdy, admin

Admin Tools | Edit an email template

Select a reason: All

Subject: Security exception on [SITENAME]
The template of the email subject. You can use the same placeholders as the email body (see below).

Published: Published

Frequency limit: 5 emails, in 1 hours
How many emails should be sent in the defined timespan. If you're under attack, this limit will prevent your site flooding you with email alerts.

Body

Add Media

Visual Text

B I U “ ” ABC ☰ ☷ ☹ ☶ ☵ ☴ ☳ ☲ ☱ ↶ ↷ 🔗 ✕

Hello,

We would like to notify you that a security exception was detected on your site, [SITENAME], with the following details:

IP Address: [IP] (IP Lookup: [LOOKUP])
Reason: [REASON]

If this kind of security exception repeats itself, please log in to your site's back - end and add this IP address to your Admin Tools's Web Application Firewall feature in order to completely block the misbehaving user.

The template of the email body. Please remember that you are supposed to use inline styling, not CSS classes. This is a limitation imposed by email clients and popular webmail services. You can use the following placeholders:

[IP] Banned IP
[LOOKUP] Direct link to the ip lookup service
[REASON] Reason of the block
[DATE] Date of the block
[URL] Attacked url
[USER] Username
[COUNTRY] Country of the attack
[CONTINENT] Continent of the attack
[UA] User agent
[SITENAME] Name of your site

Save Changes Cancel

Thank you for creating with [WordPress](#). Version 4.9.5

Each email template consists of the following elements:

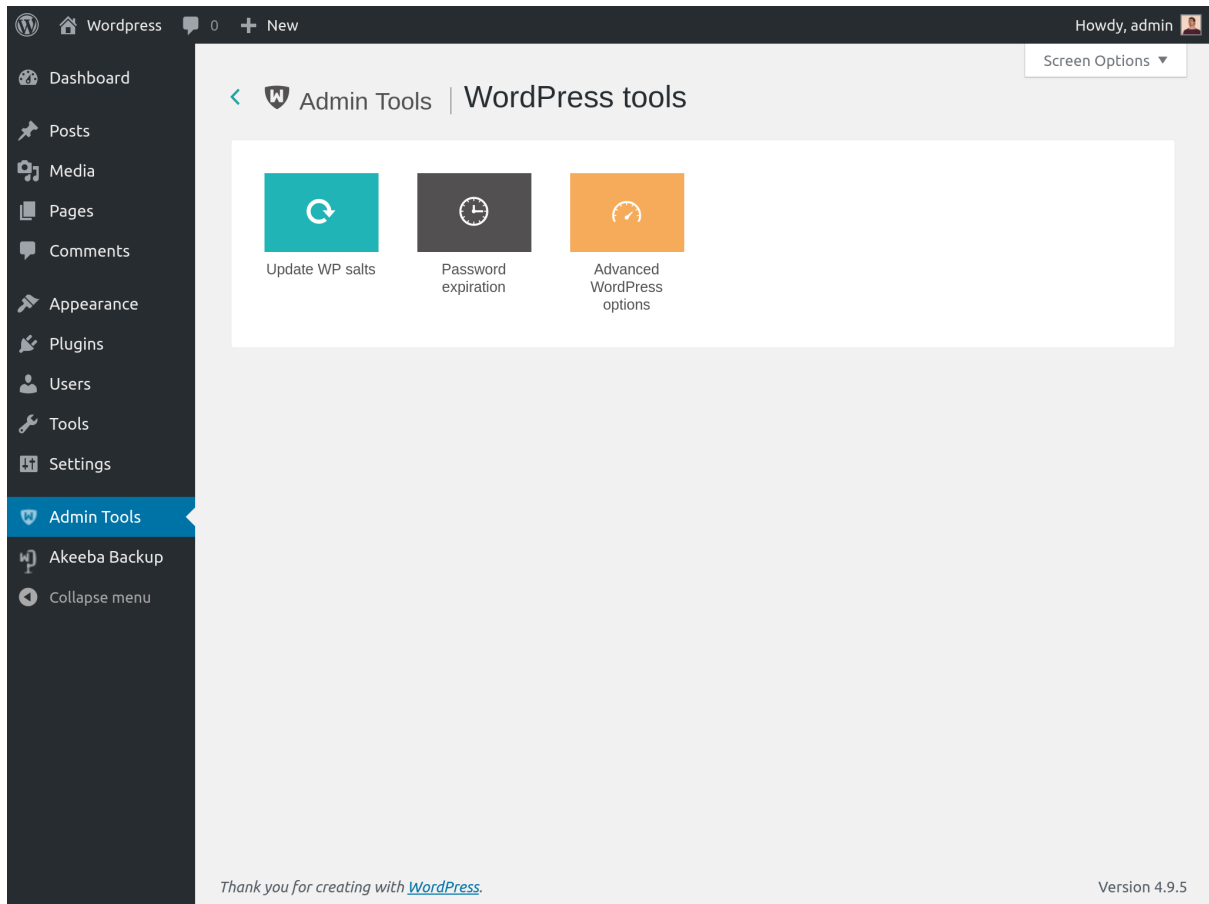
Reason	The kind of attack this email template applies to. If no specific email template is found, Admin Tools will use the one with its reason set to "All".
Subject	The subject line of the email message you will be receiving. You can use certain variables (see below).
Published	Only the email templates with Published set to Yes will be taken into account.
Frequency limit	When the "Enable security exception email throttling" option is enabled in the Configure WAF page these options will define the maximum number of emails you are going to receive. You can set the number of emails and the amount of time. For example setting 5 emails in 1 hour means that if 5 emails for this Reason have been sent in the last 1 hour Admin Tools will not send out any more emails about it.
Body	The body text of the email message. You can use full HTML and certain variables (see below).

The variables you can use are enclosed in square brackets and are always in uppercase. The available variables are:

- [IP] Blocked IP address
- [LOOKUP] Direct link to the ip lookup service
- [REASON] The detected kind of the attack
- [DATE] Date and time of the attack
- [URL] Attacked URL. **THIS IS POTENTIALLY UNSAFE.** You are advised to **NOT** include this in your emails to avoid attackers triggering Cross Site Scripting (XSS) attacks.
- [USER] Username of the attacker (if the user is logged in)
- [UA] User agent of the attacker. **THIS IS POTENTIALLY UNSAFE.** You are advised to **NOT** include this in your emails to avoid attackers triggering Cross Site Scripting (XSS) attacks.
- [SITENAME] The name of your site.

10. WordPress tools

WordPress Tools



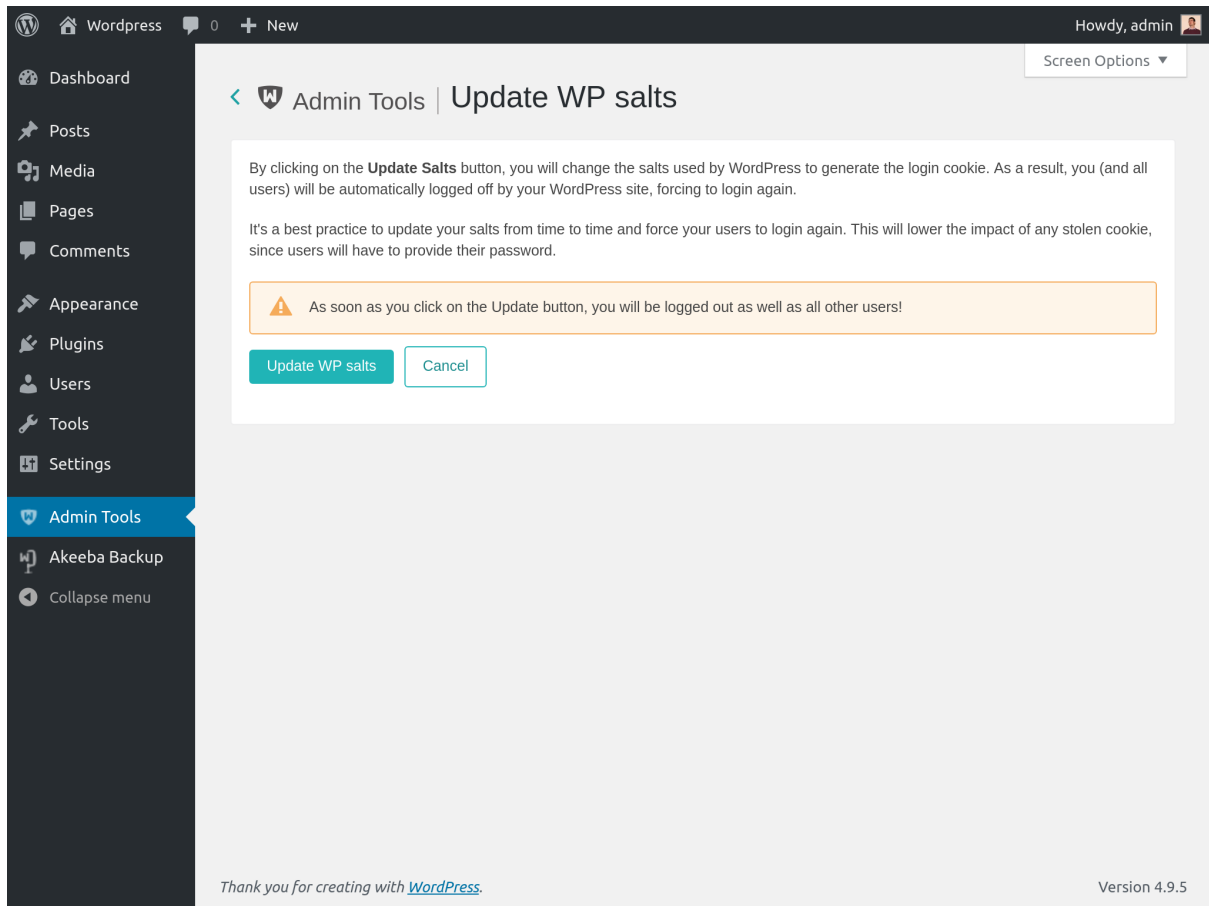
WordPress offers several options to tweak your site, but most of the time they are deep buried inside its documentation and requires you to manually write some PHP code and modify some configuration files.

These steps are extremely error prone: if everything is done correctly, your changes will make effect; on the other side, if anything goes wrong, your site will break.

Admin Tools offers a friendly graphical interface to enable or disable those options.

10.1. Update WordPress salts

Update WordPress salts



While logging in, WordPress allows users to set the option **Remember me**. In this way users won't have to type their passwords over and over.

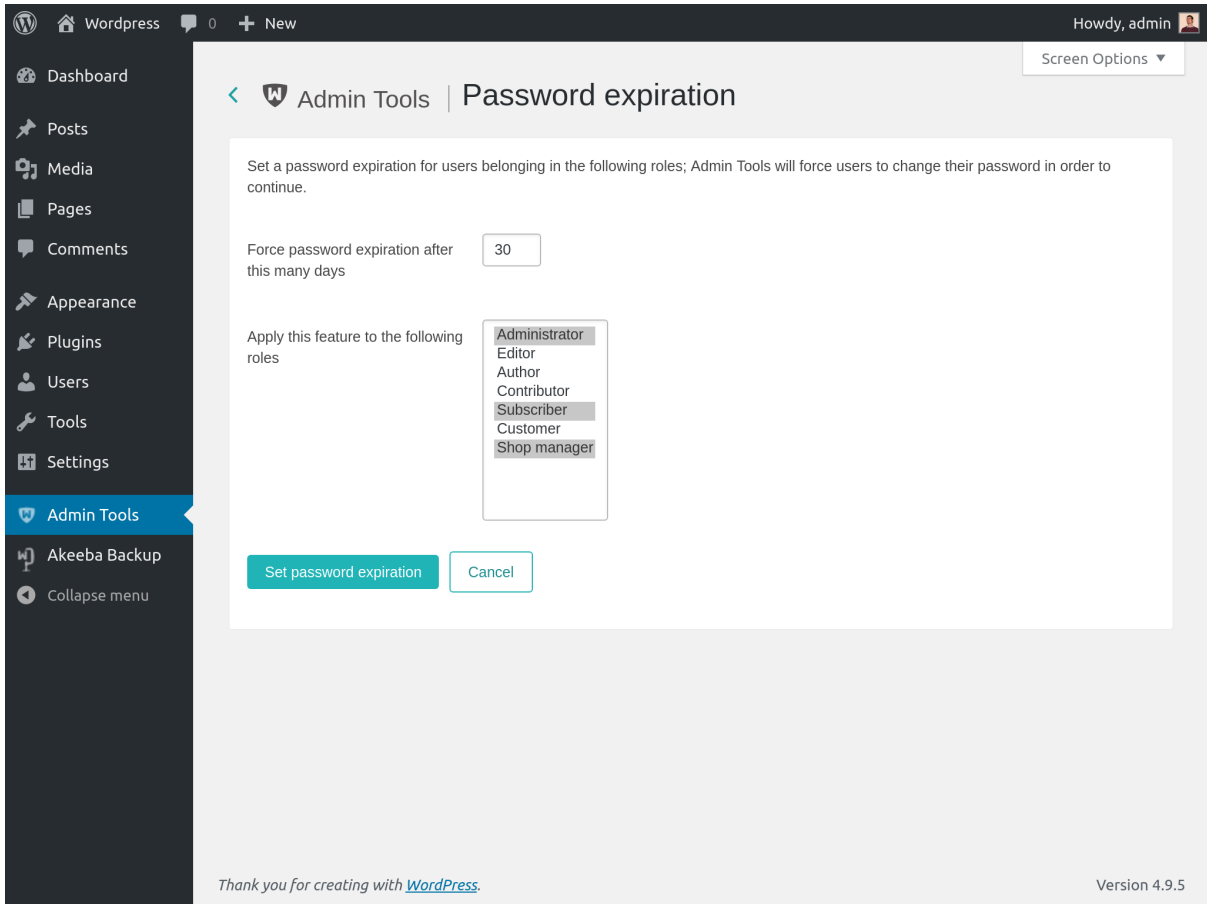
However this feature has two downsides:

- if user's cookies are stolen, an attacker can easily access your site
- if the user is using a shared computer and he forgot to logout, anyone could access his account

For those reasons, it's good practice from time to time to reset your site salts: this will invalidate ALL your user cookies, forcing them to login again.

10.2. Password expiration

Password expiration



Choosing a good password is fundamental to protect your account, however in very sensitive environments it could be worth to setup a password expiration policy.

This means that for select roles (usually the most powerful ones, like the Administrator one), Admin Tools will force the users to reset their password based on the expiration you set.

Force password expiration after this many days After how many days a password should be considered expired? If it's expired, Admin Tools will force the user to reset his password using WordPress core feature.

Leave this field to 0 to disable this feature

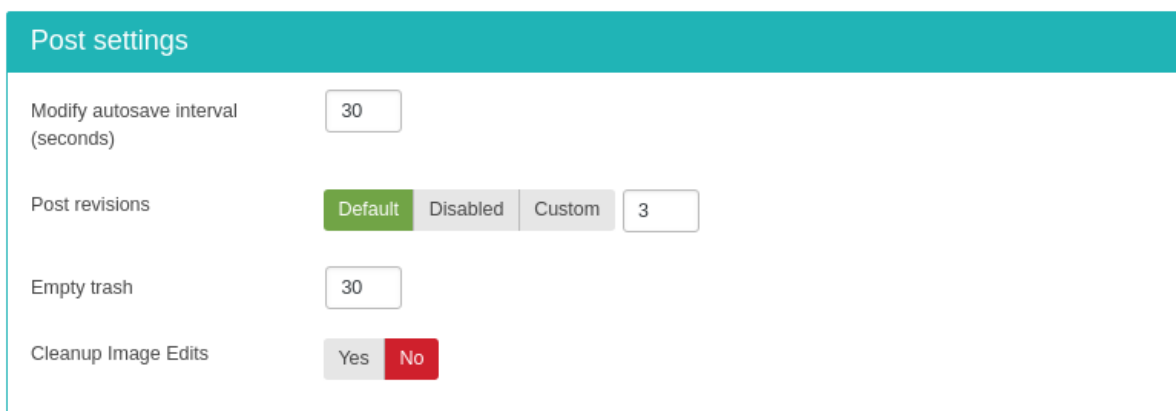
Apply this feature to the following roles Select which roles should have their password reset. Hold Ctrl key and click to select multiple roles.

10.3. Advanced WordPress options

Finally, WordPress has several advanced options, for example specific debug modes or post settings. In this section you can easily switch them on or off using few clicks of your mouse.

10.3.1. Post settings

Post settings



The screenshot shows the 'Post settings' section of the WordPress admin interface. It contains four settings:

- Modify autosave interval (seconds):** A text input field containing the number '30'.
- Post revisions:** A group of three radio buttons labeled 'Default', 'Disabled', and 'Custom'. The 'Default' button is selected and highlighted in green. To the right of these buttons is a text input field containing the number '3'.
- Empty trash:** A text input field containing the number '30'.
- Cleanup Image Edits:** Two radio buttons labeled 'Yes' and 'No'. The 'No' button is selected and highlighted in red.

Modify autosave interval (seconds) When editing a post, WordPress uses Ajax to auto-save revisions to the post as you edit. You may want to increase this setting for longer delays in between auto-saves, or decrease the setting to make sure you never lose changes. The default is 60 seconds.

Post revisions WordPress, by default, will save unlimited copies of each edit made to a post or page. Here you can disable this feature, set a custom limit to the revision number or revert to the default behavior.

Empty trash Number of days before WordPress permanently deletes posts, pages, attachments, and comments, from the trash bin. Set it to 0 to disable the trash.

Cleanup Image Edits By default, WordPress creates a new set of images every time you edit an image and when you restore the original, it leaves all the edits on the server. When this option is set, only one set of image edits are ever created and when you restore the original, the edits are removed from the server.

10.3.2. System settings

System settings

System settings

Disable file editing	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Enable debug	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Enable debug log	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Display all errors in Debug mode	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Custom error reporting	<input type="text" value="System default"/>
Javascript Concatenation	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Memory limit	<input type="text" value="64"/>
Enable cache	<div style="display: flex; align-items: center;"> ⚠ You can enable this option only if the file wp-content/advanced-cache.php exists </div>

Disable file editing	Disable the plugin or theme editor to prevent users from being able to edit sensitive files and potentially crash the site.
Enable debug	Enable WordPress debug mode. It causes very verbose information to be printed on the browser. This information may tip off hackers about how your site works. As a result it is not recommended for production sites. Only use this when you are trying to troubleshoot an error on your site.
Enable debug log	When enabled, WordPress will produce a log file with debug information in wp-content/debug.log. WARNING! This file can be accessed over the web by default and can be used to tip off hackers about the internal workings of your site. Only use on local development sites when you are trying to troubleshoot an error on your site.
Display all errors in Debug mode	Display all PHP errors and warnings when WordPress Debug mode is enabled.
Custom error reporting	<p>Set a custom level for PHP error reporting, the following levels are available:</p> <ul style="list-style-type: none"> • System default Use server configuration to decide which errors to render • None Never display the errors • Errors Displays only PHP Errors (error reporting E_ERROR) • Minimal Displays PHP Errors, Warnings and Parse errors (error reporting set to E_ERROR E_WARNING E_PARSE) • Full Displays PHP Errors, Warnings, Parse and Notices errors (error reporting set to E_ERROR E_WARNING E_PARSE E_NOTICE)

- **Developer** Displays PHP Errors, Warnings, Parse, Notices and Deprecation errors (error reporting set to `E_ERROR` | `E_WARNING` | `E_PARSE` | `E_NOTICE` | `E_DEPRECATED`)

Javascript concatenation By default, WordPress concatenates scripts in admin area. Set it to No to disable javascript concatenation

Memory limit Ask WordPress to increase current memory limit to the following value (in MegaBytes). **WARNING!** Values too low, e.g. below 64, may cause your site to stop loading (you will see a PHP error, 500 Internal Server error or white page instead of your site). Values too high may be incompatible with your server. Only change this if you have a good reason to. If unsure, please ask your host about the valid range for your site.

Enable cache Enable WordPress cache. Please note that the file `wp-content/advanced-cache.php` must exist

11. Database tools

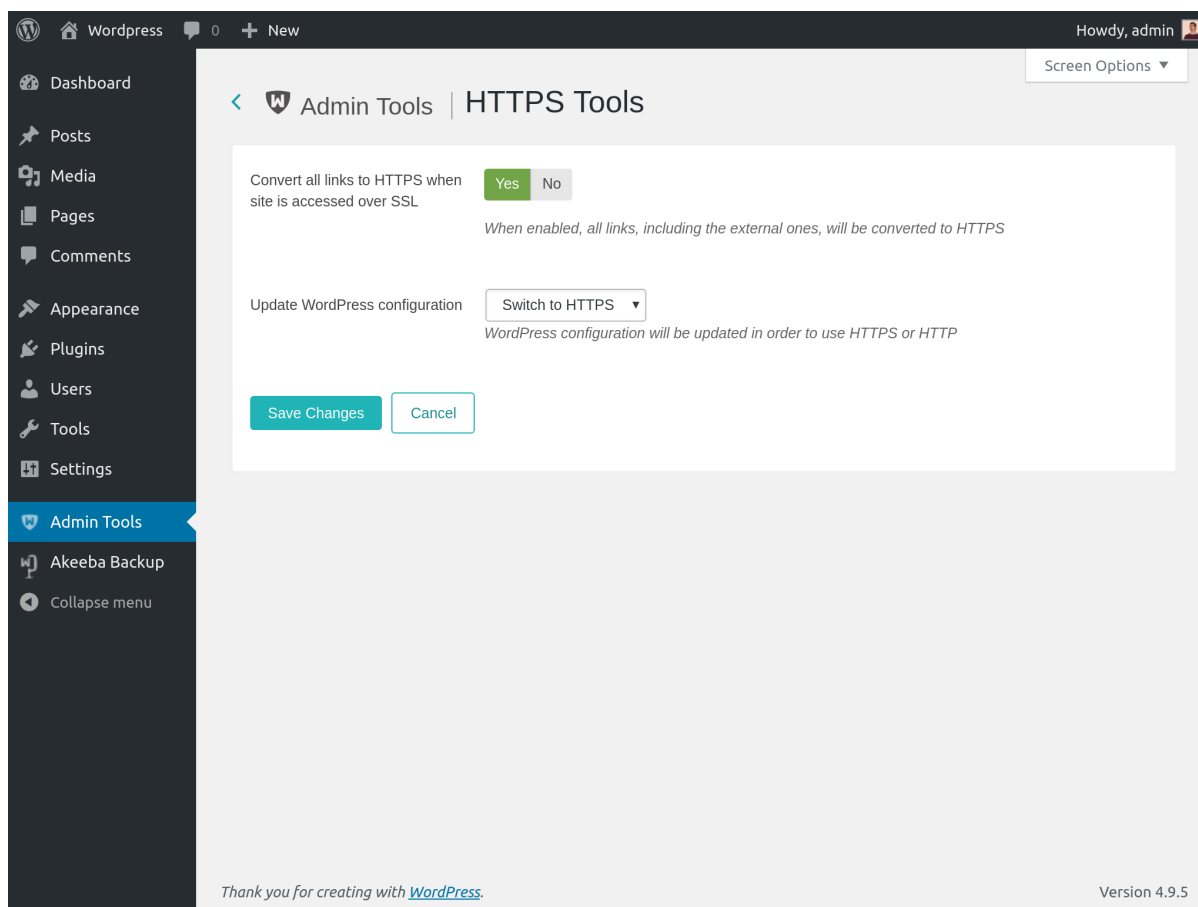
The database is the most important part of our websites. It holds all the data and most configuration options, i.e. everything which makes our site what it is. However, since data is being written to and deleted from the database, the database table are becoming slow or even corrupted. It's the same thing as what happens with hard drives.

On a hard drive you know that you can always defragment it and run `chkdisk` or `fsck` (depending on your Operating System). For databases you have to go through a tedious process using a database administration tool, such as `phpMyAdmin`, to repair and optimize each and every table. Admin Tool's Database Tools are here to automate this tedious process for you!

Repair & Optimise Tables will run the repair and optimisation process on all of your site's tables. If the process hangs for a long time after the first time you use it, run it again. The usual problem is that the a database table is so bloated that PHP times out waiting for your database server to optimise this table.

12. HTTPS Tools

HTTPS Tools



When you access your site over SSL (HTTPS) you might end up with a "partially encrypted page" warning on several browsers. This happens because some resources, such as Javascript, CSS or external pages (maps, calendars) loaded in IFRAMEs are accessed over HTTP. It is usually extremely difficult to spot all of them and change them. Some are outright impossible to change unless you edit the code of the plugin which produces them. Not any more. Just enable the Convert all links to HTTPS when site is accessed over SSL option and Admin Tools will automatically convert all HTTP URLs to HTTPS URLs when your site is accessed over SSL (HTTPS). This will make the partially encrypted page warnings finally go away.

Moreover, you can update WordPress configuration to instruct it to always use HTTPS while accessing your site.

Warning

All links to external files and pages, including regular links to other web sites, will be converted to use the https:// scheme. And we really mean EVERY SINGLE ONE OF THEM. That's exactly what this feature is designed to do.

13. URL Redirection

Note

This feature is only available in the Professional release

Sometimes you need to create short, memorable URLs to some of your site's pages. Our friend Brian Teeman calls them PEF (Pub Ear Friendly). Arguably, telling someone to visit `http://www.example.com/downloads` is much easier to remember than a 100+ character long URL.

Some other times you would like to use a short URL to an external site but do not wish to use one of the free services, like bit.ly, ow.ly, t.co or tinyurl.com for privacy reasons. Admin Tools to the rescue! The custom URL redirection feature allows you to do all of the above with a ridiculously simple interface.

The URL Redirection management page

The screenshot displays the WordPress Admin Tools interface for URL Redirection. The sidebar on the left contains various navigation options, with 'Admin Tools' highlighted. The main content area shows the 'URL Redirection' management page. At the top, there is a toggle to 'Enable the URL Redirection feature?' with 'Yes' and 'No' buttons and a 'Save preference' button. Below this are input fields for 'Existing URL', 'New URL', and a '- Select state' dropdown with a 'Search' button. A table lists existing redirections with columns for 'Existing URL', 'New URL', 'Keep URL Parameters', and 'Published'. The table shows three entries: one for 'googlethis', one for 'wp-content/google', and one for 'example'. Each entry has a checkbox on the left and a green checkmark in the 'Published' column. At the bottom, there is a footer with 'Thank you for creating with WordPress.' and 'Version 4.9.5'.

The main administration page shows you a list of the custom URL redirections defined on your sites. Each entry consists of the following information:

- The left hand checkbox. The toolbar operations will apply only to the checked items.
- Existing URL. The URL where your visitors will be taken to. It's called "Existing" because it exists even when the URL Redirection feature is not enabled. It is existing content and you're about to create a new URL which will take your visitors to it. Clicking on it will open it in a new window so that you can preview the results.
- New URL. The relative path on your site which triggers the redirection. It's called "New" because it doesn't exist when the URL Redirection feature is disabled. With the redirections you essentially create a new URL for existing content. For example, if your site is accessible at `http://www.example.com/wordpress` and this field reads `search/google`, then all requests to `http://www.example.com/wordpress/search/google` will be redirected to the Existing URL with a 301 (Permanently Moved) HTTP status code, to keep search engines happy. Clicking on the displayed value will open the Edit/Add page so that you can edit the entry.
- Keep URL Parameters. During the redirection, what should happen to URL parameters? Read below for further details.

- **Published.** When unpublished, the redirection will not take place. Useful to temporarily take down a redirection without deleting it.

When adding a new entry or editing an existing entry, the following page appears:

The URL Redirection editor page

The screenshot shows the WordPress Admin Tools interface for editing a URL redirection. The page title is 'Admin Tools | Edit a URL Redirection'. The form contains the following fields and options:

- Existing URL:** A text input field containing 'https://www.google.com'. Below it is a note: 'This is where the browser will be redirected to. This URL must be valid even if you turn off the redirection feature. It can be a URL to the same or another site. Example: http://www.google.com'.
- New URL:** A text input field containing 'googlethis'. Below it is a note: 'This is the relative URL which will trigger the redirection. It must not have the http:// or https:// protocol prefix, your domain name or a leading slash. Example: search/on/google'.
- Keep URL Parameters:** A dropdown menu set to 'Override all'. Below it is a note: 'When enabled any query string parameters in the URL will be kept in the redirection.'
- Published:** Two radio buttons, 'Yes' (selected) and 'No'. Below it is a note: 'When set to Unpublished the redirection is disabled'.

At the bottom of the form are two buttons: 'Save Changes' and 'Cancel'. The footer of the page includes the text 'Thank you for creating with WordPress.' and 'Version 4.9.5'.

There are three fields to edit:

Existing URL An existing URL on your site, or a link to an external page.

When using a URL in your own site you do not have to include the URL to your site's root. Use the relative path instead.

The biggest strength of this feature is the ability to enter external links. For instance you can enter `http://www.google.com` to redirect your visitors to Google's search page. Using this powerful feature allows you to run your private URL shortening service on your own domain!

New URL The **relative** path which triggers the redirection.

For example, if your site is accessible as `http://www.example.com/wordpress`, entering `google` in this field will cause the URL `http://www.example.com/wordpress/google` to redirect to the the URL you entered in the Existing URL field above. You can use subdirectories in your path, e.g. `search/external/google`.

Keep URL Parameters When set to None any query string parameters in the URL (i.e. anything after the question mark) will be ignored.

When set to Override All any query string parameters in the URL will override any parameters in the Existing URL, or added to it if they didn't exist in the first place.

When set to Add New any query string parameters in the URL which do not exist in the Existing URL will be added to it. Existing query parameters will not be overridden.

Published When unpublished, the redirection will not take place. Useful to temporarily take down a redirection without deleting it.

Tip

If you want to make a simple redirection set Existing URL to the URL you are redirecting to, New URL to the URL you are redirecting from and Keep URL Parameters to None.

14. Import and Exporting Settings

Sometimes you need to be able to import and export Admin Tools it. Some indicative use cases are:

- Backing up your Admin Tools settings before trying massive changes which could break your configuration
- Transferring your settings to another site on the same or an identical server
- Copying the IP white- and black-lists or email templates

With Admin Tools you can do that through the Export Settings and Import Settings pages of the component.

Warning

Exporting and importing very large datasets (more than a thousand rows) IS NOT RECOMMENDED and CAN LEAD TO TIMEOUT ERRORS. This is a limitation of PHP, namely the `memory_limit` (maximum memory usage limit) and `max_execution_time` (maximum time to execute the page) imposed by your server's `php.ini`. Besides, it is a very bad idea having so many IP white-/black-list and/or email template rows as your site's performance would become extremely bad. If you find yourself putting more than 100 records into these features you are doing something really wrong.

Exporting Settings

In this page you can choose which settings you want to export. The available options are:

WAF configuration	This includes all settings in the Configure WAF
WAF exceptions	Includes the list of URLs were Admin Tools should be deactivated
IP Blacklist	The permanently blacklisted IP addresses from the IP Blacklist page
IP Whitelist	The whitelisted administrator IP addresses from the IP Whitelist page
Bad words	All the words that are flagged as spam and should be blocked
Email templates	All email templates from the Email Templates page

After selecting what you want to export click on the Export settings button. Your browser will download a JSON file with all of the selected configuration settings.

Importing Settings

Choose the exported JSON file and click on the Import settings button. The imported settings will overwrite your existing settings.

Appendix A. GNU General Public License version 3

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program—to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a. The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b. The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.
- c. You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

- d. If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation’s users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c. Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d. Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e. Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a. Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b. Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c. Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d. Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e. Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f. Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of

making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

```
one line to give the program's name and a brief idea of what it does.  
Copyright (C) year name of author
```

```
This program is free software: you can redistribute it and/or modify  
it under the terms of the GNU General Public License as published by  
the Free Software Foundation, either version 3 of the License, or  
(at your option) any later version.
```

```
This program is distributed in the hope that it will be useful,  
but WITHOUT ANY WARRANTY; without even the implied warranty of  
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the  
GNU General Public License for more details.
```

```
You should have received a copy of the GNU General Public License  
along with this program. If not, see http://www.gnu.org/licenses/.
```

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
program Copyright (C) year name of author  
This program comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.  
This is free software, and you are welcome to redistribute it  
under certain conditions; type 'show c' for details.
```

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an “about box”.

You should also get your employer (if you work as a programmer) or school, if any, to sign a “copyright disclaimer” for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

Appendix B. GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc. [<http://www.fsf.org/>]

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “Modified Version” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with

generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

The “publisher” means any person or entity that distributes copies of the Document to the public.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a

computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties — for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See Copyleft [<http://www.gnu.org/copyleft/>].

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy’s public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

“Massive Multiauthor Collaboration Site” (or “MMC Site”) means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A “Massive Multiauthor Collaboration” (or “MMC”) contained in the site means any set of copyrightable works thus published on the MMC site.

“CC-BY-SA” means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

“Incorporate” means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is “eligible for relicensing” if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright © YEAR YOUR NAME

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with... Texts.” line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.