# Admin Tools User's Guide

**Nicholas K. Dionysopoulos**

# Admin Tools User's Guide

Nicholas K. Dionysopoulos


**Abstract**

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

# Table of Contents

# Chapter 1. Getting Started

## 1. What is Admin Tools?

Admin Tools is a security component, i.e. a software solution which will help you tighten the security of your Joomla! 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 Joomla! best practices in mind. It uses a native Joomla! plugin to apply its security and performance enhancing feature. It does not touch Joomla's core files ("core hacks").

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

A summary of the features of Admin Tools and how they relate to each edition can be found on our site [http://www.akeebabackup.com/products/admin-tools.html].

## 1.1. Disclaimer

Security applications —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 For instance, if you have an outdated Joomla! installation or a vulnerable component installed on your site there is nothing —and, let us stress that, NOTHING — which can stop a hacker from successfully attacking your site.

We are aware that some developers may market their products as a "complete protection" for your site, which simply is technically impossible. If such a magic solution existed would they be selling it for a few dozen dollars a years to everyone or for millions of dollars per year to high profile targets (large corporations and government agencies)? Exactly.

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.

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 Joomla! we have stopped supporting and expect that site to be impregnable by hackers. Old versions of Joomla! may have 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 Joomla! core or third party extension code itself is updated. That is why we will only officially provide support to the latest and the previous Joomla! version family. 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 extension 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:

- Joomla!™ and PHP version compatibilities are detailed in our Compatibility page [https://www.akeebabackup.com/compatibility.html].
- MySQL 5.0.42 or later. MySQL 5.6 or later recommended. MySQL 4.x is not supported.
- 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 Joomla! 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 is no different than installing any other Joomla!™ extension on your site. You can read the complete instructions for installing Joomla!™ extensions on the official help page [https://docs.joomla.org/Installing_an_extension]. Throughout this chapter we assume that you are familiar with these instructions and we will try not to duplicate them.

## 3.1. Installing or manually updating the extension

Just like with most Joomla! extensions there are two ways to install or manually update Admin Tools on your site:

- Install from URL. This works only with the Professional release of our component. It is the easiest and fastest one, if your server supports it. Most servers do support this method.
- Upload and install. That's the typical extension installation method for Joomla! extensions. It rarely fails.

Please note that installing and updating Admin Tools (and almost all Joomla! extensions) is actually the same thing. If you want to update Admin Tools please remember that you **MUST NOT** uninstall it before installing the new version! When you uninstall Admin Tools you will lose all your settings. This is definitely something you do not want to happen! Instead, simply install the new version on top of the old one. Joomla! will figure out that you are doing an update and will treat it as such, automatically.

### Tip

If you find that after installing or updating Admin Tools it is missing some features or doesn't work, please try installing the same version a second time, without uninstalling the component. The reason is that very few times the Joomla! extensions installer infrastructure gets confused and fails to copy some files or entire folders. By repeating the installation you force it to copy the missing files and folders, solving the problem.

### 3.1.1. Install from URL

The easiest way to install Admin Tools Professional is using the Install from URL feature in Joomla!.

### Important

This Joomla! feature requires that your server supports fopen() URL wrappers (`allow_url_fopen` is set to 1 in your server's `php.ini` file) or has the PHP cURL extension enabled. Moreover, if your server has a firewall, it has to allow TCP connections over ports 80 and 443 to `www.akeebabackup.com`, `www.akeeba.com` and `cdn.akeebabackup.com`. If you don't see any updates or if they fail to download please ask your host to check that these conditions are met. If they are met but you still do not see the updates please file a bug report in the official Joomla! forum [http://forum.joomla.org/]. In the meantime you can use the manual update methods discussed further below this page.

First, go to our site's download page for Admin Tools [https://www.akeebabackup.com/download/admintools.html]. Make sure you are logged in. If not, log in now. These instructions won't work if you are not logged in! Click on the All Files button of the version you want to install. Please note that the latest released version is always listed *first* on the page. On that page you will find both Admin Tools Core and Professional. Next to the Professional edition's Download Now button you will see the Direct Install Link link. Right click on it and select Copy link address or whatever your browser calls this.

Now go to your site's administator page and click on Extensions, Manage. Click on the Install from URL tab. Clear the contents of the Install URL field and paste the URL you copied from our site's download page. Then click on the Install button. Joomla! will download and install the software.

If Joomla! cannot download the package, please use one of the methods described in this section of the documentation. If, however you get an error about copying files, folder not found or a cryptic "-1" error please follow our installation troubleshooting instructions [https://www.akeebabackup.com/documentation/troubleshooter/abinstallation.html].

## 3.1.2. Upload and install.

You can download the latest installation packages our site's download page for Admin Tools [https://www.akeebabackup.com/download/admintools.html]. Please note that the latest version is always on top. If you have an older version of Joomla! or PHP please consult our Compatibility page [https://www.akeebabackup.com/compatibility.html] to find the version of Admin Tools compatible with your Joomla! and PHP versions. In either case click on the version you want to download and install.

If you are not a subscriber, click on the Admin Tools Core to download the ZIP installation package of the free of charge version.

If you are a subscriber to the Professional release, please make sure that you have logged in first. You should then see an item on this page reading Admin Tools Professional. If you do not see it, please log out and log back in. Click on the Professional item to download the ZIP installation package.

All Admin Tools installation packages contain the component and all of its associated extensions. Installing it will install all of these items automatically. It can also be used to upgrade Admin Tools; just install it *without* uninstalling the previous release.

In any case, do not extract the ZIP files yet!

### Warning

**Attention Mac OS X users**! Safari, the default web server provided to you by Apple, is automatically extracting the ZIP file into a directory and removes the ZIP file. In order to install the extension through Joomla!'s extensions installer you must select that directory, right-click on it and select Compress to get a ZIP file of its contents. This behaviour was changed in Mac OS X Mountain Lion, but people upgrading from older versions of Mac OS X (Mac OS X Lion and earlier) will witness the old, automatic ZIP extraction, behaviour.

Log in to your site's administrator section. Click on Extensions, Manage link on the top menu. Please click on the Upload Package File tab. Drag and drop the installation ZIP file you had previously downloaded to start the upload and the installation. After a short while, Joomla!™ will tell you that the component has been installed.

### Warning

Admin Tools is a big extension (over 2Mb for the Professional release). Some servers do not allow you to upload files that big. If this is the case you can try the Manual installation or ask your host to follow our installation troubleshooting instructions [https://www.akeebabackup.com/documentation/troubleshooter/abinstallation.html] under "You get an error about the package not being uploaded to the server".

If you have WAMPServer (or any other prepackaged local server), please note that its default configuration does not allow files over 2Mb to be uploaded. To work around that you will need to modify

your php.ini and restart the server. On WAMPserver left-click on the WAMP icon (the green W), click on PHP, php.ini. Find the line beginning with `upload_max_filesize`. Change it so that it reads:

```
upload_max_filesize = 6M
```

Save this file. Now, left-click on the WAMP icon, click on Apache, Service, Restart Service and you can now install the component. Editing the `php.ini` file should also work on all other servers, local and live alike.

If the installation did not work, please take a look at our installation troubleshooting instructions [https://www.akeebabackup.com/documentation/troubleshooter/abinstallation.html] or try the manual installation described below.

## 3.1.3. Manual installation

This method can no longer be supported for technical reasons which have to do with the way Joomla! works when installing extensions of the type "package".

### Warning

**DO NOT UNZIP THE PACKAGE AND TRY TO INSTALL THE EXTENSIONS MANUALLY**! This will very likely make your site fail with an error. When you are installing the package extension Joomla! makes a few checks to make sure that your server meets the minimum requirements. Moreover, the installation order in the package matters. It is designed to make sure that failure to install one of the included extensions will minimize the chance of a cascading effect which breaks your site.

## 3.1.4. The installation / update broke my site!

Some users have reported that after they have installed or updated Admin Tools, they were no longer able to access parts of their site, especially the back-end. This is an indication of a failed or partial installation. Should this happen, use your FTP client to remove the following directories (some of them may not be present on your site; this is normal):

```
administrator/component/com_admintools
component/com_admintools
media/com_admintools
plugins/system/admintools
```

This will do the trick! You will now be able to access your site's administrator page again and retry installing Admin Tools without uninstalling it first. Remember, uninstalling Admin Tools will remove your settings; you do not want that to happen!

### Note

If you get a username and password dialog *from your browser* (not Joomla!) OR a server error when you access your site's backend (administrator) URL, try deleting the `.htaccess` and `.htpasswd` files inside your site's administrator folder.

In some cases Joomla! forgets to install files for the FOF 3 library used by most of our components (Akeeba Backup, Admin Tools, Akeeba Ticket System and others). This could mean that even removing the directories above you could still be unable to access your site. If this happens, try the following solution:

1. Delete the folder libraries/fof30 from your site. **ATTENTION**! Do NOT remove the libraries/fof folder, it's something entirely different and you will break your site if you remove that folder instead!

2. Go to our Download page [https://www.akeebabackup.com/download.html] and download the latest version of FOF. This downloads a file named something like `lib_fof30-1.2.3.zip` on your computer.

3. Extract (unzip) the file you downloaded. You see a `fof` directory being extracted.

4. Rename to `fof` directory to `fof30`
5. Upload the `fof30` directory into your site's `libraries` directory.
6. You now have a `libraries/fof30` directory and you can log in to your site's backend.
7. Reinstall our extension *twice* in a row

# 4. Upgrading from Core to Professional

Upgrading from Admin Tools Core to Admin Tools Professional is by no means different than installing the component. You do not have to uninstall the previous version; in fact, you MUST NOT do that. Simply follow the installation instructions to install Admin Tools Professional over the existing Admin Tools Core installation. That's all! All your settings are preserved.

### Important

When upgrading from Core to Professional you usually have to install the Professional package **twice**, without uninstalling anything in between. Sometimes Joomla! does not copy some of the files and folders the first time you install it. However, if you install the package again (without uninstalling your existing copy of Admin Tools) Joomla! copies all of the necessary files and performs the upgrade correctly.

# 5. Automatic updates

Admin Tools can be updated just like any other Joomla! extension, using the Joomla! extensions update feature. Please note that Joomla! is fully responsible for discovering available updates and installing them on your site. Akeeba Ltd does not have any control of the update process.

### Note

This Joomla! feature requires that your server supports fopen() URL wrappers (`allow_url_fopen` is set to 1 in your server's `php.ini` file) or has the PHP cURL extension enabled. Moreover, if your server has a firewall, it has to allow TCP connections over ports 80 and 443 to `www.akeebabackup.com`, `www.akeeba.com` and `cdn.akeebabackup.com`. If you don't see any updates or if they fail to download please ask your host to check that these conditions are met. If they are met but you still do not see the updates please file a bug report in the official Joomla! forum [http://forum.joomla.org/]. In the meantime you can use the manual update methods discussed further below this page.

### Warning

Admin Tools Professional needs you to set up the Download ID before you can install the updates. You can find your main download ID or create additional Download IDs on our site's Add-on Download IDs [http://akee.ba/downloadid] page. Then go to your site's administrator page and click on Components, Admin Tools, Options (in the toolbar). Click on the Live Update tab and paste your Download ID there. Finally, click on Save & Close.

You can access the extensions update feature in two different ways:

- From the icon your Joomla! administrator control panel page. You will find the icon in the left-hand sidebar, under the Maintenance header. When there are updates found for any of your extensions you will see the Updates are available message. Clicking on it will get you to the Update page of Joomla! Extensions Manager.
- From the top menu of your Joomla! administrator click on Extensions, Manager. From that page click on the Update tab found in the left-hand sidebar. Clicking on it will get you to the Update page of Joomla! Extensions Manager.

If you do not see the updates try clicking on the Find Updates button in the toolbar. If you do not see the updates still you may want to wait up to 24 hours before retrying. This has to do with the way the update CDN works and how Joomla! caches the update information.

If there is an update available for Akeeba Backup tick the box to the left of its row and then click on the Update button in the toolbar. Joomla! will now download and install the update.

If Joomla! cannot download the package, please use one of the manual update methods described below. If, however you get an error about copying files, folder not found or a cryptic "-1" error please follow our installation troubleshooting instructions [https://www.akeebabackup.com/documentation/troubleshooter/abinstallation.html].

If you get a white page while installing the update please try either the Built-in method (described above) or the manual update method (described below).

## Updating manually

As noted in the installation section, installing and updating Admin Tools is actually the same thing. If the automatic update using Joomla!'s extensions update feature does not work, please install the update manually following the instructions in the installation section of this documentation.

### Important

When installing an update manually you MUST NOT uninstall your existing version of Admin Tools. Uninstalling Admin Tools will always remove all your settings. You do not want that to happen!

Sometimes Joomla! may forget to copy some files when updating extensions. If you find Admin Tools suddenly not working or if you get a warning that your installation is corrupt you need to download the latest version's ZIP file and install it *twice* on your site, *without* uninstalling it before or in-between these installations. This will most certainly fix this issue.

If the error occurs again after a while, without you updating our software, please contact your host. Some hosts will delete or rename files automatically and without any confirmation as part of a (broken and unfit for purpose) "malware scanner / antivirus". Unfortunately, these scanners return a lot of false positives -innocent files mistakenly marked as malicious- but rename / delete them nonetheless, breaking software installed on the server. If you are on such a host we very strongly recommend that you move to a decent host, run by people who actually know what they are doing. It will be far less headache for you and would actually improve your site's security.

# 6. 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 you can request support for it through our site. You will need to log in to our site and go to Support, Admin Tools 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 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 official Joomla! 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 the official Joomla! forum or any other Joomla!-related forum in your country/region. We have to impose those restrictions in support to ensure a high level of service and quality. Thank you for your understanding.

# 7. Quick Setup

## Important

This section applies only to Admin Tools Professional and refers only to its security 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 section (as a standard Joomla! error message) until you run the wizard or manually configure Admin Tools through the Configure WAF and .htaccess Maker / NginX Conf Maker / web.config Maker pages or import a configuration from the Import Settings page.

If you have already configured Admin Tools you will NOT see the Quick Setup Wizard button any more.

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 will provide no support if you choose to do that. Instead go to Admin Tools, Web Application Firewall, Configure WAF to configure the Joomla! system plugin protection settings or Admin Tools and .htaccess Maker (or Nginx Conf Maker; or web.config Maker depending on your web server) to configure the server-level protection settings.

The fundamental functionality of Admin Tools Professional is to allow you to secure your site. However, setting up your site's security does require some tweaking, as each site is 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! In this tutorial we will go through the basic security configuration and point you to what you want to do next.

Go to the back-end of your site and click on Components, Admin Tools, Web Application Firewall, Configure WAF and set the following optional settings:

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/administrator?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 (NOT RECOMMENDED AND NOT SUPPORTED!) a NEW, COMPLETELY RANDOM value will be shown in this field.

2. Enter your email address in Email this address on successful back-end login and Email this address on failed back-end login. Admin Tools will be sending you an email whenever anyone tries to log in to your site's back-end as a Super 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.

3. Set Hide/customise generator meta tag to `Yes` and enter something obscure in the Generator tag. I usually jokingly set "Drumlapress" in there, mudding the waters as to which CMS I'm really using. Be creative! This is

a low-priority thing to do, but stops "dork scanning" attacks. What I mean is that normally Joomla! spits out its name in the (hidden) generator meta tag on every HTML page on your site. An attacker looks for "dorks" (sites to exploit) by searching for "Joomla! 1.5" on Google. This feature removes that generator tag and you're not susceptible to this kind of attack.

4. 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 Admin Tools' Project Honeypot HTTP:BL Key field. Also set Enable HTTP:BL filtering to Yes. Why? 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 Joomla!.

5. Optional, but highly recommended, enable the IP blocking of repeat offenders. This feature 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. If that does happen, please take a look at https://www.akeebabackup.com/documentation/troubleshooter/atwafissues.html

6. There are a couple of potentially annoying features in Admin Tools Professional's Web Application Firewall. These features have a strong tendency to throw false positives, i.e. mark legitimate requests as attacks. These features are:

   - CSRF/Anti-spam form protection (CSRFShield)

   If you are not a very advanced user we strongly recommend turning them off; all of them are considered "paranoid security" features and do need you to be on the lookout for false positives and apply workarounds (WAF Exceptions, adding IPs to the "Never block these IPs" list, etc). Problems are especially common on sites with a forum or a payment system, as this is what triggers most of the false positives. We'd like to note that most sites do not need them to be enabled and, in fact, we even disable them on most of our own sites.

If you are using the Apache web server another thing to do is to go to Components, Admin Tools, .htaccess Maker and click on Save and Create .htaccess. If you get a blank page or 500 Internal Server Error on your site, use your FTP client to delete the `.htaccess` file (if it's not visible, just upload an empty text file named `.htaccess`), go back to .htaccess Maker, try disabling some option and repeat the whole process until your site loads correctly. For more information, take a look at https://www.akeebabackup.com/documentation/troubleshooter/athtaccess500.html

If you are using the NginX web server you should go to to Components, Admin Tools, NginX Configuration Maker and follow the instructions on the page to create a security and performance optimised site configuration file.

If you are using the Microsoft IIS web server you should go to to Components, Admin Tools, web.config Maker and follow the instructions on the page to create a security and performance optimised site configuration (web.config) file.

After applying all of the above protections, it is very likely that some of your site's functionality is no longer working. This is normal. The default settings are very restrictive by design. On each page with a problem, first try applying the step by step process outlined in https://www.akeebabackup.com/documentation/troubleshooter/athtaccessexceptions.html

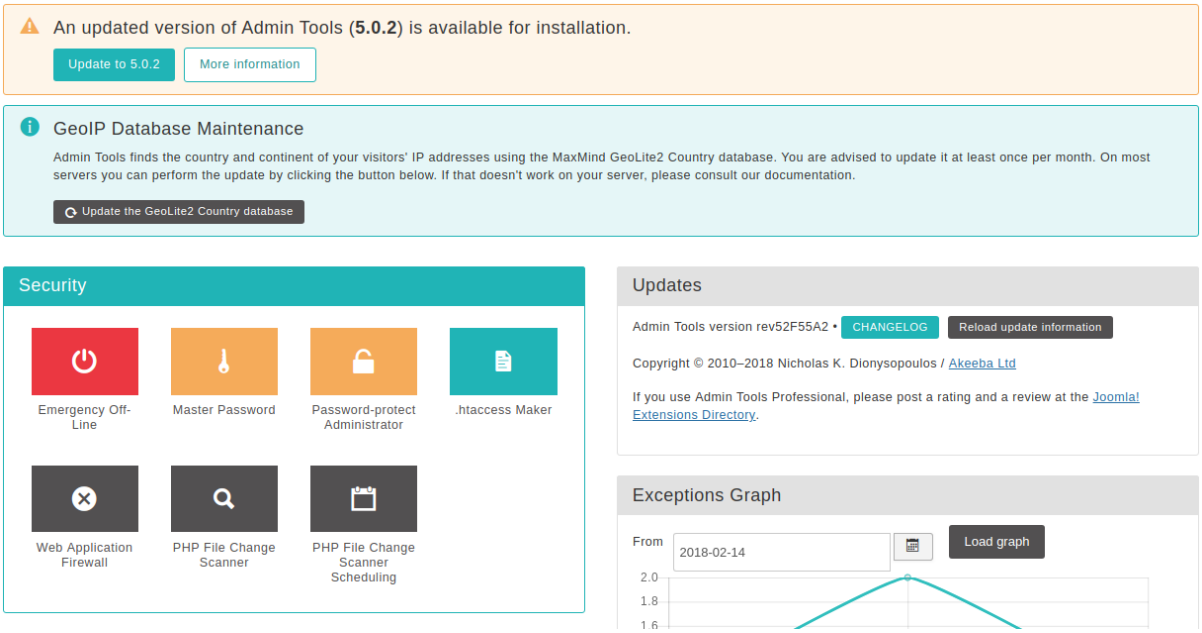
If you get stuck somewhere, feel free to file a support ticket (if you are a subscriber). We are here to help!

# Chapter 2. Using Admin Tools

## 1. The Control Panel

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

### The Control Panel page




The Control Panel is split in three areas, a top area, the left-hand control panel icons and the right-hand information boxes.

If there is an update available, you will see the information about it at the very top of the page. Click on the Update button to go to the Joomla! extensions update page where you can install the update.

The top area displays information about the Geographic IP (GeoIP) database. Please read on towards the bottom of this section for more information.

In the left hand area you have icons which launch the individual tools out of which Admin Tools is made when clicked. Each of those tools is described in a section of its own in the rest of this documentation.

Clicking on the Scheduling (via plugin) button will launch the System - Admin Tools plugin configuration page in a pop-up dialog box. In there, you can configure the scheduling options for Admin Tools' utilities. Do note that this feature is only available in the Professional edition.

The topmost right hand information pane displays the Admin Tools version information. You can see the version of the software, as well as force-reload the update information for Admin Tools itself. The latter is only necessary if there was an update released in the last 24 hours and your copy of Admin Tools has not "seen" it yet.

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.

## What is the GeoIP database, installing and updating it

#### Note

This product includes GeoLite2 data created by MaxMind, available from MaxMind [http://www.maxmind.com]. This is only required by the Professional version of the component.

Certain features in Admin Tools require it to be able to find out the country and / or continent associated with the IP address of a visitor of your site. This is used to provide country information on blocked requests, as well as the Geographic IP Block feature. Naturally, IPs do not carry geographic information so we need an external database which has this kind of information.

Admin Tools requires you to install an optional plugin called "System - Akeeba GeoIP provider plugin". You can download it for free from our site [https://www.akeebabackup.com/download/akgeoip.html]. Please remember to enable it after you install it.

This plugin is using the third party MaxMind GeoLite2 database to match IPs to countries and continents. This list is not static, i.e. it is updated about once per month. Admin Tools can attempt to download its newest version by clicking the Update the GeoLite2 Country database button in the Control Panel page. However, if this is not possible (for reasons ranging from your host restrictions to permissions issues) you can do so manually.

You can download the latest version of MaxMing GeoLite2 database [http://dev.maxmind.com/geoip/geoip2/geolite2/] in binary format, from http://geolite.maxmind.com/download/geoip/database/GeoLite2-Country.mmdb.gz. Extract the downloaded compressed file using gunzip on Linux, 7-Zip on Windows or BetterZIP on Mac OS X. It will result in a file named `GeoLite2-Country.mmdb`. Upload it to your site's `plugins/system/akgeoip/db` directory overwriting the existing file.

### Important

Capitalization matters! You have to upload the file as `GeoLite2-Country.mmdb.gz`, not `geolite2-country.mmdb.gz` or any other combination of lowercase / capital letters, otherwise IT WILL NOT WORK, AT ALL.

### Tip

If you are a subscriber to MaxMind's more accurate (99.8% advertised accuracy), for-a-fee GeoIP Country database you can use that database instead of the free GeoLite2 database included in the component, using the same procedure.

Do note that security exception log records prior to installing the new version of the database will not be affected. Only security exceptions logged after uploading the new database version will be affected by the new database version.

# 2. The component Options

You can access the component-wide options of Admin Tools through the Options button in its Control Panel page. Alternatively, you can go to your site's System, Global Configuration menu item and click on Admin Tools on the left hand sidebar.

Please note that this page is rendered and managed by Joomla! itself. We have very minimal control over it, namely on the names and types of the fields. The way that page displays and behaves is entirely controlled by Joomla! and your backend template. If you have observed a display or behavior issue the chances are we cannot help you since we cannot (and must not!) modify core Joomla! code. Such bugs should be reported to Joomla! instead.

The page has several tabs, documented below.

## File Scanner

Configure how the PHP File Change Scanner works . This option only makes sense in the Professional edition which has the PHP File Change Scanner feature.

| | |
|---|---|
| Calculate diffs when scanning | When this option is enabled, Admin Tools will calculate a "diff" for each modified file detected by the PHP File Scanner feature. The "diff" is a compact summary of the differences between the original and the current file. In order for this to be possible, Admin Tools has to |

keep a copy of each and every .php file on your site inside the database. Be advised that this consumes **a lot** of database space, about 20M for a relatively low to medium complexity site.

Send results to this email
When you make a scan from the site's frontend or through the CLI script the scan results will be automatically sent to this email address. If you leave it blank no email will be sent in this case.

Email only on actionable items
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. If nothing has changed you will get no email. Please remember that being sent an email requires setting up the Send results to this email option above.

# Backend

Options which define how the backend of the component works.

Show graphs and statistics
Display graphs and statistics about security exceptions (Professional release only). 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.

Long Configure WAF page
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. We generally recommend the tabbed version as it's easier to manage.

Automatically reorder the plugin
The System - Admin Tools plugin needs to be ordered as the first published plugin to work correctly. When you visit Admin Tools in the backend the plugin is automatically reordered to be the first one. In some rare cases other plugins need to be published first, for example alternative mail handlers such as CMandrill. In this case set this option to No.

WARNING! If you set this option to No it's up to you to reorder the plugin. If a vulnerable plugin is published before the System - Admin Tools plugin your site can be hacked. Admin Tools will be unable to protect you in this case since it will not be running before the vulnerable code, therefore unable to detect the attack. Do not set this option to No unless you are absolutely sure you understand the risks.

Warn about manual edits on server configuration files
When this is enabled Admin Tools will check whether a file generated by .htaccess Maker, Nginx Conf Maker or web.config Maker has been modified outside of Admin Tools whenever you visit Admin Tools' main page in the backend of your site. This is done by comparing the checksum of the file with the one stored in your site's database when the file was generated. If the two checksums are different you will be asked whether you want to regenerate the file or ignore any such changes. The latter option changes this setting, "Warn about manual edits on server configuration files", to No.

We strongly recommend NOT changing generated files by hand. Instead, put any custom code in the provided areas for putting custom directives at the top or bottom of the file. In any other cases your manual changes will be overwritten every time you use Admin Tools' .htaccess Maker, Nginx Conf Maker or web.config Maker on your site.

# Frontend

This allows you to schedule the PHP File Change Scanner by accessing a special frontend URL.

Enable frontend scheduling
When enabled it allows you to the PHP File Change Scanner without logging in to the backend. This option is NOT required for using the CLI script.

Secret Word
Required to authorize a remote PHP File Change Scanner execution. Also protects that feature against Denial of Service attacks by requiring you to pass this secret word in the front-end PHP File Change Scanner URL.

Please note that if you use any character other than a-z, A-Z and 0-9 you MUST NOT use the secret word verbatim in the front-end URL. Instead, you have to URL-encode it. The PHP File Change Scanner Scheduling page does that automatically for you. Just go to Components, Admin Tools, click PHP File Change Scanner Scheduling, scroll all the way down and use one of the tabs to get the URL or command line you need to use with the secret word properly encoded in the URL.

For security reasons, you must use a complex enough secret word. Admin Tools enforces that by disabling the front-end scanner feature if you are using a Secret Word with a low complexity. We strongly recommend using a "secret word" consisting of at least 16 random, mixed case alphanumeric characters. It should not be a dictionary word or based off a dictionary word. One good resource for truly random secret words is Random.org's password generator [https://www.random.org/passwords/?num=1&len=24&format=html&rnd=new].

### Note

**Why is this field not a password field?** The Secret word is transmitted in the clear when you load the page and is also visible when you view the source of the page or right click on the field and choose Inspect Element. In other words, as long as someone has access to the component configuration page they can trivially find out the secret word. Not to mention that the secret work is also plainly visible in the PHP File Change Scanner Scheduling page. Always use HTTPS with a commercially signed SSL certificate when configuring or scanning your site.

Timezone for emails

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. use the option Server Timezone to let Admin Tools use the Server Timezone setting in your site's System, Global Configuration page.

Default: GMT

# Updates

Configure how updates to the component work

Download ID

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 AkeebaBackup.com 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.

### Note

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

Enable anonymous PHP, MySQL and Joomla! version reporting

Help us improve our software by anonymously and automatically reporting your PHP, MySQL and Joomla! versions. This information will help us decide which versions of Joomla!, 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.

# Permissions

This is the standard Joomla! ACL permissions setup tab. Admin Tools fully supports supports Joomla! ACLs.

# 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. If you are on a shared host you will most likely want to enable Joomla!'s FTP layer in your site's Global Configuration. Admin Tools will detect that and when it runs across a file or directory whose permissions can't be changed by PHP will use FTP to perform this task.

### Note

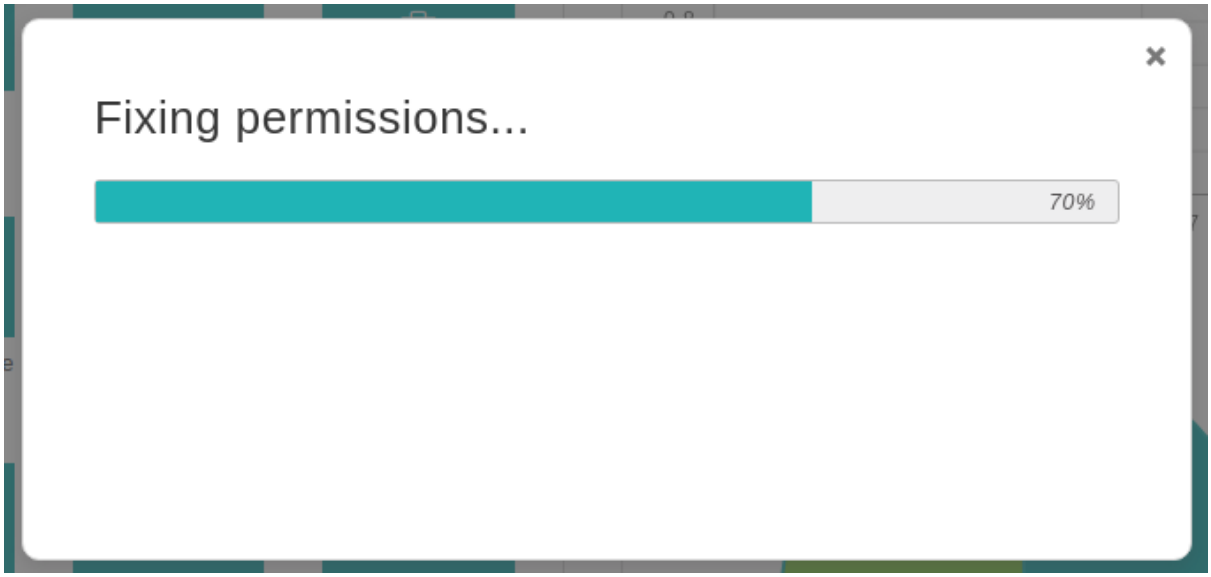
You can customize the permissions per folder and file using the Permissions Configuration page.

### 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.

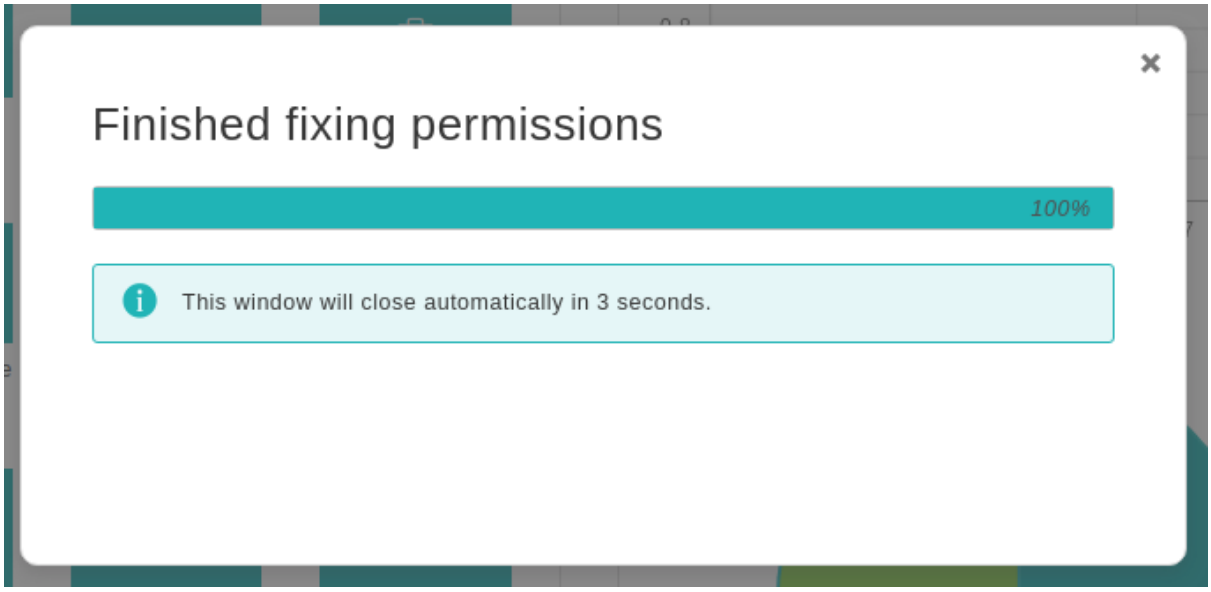
When you click on the Fix Permissions tool you are going to see the "Fixing Permissions..." pop-up window with a progress bar filling up as Admin Tools is changing the permissions of all your directories and files.

**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**




Just click on the Back button to return the the Control Panel page.

# 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. All you have to do is go to the Global Configuration page of your site, enter your FTP details and enable Joomla!'s FTP option. Admin Tools will pick it up next time you try to fix permissions and automatically use the FTP mode whenever it can't change permissions directly.

# I can see a lot of JFTP error messages in red background during that process. What's wrong?

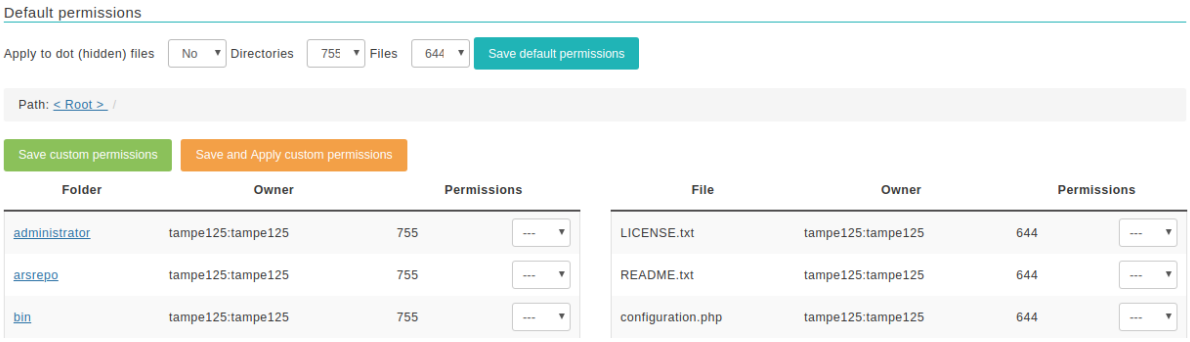
Admin Tools, as explained in the above paragraph, tries to use the FTP mode whenever it can't change the permissions directly. In order for this trick to work, your FTP server must support the CHMOD command. Not all servers do, though, especially those running on Windows where there is no notion of permissions. If you get this long list of JFTP Bad Response messages, please ask your host whether their FTP server supports the CHMOD command.

Finally, some hosts place directories inside your web root which are not meant to be directly accessible to you, i.e. a `cgi-bin` or a `stats` directory. You can't change the permissions of those directories due to their ownership (they are usually owned by a reserved system user or the root user) and will cause a few JFTP error messages to be spat out. This is normal and you shouldn't worry about that.

# 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. Since Admin Tools 1.0.b1 you can do that using the Permissions Configuration button in the component's 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. Click on the Back button to return to the Control Panel page where you can find this button.

Alternatively, you can click on the Fix and Apply 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.

Joomla!'s off-line feature, the one you can enable in your site's Global Configuration, has a major deficiency. It doesn't put the site off-line. All it does is to replace the output of the component with the "off-line" page. This has grave security implications, especially when you need to take your site off-line to deal with a security breach (e.g. a hacked site) or to update a key component of your site. For more information about this problem, please read this article [http://www.dionysopoulos.me/blog/how-offline-is-joomla-offline-mode].

The Emergency Off-Line Mode of Admin Tools enables you to *really* and *securely* take your site off-line. More specifically, the Emergency Off-Line Mode does 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


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 always use the emergency off-line mode instead of Joomla!'s off-line feature?

The short answer is, simply, no. There are many cases where using Joomla!'s off-line feature is more convenient, i.e. when you want to simply make your site's content unavailable to random web visitors and search engines while building a new site. The only cases when you should use the Emergency Off-Line Mode are:

- If you believe that your site has been compromised (hacked). The Emergency Off-Line will make it impossible for the hacker to access your site while you are working to restore it.
- When updating key components of your site and don't want to risk a user following a direct link to screw up the process.

In all other cases it's more convenient and sufficient to go to your site's Global Configuration and enable the off-line feature of Joomla! itself.

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

Thank you for noticing that! 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 my PC and I can still see my site.

First, I have to ask the obvious question: did you *really* read the description of this feature? You are supposed to be able to see your site only from your PC. 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. One good idea is to use your cellphone, as long as it connects to the Internet over 3G, 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 an old version of Apache —1.3 or 2.0— which doesn't support one 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, I don't know. When I used to have a dynamic IP address I observed that my IP address wouldn't change if my connection dropped for less than 1-2 minutes. 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. Protect your administrator back-end 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 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.

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

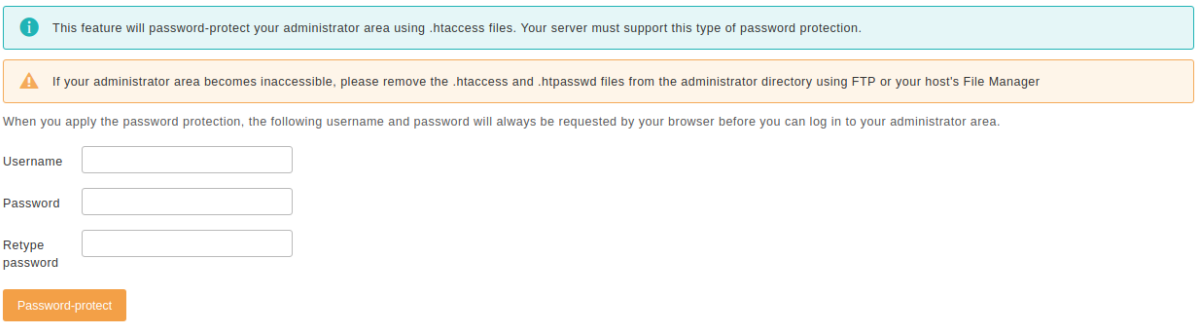
### Important

Some prepackaged server bundles, such as Zend Server CE, 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 (for Zend Server CE this is located in `C:\Program Files\Zend\Apache2\conf` or `C:\Program Files (x86)\Zend\Apache2\conf`) 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 administrator 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 administrator 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 administrator 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 Joomla error page when enabling this feature

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 administrator 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.

If that wasn't bad enough, Joomla is always configured to catch all missing files and try to figure out if it should try and serve a Joomla page instead. This is required for the correct operation of search engine friendly URLs. So, Joomla sees the missing file error. Not knowing what to do with it, it tries to route it through com_content (the built-in Articles component). Hard as it may try, it can't find an article category which matches the URL. This causes Joomla to throw an error. This is what ends up being displayed as the 404 or Joomla error page you are receiving.

When you disable custom error pages for the 401 error code you let Apache communicate that status directly to the browser without Joomla 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.

# 6. 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 search engine friendly (SEF) URLs, 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, such as Zend Server CE, 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 (for Zend Server CE this is located in `C:\Program Files\Zend\Apache2\conf` or `C:\Program Files (x86)\Zend\Apache2\conf`) and modify all AllowOverride lines to read:

```
AllowOverride All
```

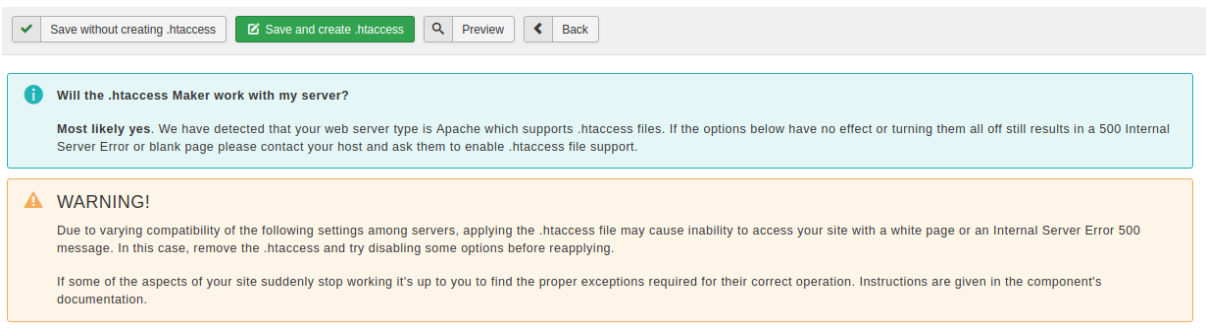
If you are on a live host, please consult your host about the possibility of them allowing you to use this feature on your site.

### 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 create a `.htaccess` file which is essentially the same as the one shipped with Joomla! (`htaccess.txt`).

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

## The .htaccess Maker's toolbar



- Save without creating .htaccess saves the changes you have made in this page's options without actually creating the customized `.htaccess` file. This should be used when you have not decided on some options yet, or if you want to preview the generated `.htaccess` file before writing it to disk.
- Save and create .htaccess is the logical next step to the previous button. It not only saves the changes you made, but also creates and writes the new `.htaccess` file to the disk. If you already had a `.htaccess` file on your site, it will be renamed to `.htaccess.admintools` before the new file is written to disk.
- Preview pops up a dialog where you can see how the generated `.htaccess` file will look like without writing it to disk. This dialog shows the saved configuration. If you have modified any settings they will not be reflected in there until you click either of the previous two buttons.
- The Back button takes you back to the Control Panel page.

Below the toolbar there are five panes with different options, described below. Before you do that, please read and understand the following warning. Support requests which indicate that you have not read it will be replied with a link back to this page.

### 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 remove the `.htaccess` file from your site's root directory using an FTP application or the File Manager feature of your hosting control panel. Since Admin Tools 1.2, your old `.htaccess` file is saved as `.htaccess.admintools`. 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. In this case you are strongly suggested to enable it. 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.

# Other important things you can add to your .htaccess

Some things cannot be added as features to the .htaccess Maker because the interface would become truly unwieldy. However, there are tools which can generate rather compact .htaccess rules which you can add to .htaccess Maker, in the Custom .htaccess rules at the top of the file section. Here we'd like to point you to some of them.

**Content security policy (CSP)**

It mitigates the risk of cross-site scripting and other content-injection attacks. You can read more about it on the dedicated site for this feature [http://content-security-policy.com/]. There is a simple tool [http://cspisawesome.com/] which allows you to generate the required .htaccess code for the CSP feature according to your preferences. Keep in mind that when you restrict the scripts' origin you should keep in mind that several extensions (including many templates) will load their scripts off a third party CDN which must be whitelisted or your site will no longer work!

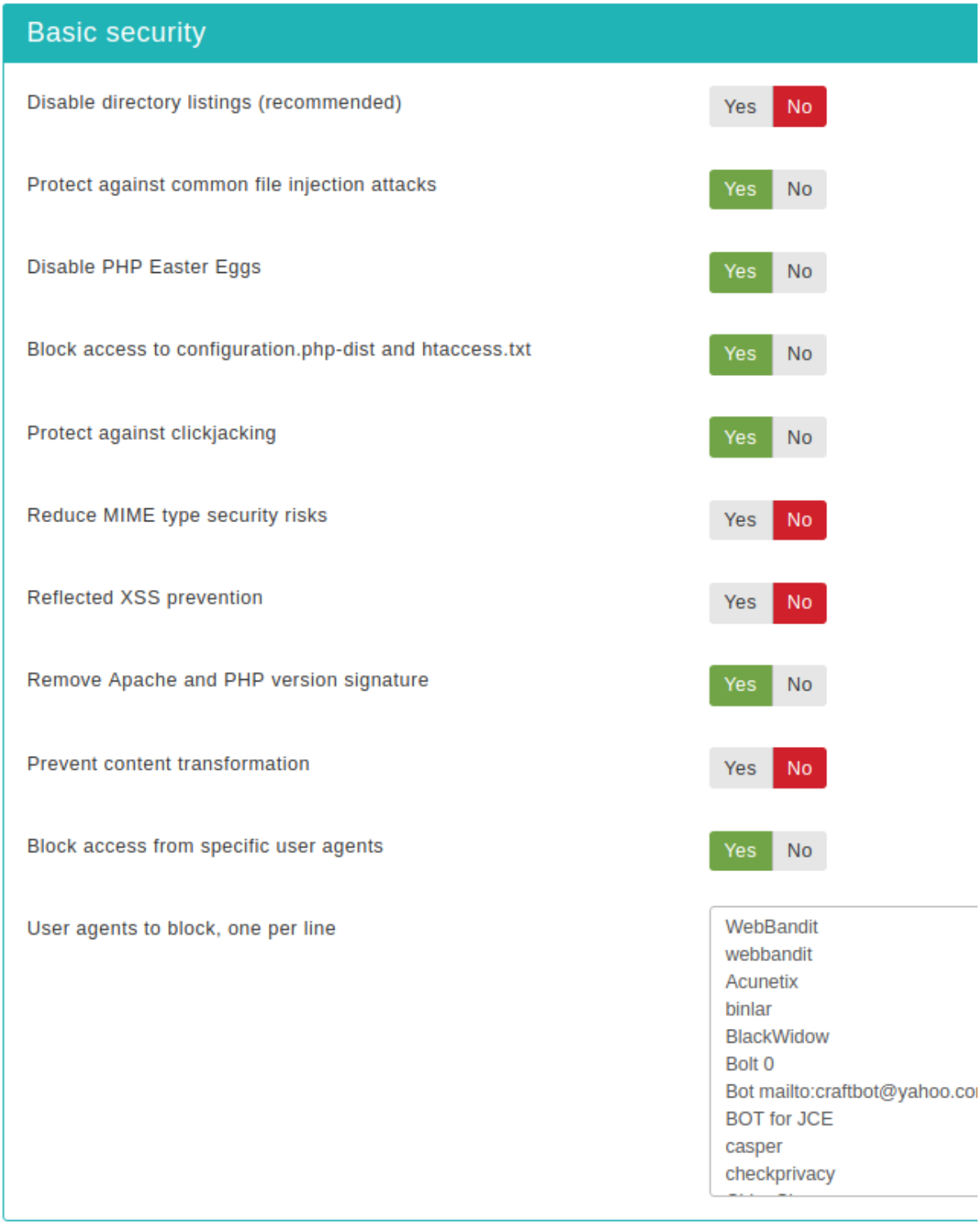
**Custom error documents**

Most hosting control panels allow you to specify custom HTML pages for common server error pages. The most important ones are for errors 403 (Access Forbidden), 404 (Not Found) and 500 (Internal Server Error). It's always

a good idea showing a nicely designed page instead of the default, text-only, ugly page of Apache for these error messages!

# 6.1. Basic Security

### Basic security




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 gallery components 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

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.

Note: You are advised to also set *`expose_php`* to `Off` in your `php.ini` file to prevent accidental leaks of your PHP version.

Block access to configuration.php-dist and htaccess.txt

These two files are left behind after any Joomla! installation or upgrade and can be directly accessed from the web. They are used by attackers to tell the Joomla! version you are using, so that they can tailor an attack targeting your specific Joomla! 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. This option also hides the web.config.txt file included in Joomla! 3 and later for use with the IIS server.

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

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).

This is a commonly used method used by attackers to compromise web sites, especially when a zero-day XSS vulnerability is discovered in popular Joomla! extensions or Joomla! 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.

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 Javscript 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 tragically ancient 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 Joomla!, 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 3. 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 try it out. Just copy it and paste it in the User agents to block, one per line are in the .htaccess Maker configuration. 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.

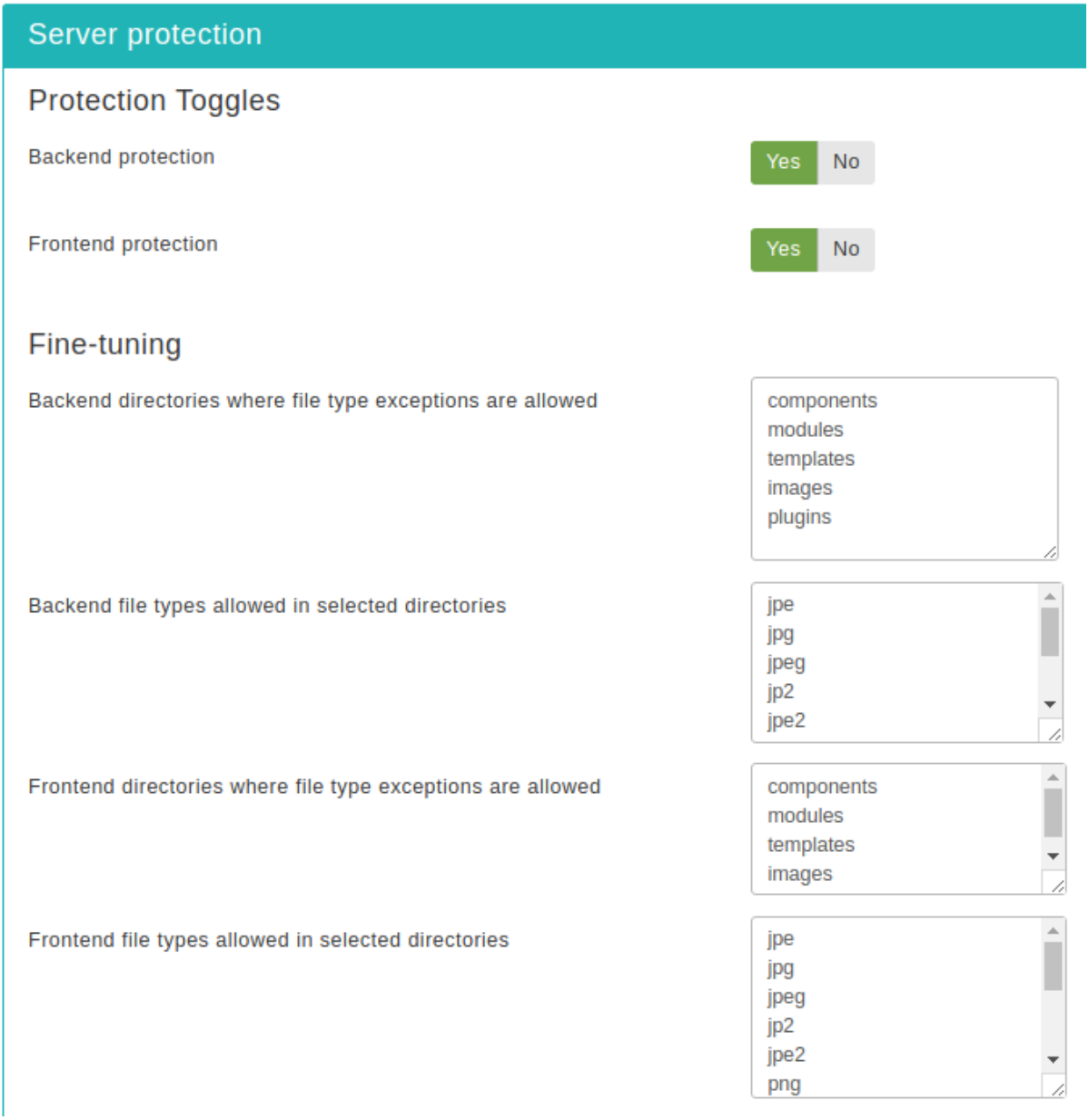
```
WebBandit
webbandit
Acunetix
binlar
BlackWidow
Bolt 0
Bot mailto:craftbot@yahoo.com
BOT for JCE
casper
checkprivacy
ChinaClaw
clshttp
cmsworldmap
comodo
Custo
Default Browser 0
diavol
DIIbot
DISCo
dotbot
Download Demon
eCatch
EirGrabber
EmailCollector
EmailSiphon
EmailWolf
Express WebPictures
extract
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
planetwork
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
Wget
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
```

# 6.2. Server protection

### Server protection




This is the most coveted feature of our software, offering a near-inclusive protection against the vast majority of known threats when enabled. This feature's mission statement can be summed up with a single phrase: nothing executes on your site unless you allowed it to. By blocking access to front-end and back-end 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 INI files, which are usually used by attackers to find out which version of Joomla! you are running on your site to tailor an attack to your site. On the downside, you have to explicitly enable access to some extensions' PHP files which are designed to be called directly from the web and not through Joomla!'s main file, `index.php` and `index2.php`.

Do note that enabling this feature will kill the functionality of some extensions which create arbitrarily named PHP files throughout your site, such as RokGZipper. In our humble opinion the security risk of having your site

unprotected outweighs the benefits of such solutions by a dramatic factor. As a result, we strongly suggest disabling RokGZipper and other similar software using similarly questionable security practices.

There are three sections of configuration settings controlling the functionality of the Server Protection feature. The first one is the Protection Toggles which allows you to enable or disable the four main aspects of protection:

Back-end protection
: Disables direct access to most back-end resources, except those in the exceptions lists. It is generally recommended to turn it on to enhance the protection of your site, unless you have enabled the administrator password protection feature. In the latter case this option is redundant and we recommend turning it off.

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

  Enabling this feature will prevent web access to all folders in your site's root, not just Joomla's folders (such as components). If you need to enable direct access to a folder you will need to place it in one of the *front-end* directory exception lists in the Fine-tuning or Exceptions section.

The next section is called Fine-tuning and contains the necessary options to tweak the protection's behaviour to suit your site. 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. Joomla!'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 Joomla! 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.

Back-end directories where file type exceptions are allowed
: This is a list of back-end directories (that is, subdirectories of your site's administrator directory) where you expect media files to be present. Place one directory on each line. Subdirectories of those directories are automatically added to the exceptions list without having to explicitly list them here.

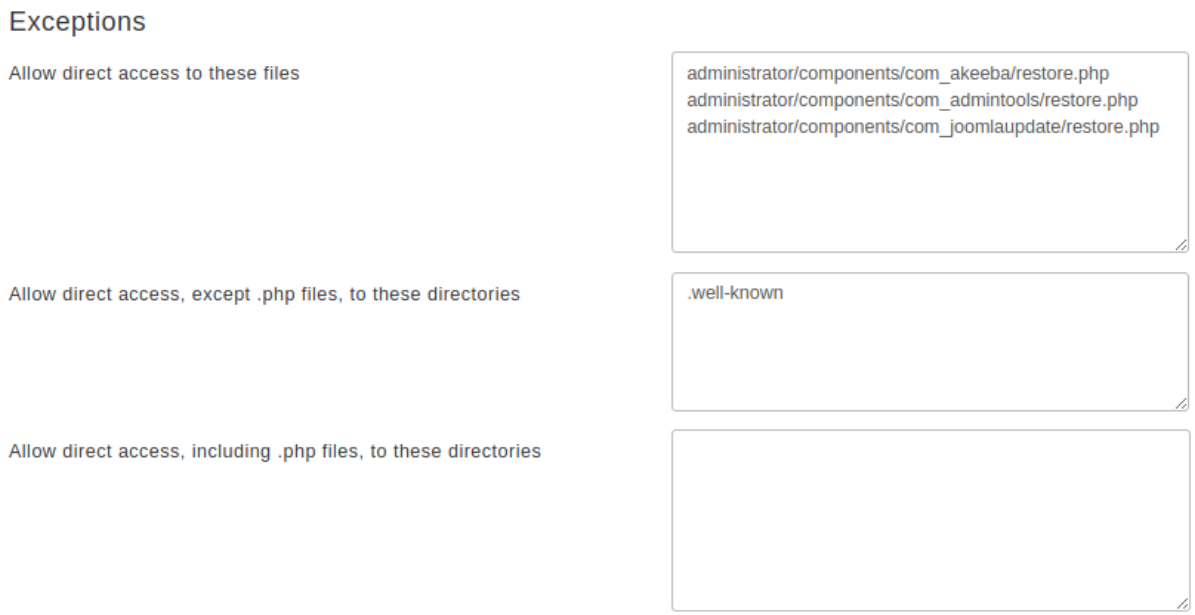
Back-end file types allowed in selected directories
: The extensions of back-end files which allowed to pass through the server protection filter, as long as the files with those extensions are in the list above. Place one file extension per line, without the dot. For example, if you want to allow access to all PDF files you have to type in "pdf" (without the quotes) 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.

Front-end directories where file type exceptions are allowed
: This is a list of front-end directories (that is, directories in your site's root) where you expect media files to be present. Place one directory on each line. Subdirectories of those directories are automatically added to the exceptions list without having to explicitly list them here.

  Use this to allow access to specific types static media files inside specific directories. This is the least permissive exception to front-end blocking. Use this for folders which have a mix of public and private content, as long as the private content is NOT of an allowed file type (see below).

Front-end file types allowed in selected directories
: The extensions of front-end files which allowed to pass through the server protection filter, as long as the files with those extensions are in the list above. 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" (without the quotes) 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.

## Exceptions




Finally, we have the Exceptions section. 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, some extensions need to directly access PHP files, without passing them through Joomla!'s main files. 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. Other prime examples are CSS and Javscript minifiers, either included in your template or installed on top of your site. Forum attachments are also part of the same problem, as they tend to create a dedicated directory for their attachments, avatar icons and so forth. Moreover, some extensions place PHP files inside your site's `tmp` and `cache` directories and expect them to be directly accessible from the web. While this is a stupid behaviour, contrary to the design goals of Joomla! itself, you still need a way to work around them and we have to provide it. Finally, you may have a third party script (e.g. Coppermine gallery, phpBB forum, WordPress blog, or even another Joomla! site in a subdirectory) which doesn't install as a Joomla! extension. 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:

| | |
|---|---|
| Allow direct access to these files | Place one file per line which should be exempt from filtering, therefore accessible directly from the web. The default settings include Akeeba Backup Professional and, of course, Admin Tools itself. |
| Allow direct access, except .php files, to these directories | Direct access to all files (except for .php files) will be granted if they are inside any of the directories in this list. Normally you should only need to add your forum's attachments, avatars and image galleries directories, or other directories where you only intend to store media files. The example is Agora forum's user files directory. As with all similar options, add one directory per line, without a trailing slash.<br><br>Use this to allow access to all files, except executable .php files, in specific directories. This is a middle ground in front-end blocking. You should use this only for folders which have only public content, i.e. if it's in that folder you are OK with it being shared with the rest of the world. |
| Allow direct access, including .php files, to these directories | 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:<br><br>• If you have installed another Joomla!, WordPress, phpBB, Coppermine gallery 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 templates and template frameworks may wrap their CSS and Javscript 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 extensions do something silly: they place files inside your site's `tmp` or `cache` directories and expect them to be directly accessible from the web. This is plain wrong because these directories are designed to be protected system directories where direct access should not be allowed, most notably because they might contain sensitive information. However, if you have such extensions —most notably certain Javascript and CSS minifiers— you need a way to allow direct access to those directories.

  If you decide that convenience is better than security we can't stop you. Add tmp and cache to this list and wish for the best. You are opening a security hole on your site and you do it at your own risk and potential peril.

Use this to allow full access to specific folders, as if the front-end protection does not exist. This is EXTREMELY dangerous! It's best to use the Allow direct access to these files feature if possible, allowing access only to very specific .php files.

Remember that an attacker who has found an upload vulnerability on your site can upload a malicious script inside one of these folders and use it to hack you. These folders are bare and unprotected. That's why we very strongly advise against using this feature unless it's absolutely necessary - keeping in mind that you are, at the same time, leaving a hole in your security defences. Holes in defences is what gets sites hacked.

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.

## 6.2.1. How to determine which exceptions are required

After applying the Server Protection settings you may notice that some aspects of your site no longer work properly or at all. This could be something obviously throwing an error; files being inaccessible with a 403 or 404 error message; or something more subtle, as if CSS and JavaScript no longer load. These are probably caused by the Server Protection settings disallowing access to files. We can find which files need to be accessed and add exceptions to them to restore the functionality of your site.

### Tip

There is no valid reason for software integrated with Joomla! to require such exceptions for .php files anymore. Since early 2013 Joomla! has shipped with com_ajax, a built-in method to access dynamic content without needing direct access to arbitrarily named .php files. Developers who have not caught up to this technology after so many years are less likely to follow security best practices. Moreover, most of these directly accessible .php files do not load Joomla!, therefore they do not load Admin Tools, meaning that you are no longer protected by Admin Tools' Web Application Firewall if malicious requests are being sent to those files. As a result, adding extensions for their software's .php files to be accessible directly from the web can compromise your site's security.

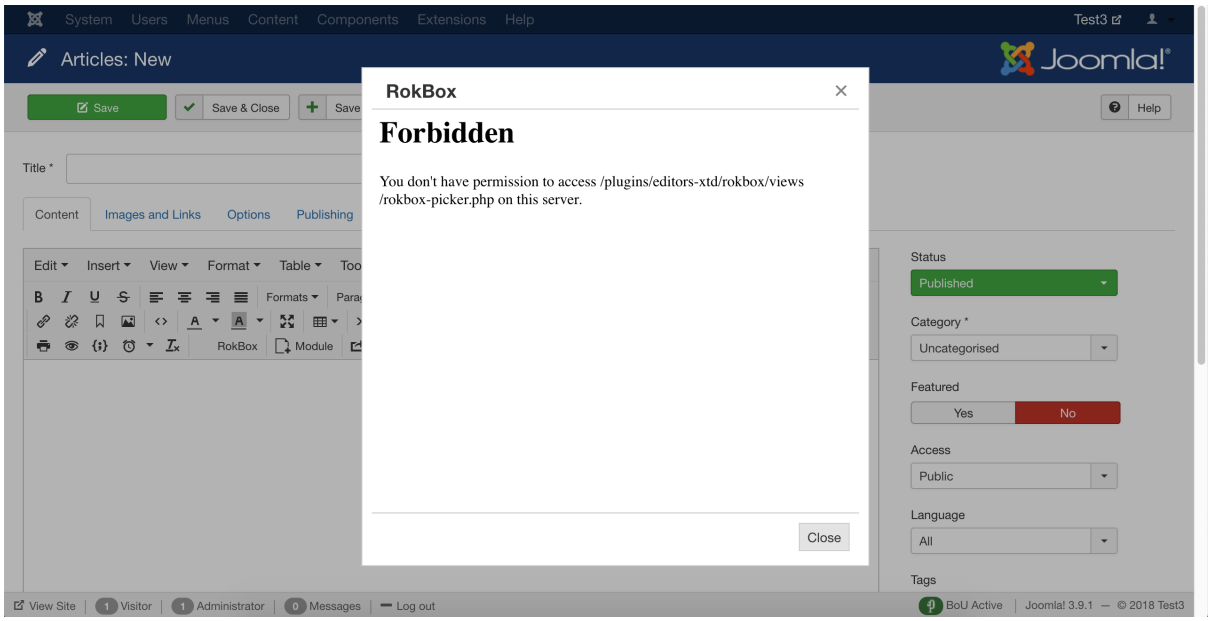
Exceptions for non-.php files – such as CSS, JavaScript, images, fonts etc – may still be required and are generally not a security issue. Some static content can be a security issue if it's accessible over the web (e.g. JSON files containing privileged information such as usernames, passwords and API keys) but these cases are rare and you shouldn't be overly worried about them.

The process of determining which exceptions are required is made relatively easy by modern browsers. All modern browsers include "developer tools" which give us insight on what is going on when the browser tries to load your page. They even highlight the errors for us, making our work much easier.

In the following example we are going to be using Mozilla Firefox. The process is very similar on Google Chrome, Opera, Safari and Microsoft Edge. If you are not sure how to open the developer tools for your browsers do a quick search on the Internet similar to *`developer tools <your browser name here>`*.

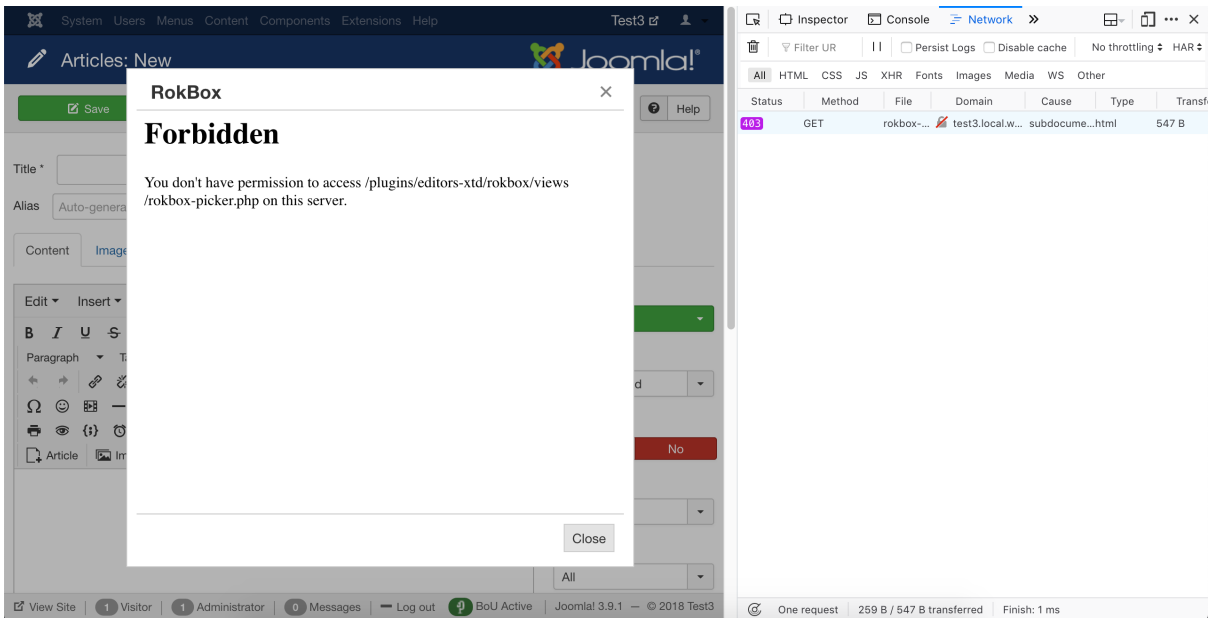
Our example makes use of RokBox, an extension by RocketTheme, which causes a problem when used through the Joomla! article editor in the backend of the site. The instructions also apply to the frontend of your site and any other extension which might be causing a problem.

After applying the Server Protection settings in the .htaccess Maker we get the following error when we click on the RokBox button in the editor:



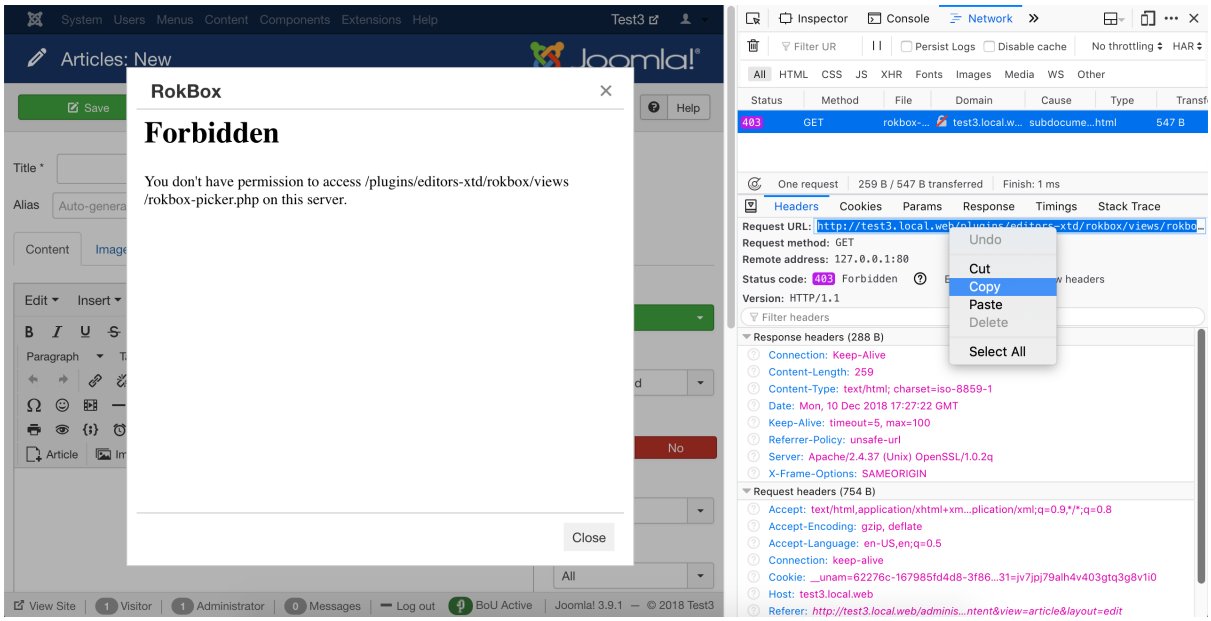

This is a vague error message. We want it to be that way to not give away any information about our site to bad guys. At the same time it makes our life a bit harder. Click on Close to dismiss that non-functional dialog.

Click on Firefox' hamburger menu (the three horizontal lines button towards the top right of its window), Web Developer, Toggle Tools. This opens a side pane. On that pane there's a top menu. Click on the Network option. You may have to click on the >> arrows first to see it. Then click on the RokBox button on your editor. You now see something interesting happen in the Web Developer pane:

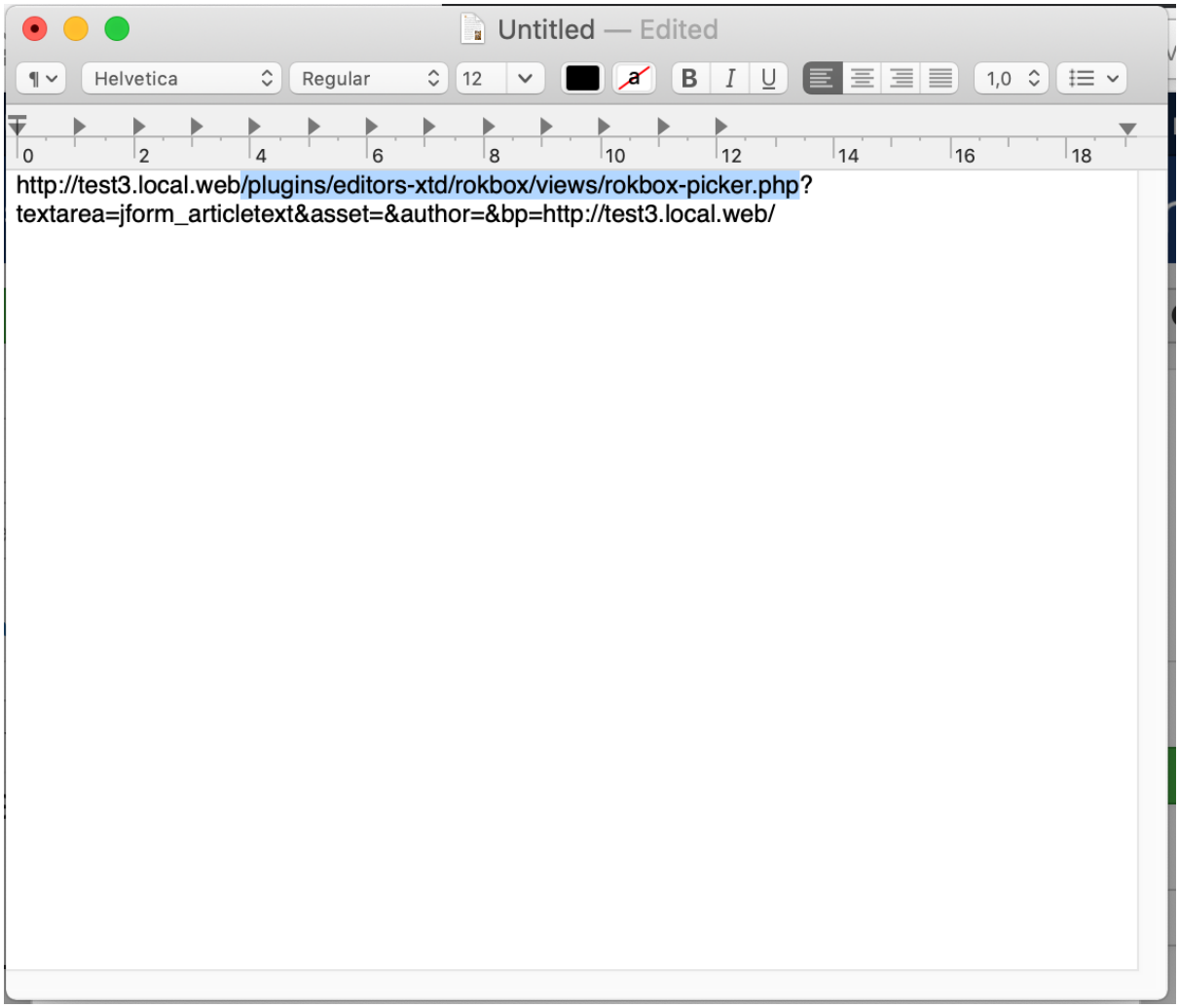



The pane shows the request made to your server and its error status 403 highlighted. 403 means access forbidden, 404 means not found. The former is an error code we definitely expect as the result of applying Server Protection. The latter can either mean that the file is genuinely not there or that Server Protection is preventing access to it. If you get a 404 always check if the file exists first. Since we have a 403 here we know it's a Server Protection issue.

Click on the line with the error code. You will see some details open below the list. Click on the Headers tab on top of those details. You see a lot of information but what is interesting to us is the Request URL. It tells us which URL the browser tried to access and failed to do so. However, it's truncated and doesn't help us any. So right click on it and choose Copy.



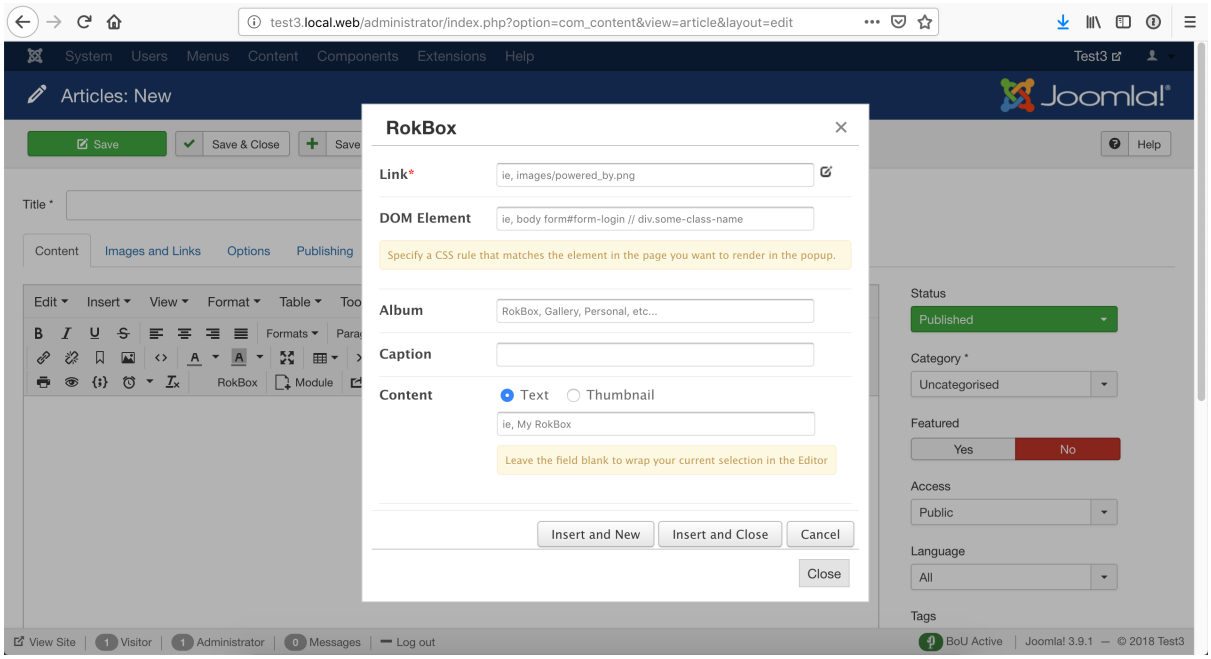

Now open a plain text editor application such as Notepad on Windows, TextEdit on macOS, gEdit or Kate on Linux and paste in the URL you copied.




Highlight the stuff between your site's root URL and the question mark (if there is no question mark, highlight to the end of the line). In our example the site's URL is http://test3.local.web and the highlighted portion is `plugins/editors-xtd/rokbox/views/rokbox-picker.php` which, as you may have guessed, is the relative path to the file blocked by Server Protection. Copy this.

Now go to Components, Admin Tools, .htaccess Maker and find the Allow direct access to these files box.


In a new line paste the relative file path you had highlighted previously. Make sure you do not include the leading slash or the trailing question mark. Click on Save and Create .htaccess in the toolbar to apply your changes. Now the extension works:




## In case you see plenty of files or files with random and changing names; or you see files in the cache, tmp and logs folders

Sometimes the above method will show a long list of files; or files with random names; or files whose names change on every page or request. Typically, you see that they are all located in the same few folders. There are two different things you can do.

**If the files you see do not have a .php extension** the the easy way is to add the path to the folder to the Allow direct access, except .php files, to these directories list. For example, if all files are in the `foobar/assets/static` folder you need to add `foobar/assets/static` to the Allow direct access, except .php files, to these directories list.

The drawback to that is that *all* files without a .php extension in this folder and its subfolders will be accessible over the web. This might be a security risk if the same folder contains files with privileged information. You can mitigate that risk by adding an exception in a harder, but more secure, way. You'd need to add the folder's path to the Backend directories where file type exceptions are allowed or Frontend directories where file type exceptions are allowed lists in the .htaccess Maker. If the folder's relative path starts with `administrator/` add it to the first list (backend) after removing the `administrator/` prefix.

For example, if the files are in the `administrator/components/com_example/media` folder you need to add `components/com_example/media` to the Backend directories where file type exceptions are allowed list. Conversely, if the files are in the `foobar/assets` folder you need to add `foobar/assets` to the Frontend directories where file type exceptions are allowed list.

Please note that in this case (hard way) if the file extension is not in the Backend file types allowed in selected directories or Frontend file types allowed in selected directories lists you will need to add the file extension, without the dot, in those lists as well. Keep in mind that capitalization matters. For example, the extensions png, PNG and Png are different and have to be listed separately.

**If the files you see have a .php extension** things are easier but also more nuanced. You can always add the path to the folder in the Allow direct access, including .php files, to these directories list. *This is potentially insecure.* It allows direct web access to all files in that folder and all of its subdirectories, bypassing Joomla! and Admin Tools entirely. If there are files with privileged information they will be accessible to everyone. If the .php files have a security issue in them you will get hacked. This is why we DO NOT advise you to do that.

What we do advise you to do is contact the developer of the offending extension and ask them to fix their code to always go through Joomla's index.php files (e.g. using com_ajax). If they decline to do that you should consider

using a different extension. There is absolutely no reason whatosever to have directly accessible .php files in Joomla! since 2013. Well, actually, there is one: when you are overwriting Joomla! itself. Since Joomla! is being overwritten with a different version you cannot also use it at the same time, thus making the only valid use case of not going through Joomla. This is exactly what the restore.php files in com_joomlaupdate (the Joomla! Update component which is part of Joomla! itself) and Akeeba Backup (when restoring a backup) do and that's why they are the only two built-in exceptions in Admin Tools. Both files were written by Akeeba Ltd, they are locked when you are not actively updating/restoring a site, they are protected with a password when you are actively updating/restoring a site and they have been audited by independent security researchers several times.

Finally, a special mention is due for extensions which try to access files stored in the `cache`, `logs` or `tmp` directories in the front- and backend of your site. These directories are NOT meant to be web accessible. In fact, they are designed in such a way that it's possible to move them outside of your site's web root. Moreover, their content is supposed to be transient, i.e. it is expected to be deleted at any point in time and the extension is supposed to not break when that happens. Web accessible files generated by extensions are supposed to go into the `media` folder in the root of your instead. This folder has been available since Joomla! 1.5.0 came out in 2007. Any developer who does not understand a concept introduced over a decade ago is certainly not following security best practices. As a result *we very strongly recommend NOT using these extensions, ever, at all cost.*

# 6.3. Custom .htaccess rules

### Custom .htaccess rules

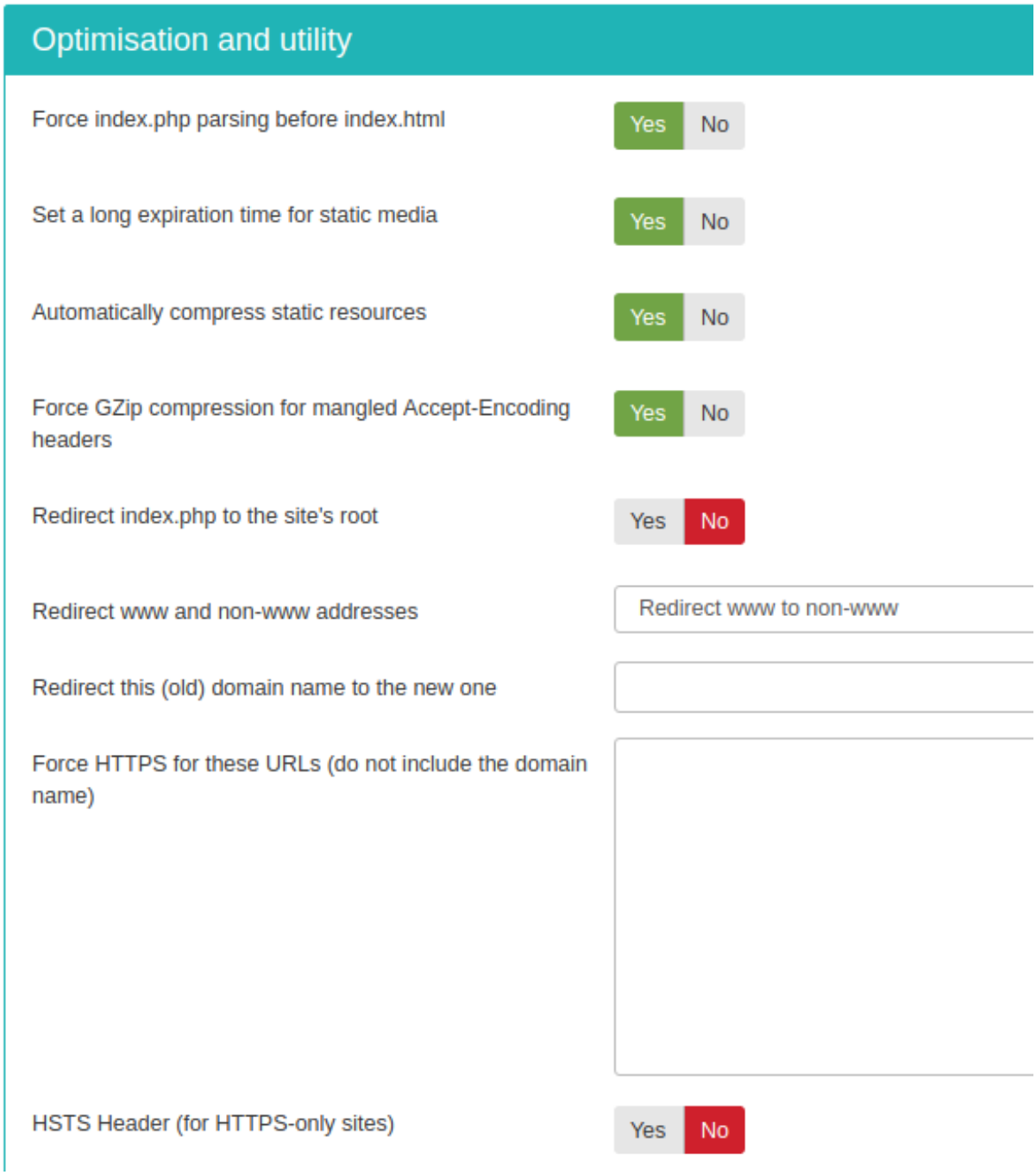

Sometimes you just need to add custom .htaccess rules beyond what the .htaccess Maker can offer. Such examples can be special directives your host told you to include in your .htaccess file to enable PHP5, change the server's default error documents and so on. If you are an advanced user you may also 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 file, 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 file. This is the place to put stuff like directives to enable PHP5 and any optimizations which should run only after the request has passed through the security and server protection rules.

# 6.4. Optimisation and utility

### Optimisation and utility




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 Joomla! 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 a long expiration time for static media

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 between 1 week or 1 month (depending from the media), which means that the browser will not try to load them over the network until that time has passed. This is a very desirable feature, as it speeds up your site.

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.

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 in 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 adresses

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, as we did migrating from joomlapack.net to akeebabackup.com. 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, sending to the darkest hole of search engine results. Not good! 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:

```
joomlapack.net, www.joomlapack.net
```

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

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

Under regular circumstances Joomla! should be able to automatically redirect certain menu items to a secure (HTTPS) address. However, this is not possible if the HTTPS domain name and the HTTP domain name are not the same, as is casual with many shared hosts. Since Admin Tools supports custom HTTPS domain names you can use this feature to make up for the lack of functionality in Joomla! itself. 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. Easy, isn't it?

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. Joomla! offers a Global Configuration setting to force SSL throughout the entire site, but this is merely a workaround: if it sees a request coming through HTTP it will forward it to HTTPS. There are two privacy implications for your users:

- If you have not enabled the SSL option in Global Configuration a man-in-the-middle attack known as "SSL Stripping" is possible. 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 Joomla! forwards your user to HTTPS 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 an 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

Since Admin Tools 4.0.0 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. In previous versions no such redirection took place.
- 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. In previous versions we were always using plain HTTP.
- Old to new domain redirection will always redirect to the HTTPS domain name, as configured in the .htaccess Maker. In previous versions all redirections were made to the HTTP 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. Previously it was send over HTTP requests which is not advisable.

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 Joomla! pages will appear correctly –Joomla! 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!

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>` elelements.
- **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 |
|---|---|---|
| https://www.yoursite.com/url1 | http://www.yoursite.com/url2 | NULL |
| https://www.yoursite.com/url1 | https://www.yoursite.com/url2 | https://www.yoursite.com/url1 |
| http://www.yoursite.com/url1 | http://www.yoursite.com/url2 | http://www.yoursite.com/url1 |
| http://www.yoursite.com/url1 | http://www.example.com | http://www.yoursite.com/url1 |
| http://www.yoursite.com/url1 | https://www.example.com | http://www.yoursite.com/url1 |
| https://www.yoursite.com/url1 | http://www.example.com | 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 |
|---|---|---|
| https://www.yoursite.com/url1 | https://www.yoursite.com/url2 | https://www.yoursite.com/url1 |
| https://www.yoursite.com/url1 | http://www.yoursite.com/url2 | NULL |
| https://www.yoursite.com/url1 | http://www.example.com | NULL |

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

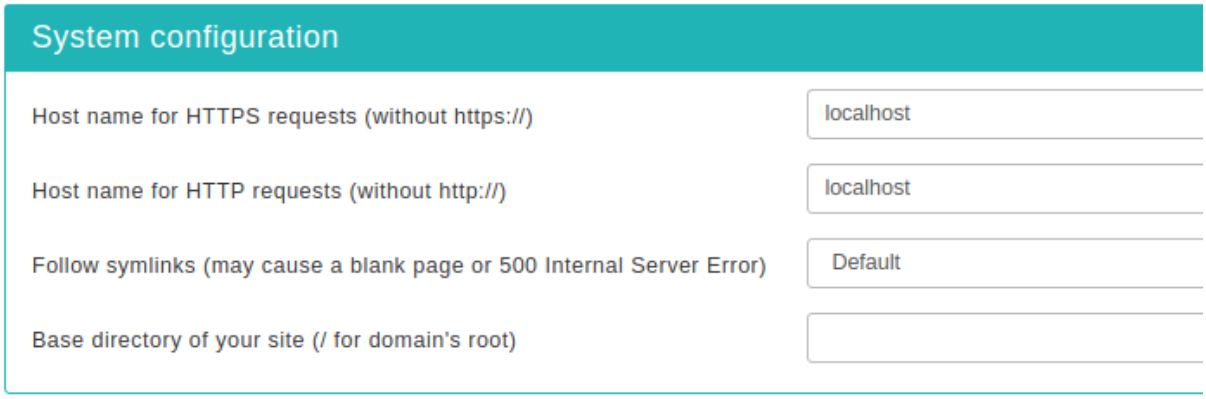
- **unsafe-url** The browser will always send the full URL with any request to any origin.

# 6.5. 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, change this parameters and then let Admin Tools create a new .htaccess file before you can use your site's front-end.

### System configuration




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 and path to your site. For example, if the address is `https://www.example.com/joomla` then type in `www.example.com/joomla`.

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 and path to your site. For example, if the address to your site's root is `http://www.example.com/joomla` then type in `www.example.com/joomla`.

Follow Symlinks
: Joomla! 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 BAD idea. Worse than bad, it's a horrible 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 or Joomla!'s htaccess.txt file.

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

# 7. The NginX configuration maker

## Note

This feature is only available in the Professional release

## Warning

This feature is only available on servers running the NginX web server. If your server is using Apache or IIS the button to launch this feature will not be shown. If the server type cannot be detected you will see this feature but you should consult with your host whether it will have any effect and how to use it..

One of the most important aspects of managing a web site hosted on an NginX server is being able to fine-tune your site configuration file. This file is responsible for many web server level tweaks, such as enabling the use of search engine friendly (SEF) URLs, 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 NginX Configuration Maker tool of Admin Tools is designed to help you create the part of such a file used for security and performance optimisation by utilizing a point-and-click interface.

## 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 nginx.conf". This will create an empty nginx.conf file.

One very important aspect of NginX is that, unlike Apache, the site configuration file is not magically loaded on every request. When using this feature you will have to do two things:

1. **Make sure NginX can load the nginx.conf file**. Admin Tools writes the (partial) NginX configuration file `nginx.conf` in the root of your site. By default, NginX won't even know this file is there! You need to include it in your site's definition file by adding a directive like this:

   ```
   include /home/myuser/www/nginx.conf;
   ```

   The exact path to the file is shown in Admin Tools' NginX Configuration Maker page itself. You only need to do this ONCE.

   If your host doesn't allow you to do that they might be giving you a way to add custom NginX configuration variables. In this case use the Preview button in the NginX Configuration Maker page to get the raw NginX configuration commands and give them to your host for inclusion in the NginX configuration.

   If you have a choice between these two methods of providing the custom NginX configuration to your server *please use the second one*. It's harder to manage but it's far more secure. The first method of having your NginX server include a configuration file off the web root is not a good idea as far as security is concerned: a sly attacker could modify that file to their benefit and just wait for the NginX server to restart. Ideally, that first method should only be used on a private test server which is not accessible from the Internet and only for debugging and development purposes.

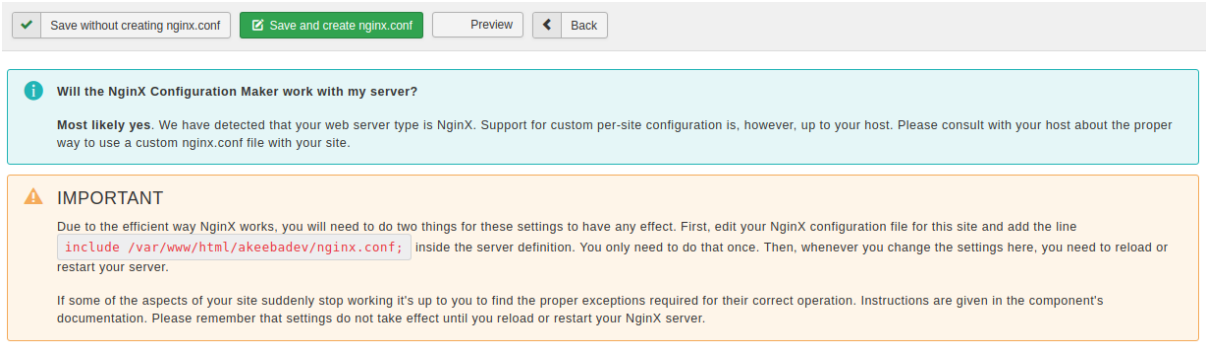
   If your host doesn't allow you to provide custom NginX configuration, sorry, you're out of luck: you will not be able to use this feature of Admin Tools.

2. **Reload or restart your NginX server**. Remember that modifying the NginX configuration has NO EFFECT until you reload or restart the NginX server. This is part of what makes NginX so incredibly fast.

FInally, do note that the NginX configuration maker makes the assumption that you've configured PHP to run through FastCGI using the exact method described in NginX's documentation [http://wiki.nginx.org/PHPFcgiExample]. If you're using a different method to enable PHP on your NginX server the generated configuration may not work on your server or even cause problems accessing your web site.

The top part of the NginX configuration maker page contains the standard toolbar buttons you'd expect:

## The NginX Configuration Maker's toolbar




- Save without creating nginx.conf saves the changes you have made in this page's options without actually creating the customized `nginx.conf` file. This should be used when you have not decided on some options yet, or if you want to preview the generated `nginx.conf` file before writing it to disk.
- Save and create nginx.conf is the logical next step to the previous button. It not only saves the changes you made, but also creates and writes the new `nginx.conf` file to the disk. If you already had a `nginx.conf` file on your site, it will be renamed to `nginx.admintools` before the new file is written to disk.
- Preview pops up a dialog where you can see how the generated `nginx.conf` file will look like without writing it to disk. This dialog shows the saved configuration. If you have modified any settings they will not be reflected in there until you click either of the previous two buttons.
- The Back button takes you back to the Control Panel page.

Below the toolbar there are five panes with different options, described below. Before you do that, please read and understand the following warning. Support requests which indicate that you have not read it will be replied with a link back to this page.

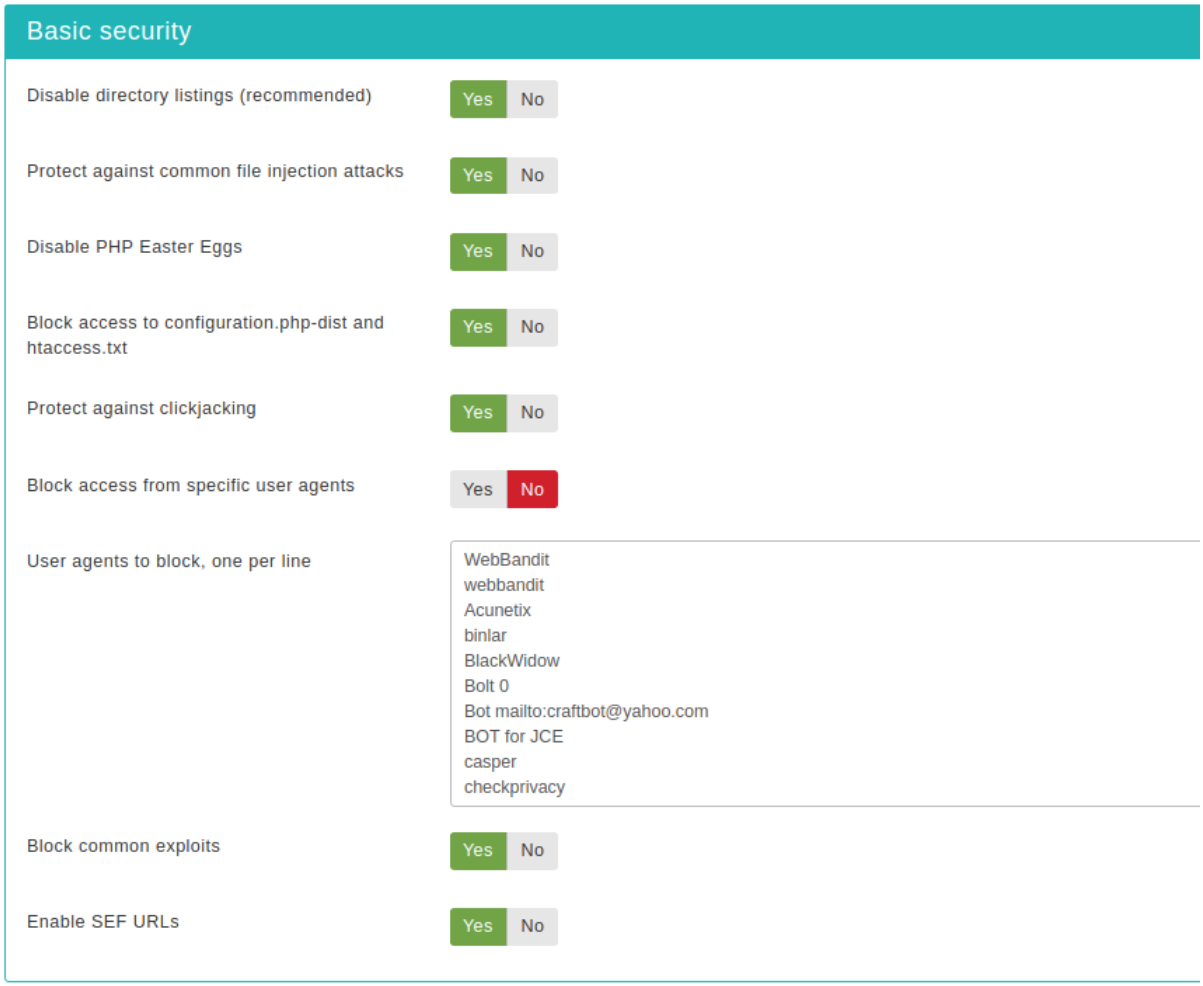
### Warning

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 remove the contents of `nginx.conf` file from your site's root directory using an FTP application or the File Manager feature of your hosting control panel OR remove all custom configuration from your NginX site configuration file (depending on which method you chose). Then you MUST reload or restart NginX for the changes to take effect.

We strongly suggest that you begin by setting all options to No and then enable them one by one, creating a new configuration (and reloading your NginX server) 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. Unfortunately, there is no other way than trial and error to deduce which options may be incompatible with your server.

# 7.1. Basic Security

### Basic security



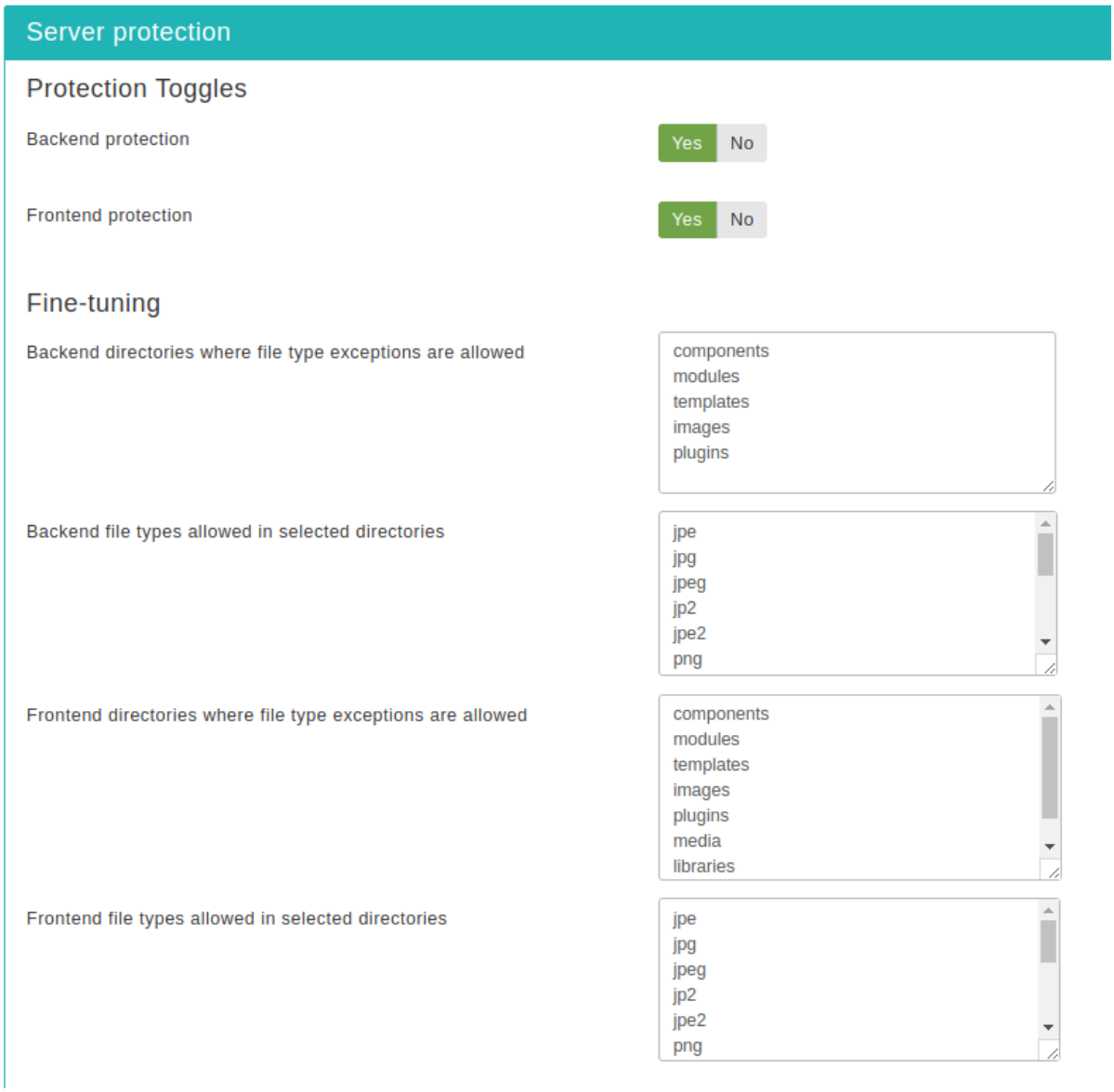

Disable directory listings (recommended)

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 gallery components use them. In this case you are recommended to use the RFIShield (Remote File Inclusion protection) in the Web Application Firewall and turn this NginX Configuration Maker option OFF. |
| Disable PHP Easter Eggs | 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.<br><br>Note: You are advised to also set *`expose_php`* to `Off` in your `php.ini` file to prevent accidental leaks of your PHP version. |
| Block access to configuration.php-dist and htaccess.txt | These two files are left behind after any Joomla! installation or upgrade and can be directly accessed from the web. They are used by attackers to tell the Joomla! version you are using, so that they can tailor an attack targeting your specific Joomla! 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. This option also hides the web.config.txt file included in Joomla! 3 and later for use with the IIS server. |
| 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. |
| 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 Joomla!, it is a server-level protection feature kicking in. Just avoid including the word Wget and you should be out of harm's way. |
| Block common exploits | Enabling this option will include a set of options recommended by Joomla! to protect against (obsolete) common exploits which no longer have any effect on Joomla! 2.5 and later. It's still a good idea to enable this option. |
| Enable SEF URLs | Enabling this option will allow your site to use SEF (a.k.a. "beautiful") URLs, with or without index.php in them. You are recommended to leave this option turned on unless you have a custom URL forwarding setup already in place. |

# 7.2. Server protection

### Server protection




This is the most coveted feature of our software, offering a near-inclusive protection against the vast majority of known threats when enabled. This feature's mission statement can be summed up with a single phrase: nothing executes on your site unless you allowed it to. By blocking access to front-end and back-end 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 INI files, which are usually used by attackers to find out which version of Joomla! you are running on your site to tailor an attack to your site. On the downside, you have to explicitly enable access to some extensions' PHP files which are designed to be called directly from the web and not through Joomla!'s 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, such as RokGZipper. In our humble opinion the security risk of having your site unprotected outweighs the benefits of such solutions by a dramatic factor. As a result, we strongly suggest disabling RokGZipper and other similar software using similarly questionable security practices.

There are three sections of configuration settings controlling the functionality of the Server Protection feature. The first one is the Protection Toggles which allows you to enable or disable the four main aspects of protection:

| | |
|---|---|
| Back-end protection | Disables direct access to most back-end resources, except those in the exceptions lists. It is generally recommended to turn it on to enhance the protection of your site, unless you have enabled the administrator password protection feature. In the latter case this option is redundant and we recommend turning it off. |
| Front-end protection | Disables direct access to most front-end resources, except those in the exceptions lists. It is generally recommended to turn it on to enhance the protection of your site. |

The next section is called Fine-tuning and contains the necessary options to tweak the protection's behaviour to suit your site. Before describing what each option does, a small explanation of how the protection works is in order. The protection code in the generated `nginx.conf` file blocks direct web access to all files. Joomla!'s standard "entry point" or "main" files, `index.php` and `index2.php`, are 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 Joomla! 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.

| | |
|---|---|
| Back-end directories where file type exceptions are allowed | This is a list of back-end directories (that is, subdirectories of your site's administrator directory) where you expect media files to be present. Place one directory on each line. Subdirectories of those directories are automatically added to the exceptions list without having to explicitly list them here. |
| Back-end file types allowed in selected directories | The extensions of back-end files which allowed to pass through the server protection filter, as long as the files with those extensions are in the list above. 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" (without the quotes) 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. |
| Front-end directories where file type exceptions are allowed | This is a list of front-end directories (that is, directories in your site's root) where you expect media files to be present. Place one directory on each line. Subdirectories of those directories are automatically added to the exceptions list without having to explicitly list them here. |
| Front-end file types allowed in selected directories | The extensions of front-end files which allowed to pass through the server protection filter, as long as the files with those extensions are in the list above. 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" (without the quotes) 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. |

## Exceptions


Finally, we have the Exceptions section. 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, some extensions need to directly access PHP files, without passing them through Joomla!'s main files. 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. Other prime examples are CSS and Javscript minifiers, either included in your template or installed on top of your site. Forum attachments are also part of the same problem, as they tend to create a dedicated directory for their attachments, avatar icons and so forth. Moreover, some extensions place PHP files inside your site's `tmp` and `cache` directories and expect them to be directly accessible from the web. While this is a stupid behaviour, contrary to the design goals of Joomla! itself, you still need a way to work around them and we have to provide it. Finally, you may have a third party script (e.g. Coppermine gallery, phpBB forum, WordPress blog, or even another Joomla! site in a subdirectory) which doesn't install as a Joomla! extension. 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:

| | |
|---|---|
| Allow direct access to these files | Place one file per line which should be exempt from filtering, therefore accessible directly from the web. The default settings include Akeeba Backup Professional and, of course, Admin Tools itself. |
| Allow direct access, except .php files, to these directories | Direct access to all files (except for .php files) will be granted if they are inside any of the directories in this list. Normally you should only need to add your forum's attachments, avatars and image galleries directories, or other directories where you only intend to store media files. The example is Agora forum's user files directory. As with all similar options, add one directory per line, without a trailing slash. |
| Allow direct access, including .php files, to these directories | 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:<br>• If you have installed another Joomla!, WordPress, phpBB, Coppermine gallery 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 templates and template frameworks may wrap their CSS and Javscript 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 extensions do something silly: they place files inside your site's `tmp` or `cache` directories and expect them to be directly accessible from the web. This is plain wrong because these directories are designed to be protected system directories where direct access should not be allowed, most notably because they might contain sensitive information. However, if you have such extensions —most notably certain Javascript and CSS minifiers— you need a way to allow direct access to those directories.

  If you decide that convenience is better than security we can't stop you. Add tmp and cache to this list and wish for the best. You are opening a security hole on your site and you do it at your own risk and potential peril.

While it might seem very tempting to put several Joomla! system directories in here, like components and templates, don't. That's right. Do not do that. It is like using a tactical weapon to kill a mosquito in the same room as you. The mosquito will hardly ever survive, but you will go down with it. Or, in computing terms, you allow potential hackers to use any security vulnerabilities you haven't had the chance to fix yet in order to upload and *execute* malicious code. You killed the mosquito (the access problems you had with an extension) but you accidentally helped to take down your site. Ouch! Even if the chance of this happening is about one in ten thousand, are you willing to take that risk *on your own site*?

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

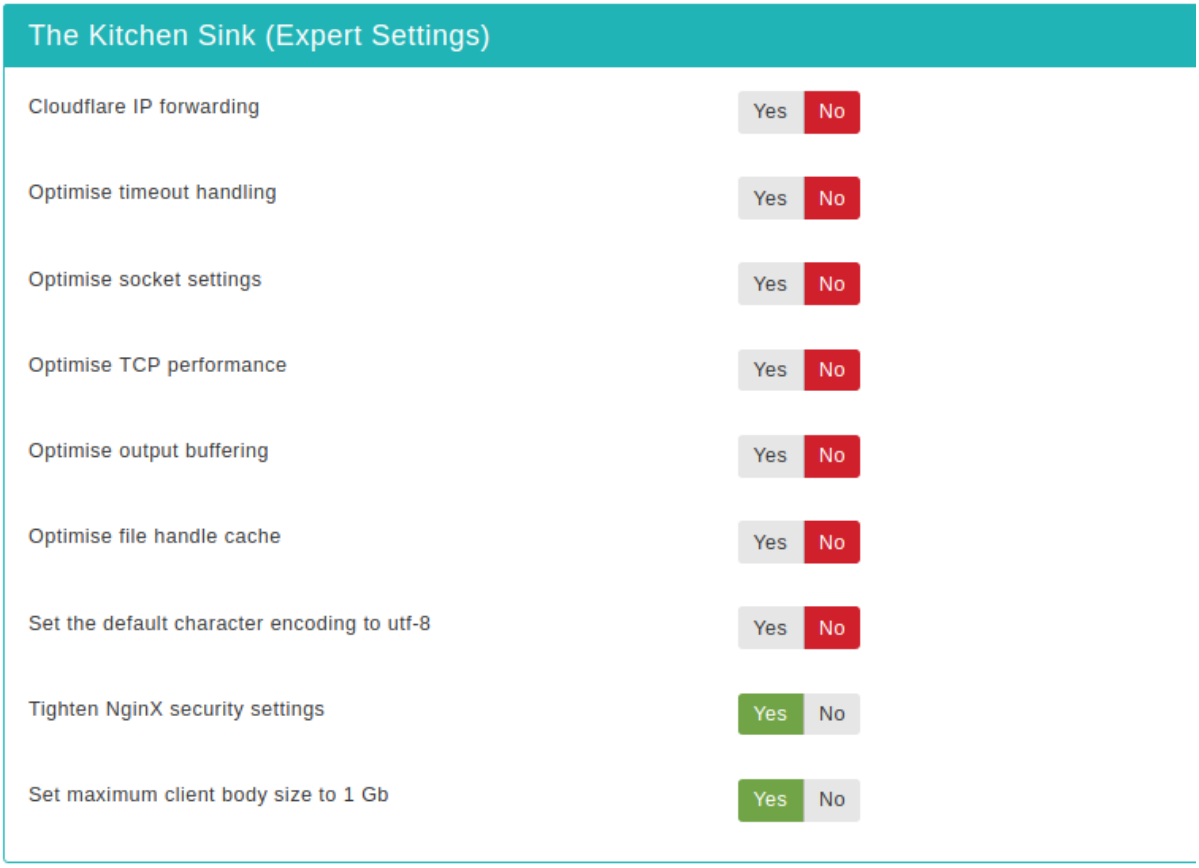
Windows users beware! *Do not* use Windows' path separator (the backslash - \) to separate directories! We are talking about directories as they appear in URLs, so you should always use the URL path separator (forward slash - /) in those settings. In other words `some/long/path` is correct, `some\long\path`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

## 7.2.1. How to determine which exceptions are required

Please refer to the section on determining exceptions under the .htaccess Maker documentation. The exact same process applies. The only difference is that you enter the exceptions in the NginX Conf Maker instead of the .htaccess Maker and you need to restart / reload NginX after adding the exceptions.

# 7.3. The Kitchen Sink (Expert Settings)

### Expert settings




This section contains advanced configuration options for use by expert users. If you are unsure you are recommended to leave them as they are. If you are an expert user you are advised to review the values used in the generated configuration file and further tweak them based on the capabilities of your server and the traffic on your site.

Cloudflare IP forwarding
: Enable if you are using the CloudFlare CDN service. Enabling this option will allow your NginX server to "see" the real visitor's IP instead of the CloudFlare CDN proxy IP. This is very important for the correct operation of the Web Application Firewall of Admin Tools.

> **Warning**
>
> This feature REQUIRES the ngx_http_realip_module module to be enabled in NginX, see http://nginx.org/en/docs/http/ngx_http_realip_module.html for more information. If the module is not enabled (default) your site will fail to load once you try reloading NginX with the new configuration.

Optimise timeout handling
: Enabling this option will create a set of rules which optimise the connection timeout. If you run into problems with lengthy processes (e.g. backups) you are advised to turn this off.

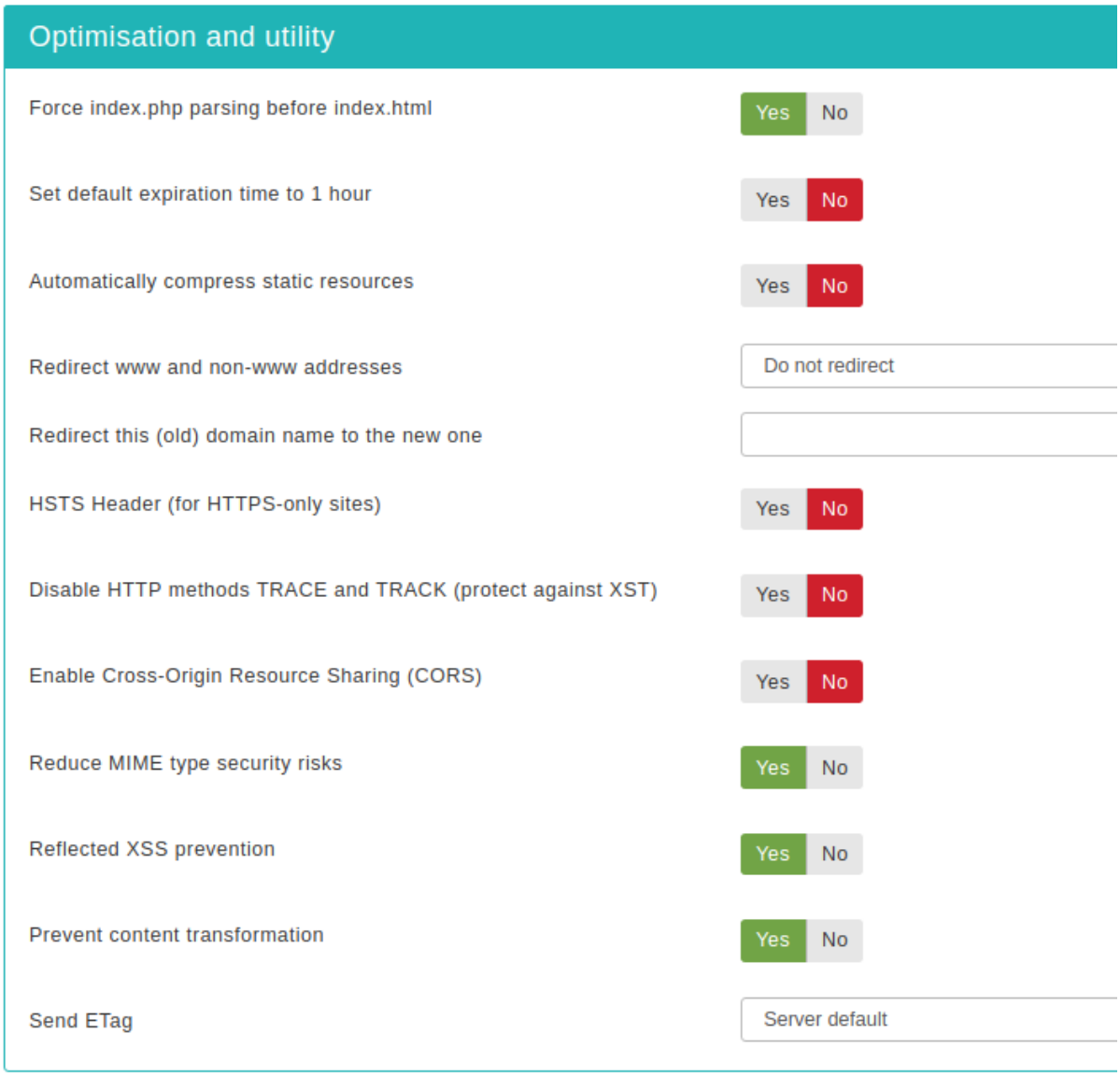
Optimise socket settings
: Enabling this option will create a set of rules which optimise the NginX connection pool size.

Optimise TCP performance
: Enabling this option will create a set of rules which optimise the TCP/IP performance of NginX and turn the sendfile feature on.

| | |
|---|---|
| Optimise output buffering | Enabling this option will create a set of rules which optimise the output buffers of NginX for typical servers. |
| Optimise file handle cache | Enabling this option will create a set of rules which optimise the NginX file handle cache for sites serving large amounts of static content (most Joomla! sites do that: images, CSS and JS are all static content). |
| Set the default character encoding to utf-8 | Enabling this option will set the default output encoding to UTF-8. This is not strictly necessary as Joomla! will do that by default in its output. This is primarily used when serving static content, e.g. CSS and JS files which may contain international characters. |
| Tighten NginX security settings | Enabling this option will create a set of rules which tighten NginX security: server names are hidden from redirects, the version of NginX is hidden from the output headers and invalid HTTP headers will be ignored. |
| Set maximum client body size to 1Gb | Enabling this option will set the maximum acceptable client body (usually this means POST and PUT) size to 1 Gb. Please note that you still need to set up the maximum POST size and maximum file upload size in php.ini to accept large uploads on your server. |

# 7.4. Optimisation and utility

### Optimisation and utility




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 Joomla! 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. Note: some files types have a higher expiration time of 1 week or 1 month.

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. We do add a directive which instructs NginX to not compress the output when accessed by IE6 but all bets are off with a browser that hasn't been updated for over a decade...

Redirect www and non-www adresses

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 on 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, as we did migrating from joomlapack.net to akeebabackup.com. 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, sending to the darkest hole of search engine results. Not good! 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:

```
joomlapack.net, www.joomlapack.net
```

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

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. Joomla! offers a Global Configuration setting to force SSL throughout the entire site, but this is merely a workaround: if it sees a request coming through HTTP it will forward it to HTTPS. There are two privacy implications for your users:

- If you have not enabled the SSL option in Global Configuration a man-in-the-middle attack known as "SSL Stripping" is possible. 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 Joomla! forwards your user to HTTPS 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 an 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].

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.

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 it 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

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).

This is a commonly used method used by attackers to compromise web sites, especially when a zero-day XSS vulnerability is discovered in popular Joomla! extensions or Joomla! 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.

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 Javscript 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].

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]

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.
- **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!

## Note

The lack of other options is intentional and has to do with an NginX limitation. NginX, unlike Apache, only offers a binary switch for ETags: you either send them or you don't.

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>` elelements.
- **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 |
|---|---|---|
| https://www.yoursite.com/url1 | http://www.yoursite.com/url2 | NULL |
| https://www.yoursite.com/url1 | https://www.yoursite.com/url2 | https://www.yoursite.com/url1 |
| http://www.yoursite.com/url1 | http://www.yoursite.com/url2 | http://www.yoursite.com/url1 |
| http://www.yoursite.com/url1 | http://www.example.com | http://www.yoursite.com/url1 |
| http://www.yoursite.com/url1 | https://www.example.com | http://www.yoursite.com/url1 |
| https://www.yoursite.com/url1 | http://www.example.com | 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 |
|---|---|---|
| https://www.yoursite.com/url1 | https://www.yoursite.com/url2 | https://www.yoursite.com/url1 |
| https://www.yoursite.com/url1 | http://www.yoursite.com/url2 | NULL |
| https://www.yoursite.com/url1 | http://www.example.com | NULL |
| https://www.yoursite.com/url1 | https://www.example.com | 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 |
|---|---|---|
| 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/ |

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

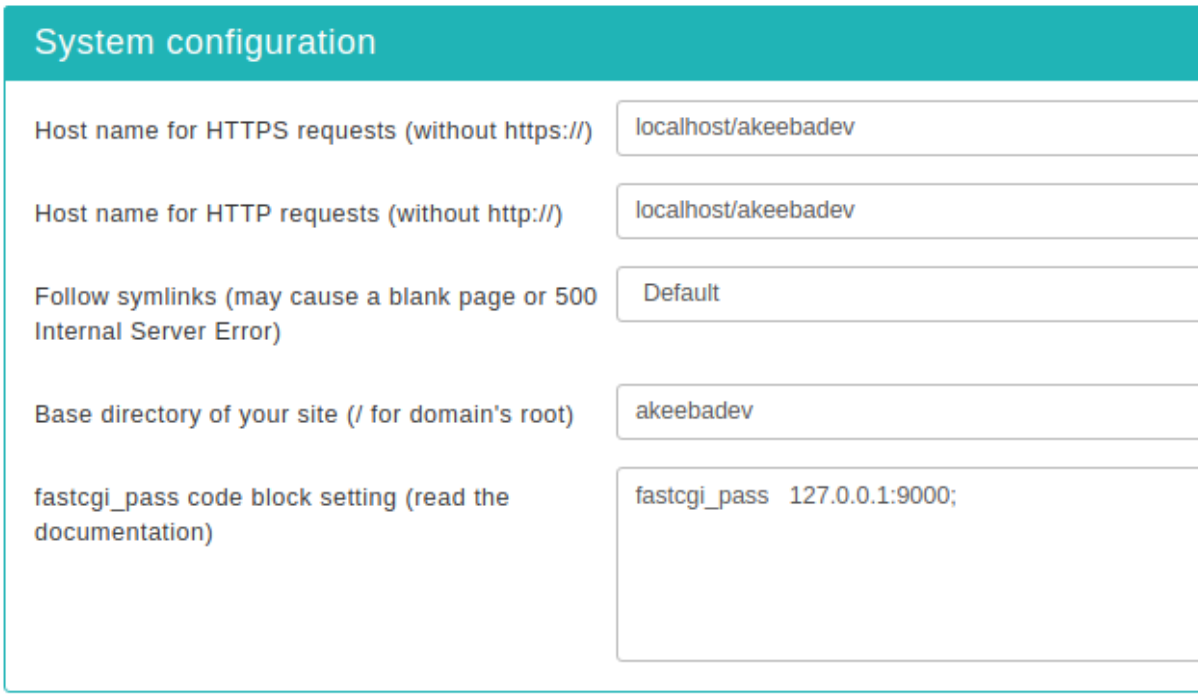
- **unsafe-url** The browser will always send the full URL with any request to any origin.

# 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. Remember to reconfigure and restart your NginX server.

### System configuration




This final section contains all the options which let the NginX Configuration 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 and path to your site. For example, if the address is `https://www.example.com/joomla` then type in `www.example.com/joomla`.

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 and path to your site. For example, if the address to your site's root is `http://www.example.com/joomla` then type in `www.example.com/joomla`.

Follow Symlinks

Joomla! 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 BAD idea. Worse than bad, it's a horrible 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 or Joomla!'s htaccess.txt file.

Base directory of your site

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

fastcgi_pass code block setting (read the documentation)

Please enter the value of the fastcgi_pass code block required by your server setup to execute PHP files, i.e. a fastcg_pass to the listening FastCGI Process Manager of PHP. This is usually `fastcgi_pass 127.0.0.1:9000;` on most servers. If you are not sure ask your host or, if you are your own host, examine the configuration files of NginX. You will probably see a block like this:

```
location ~ .php$ {
    try_files $uri =404;
    fastcgi_pass   127.0.0.1:9000;
    fastcgi_index  index.php;
    include        /Applications/MNPP/conf/nginx/fastcgi_params;
}
```

The value you are looking for is everything between the two curly braces. In the example above:

```
try_files $uri =404;
fastcgi_pass   127.0.0.1:9000;
fastcgi_index  index.php;
include        /Applications/MNPP/conf/nginx/fastcgi_params;
```

## Important

For security reasons the bare minimum you should use is something like:

```
try_files $uri =404;
fastcgi_split_path_info ^(.+\.php)(/.+)$;
fastcgi_pass   127.0.0.1:9000;
```

The first two lines **are extremely important**. They protect you against a well-documented arbitrary code execution vulnerability [https://nealpoole.com/blog/2011/04/setting-up-php-fastcgi-and-nginx-dont-trust-the-tutorials-check-your-configuration/].

# 8. The web.config maker

## Note

This feature is only available in the Professional release

## Warning

This feature is only available on servers running the Microsoft IIS web server. If your server is using Apache or NginX the button to launch this feature will not be shown. If the server type cannot be detected you will see this feature but you should consult with your host whether it will have any effect on your server.

One of the most important aspects of managing a web site hosted on an IIS server is being able to fine-tune your site configuration file, web.config. This file is responsible for many web server level tweaks, such as enabling the use of search engine friendly (SEF) URLs, 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 web.config Maker tool of Admin Tools is designed to help you create the part of such a file used for security and performance optimisation by utilizing a point-and-click interface.

## 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 web.config". This will create a web.config file that's practically the same as the web.config.txt file shipped with Joomla! itself.

## Important

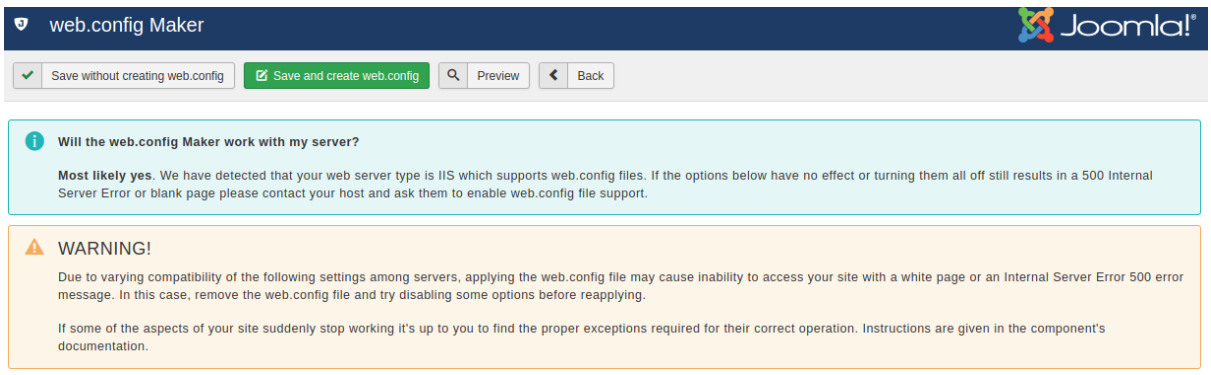
This feature relies on Microsoft's URL Rewrite 2.0 module for Microsoft IIS. This is the same optional IIS module required by the web.config shipped with Joomla! to use SEF URLs without index.php in them. If you cannot use Joomla!'s web.config after renaming the web.config.txt file to web.config then you will NOT be able to use our web.config Maker feature. If this is the case please contact your host and ask them to install and enable the URL Rewrite 2.0 module for IIS.

## Warning

This feature, like Joomla!'s SEF URLs, require IIS 7 or later. If you have an older version of IIS such as IIS 6 you will NOT be able to use this feature. Unfortunately IIS 6 and lower lack the necessary features to create a security tightening web.config file.

The top part of the web.config maker page contains the standard toolbar buttons you'd expect:

### The web.config Maker's toolbar



- Save without creating web.config saves the changes you have made in this page's options without actually creating the customized `web.config` file. This should be used when you have not decided on some options yet, or if you want to preview the generated `web.config` file before writing it to disk.

- Save and create web.config is the logical next step to the previous button. It not only saves the changes you made, but also creates and writes the new `web.config` file to the disk. If you already had a `web.config` file on your site, it will be renamed to `web.config.admintools` before the new file is written to disk.

- Preview pops up a dialog where you can see how the generated `web.config` file will look like without writing it to disk. This dialog shows the saved configuration. If you have modified any settings they will not be reflected in there until you click either of the previous two buttons.

- The Back button takes you back to the Control Panel page.

Below the toolbar there are five panes with different options, described below. Before you do that, please read and understand the following warning. Support requests which indicate that you have not read it will be replied with a link back to this page.

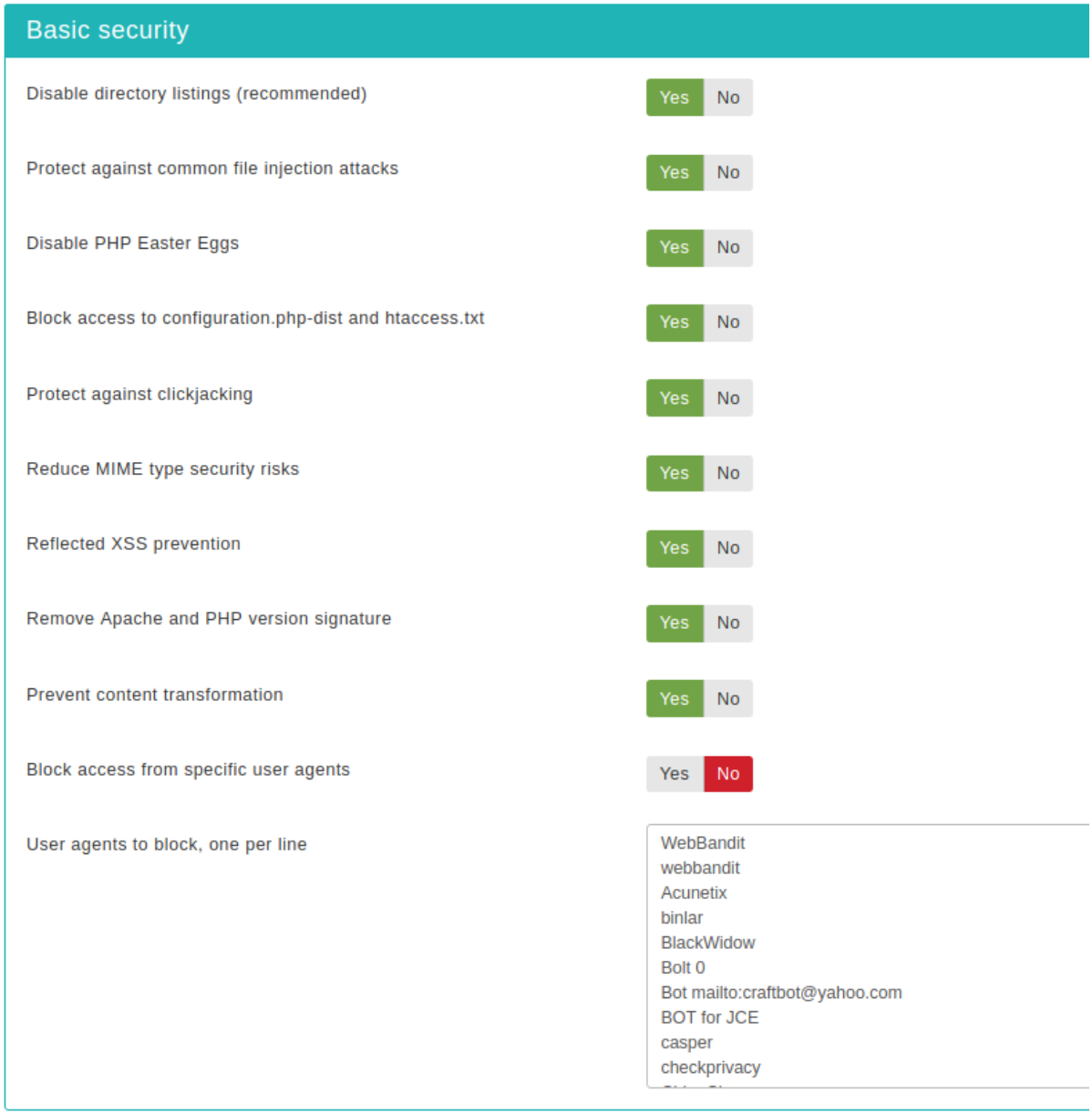
## Warning

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 remove the contents of `web.config` file from your site's root directory using an FTP application or the File Manager feature of your hosting control panel.

We strongly suggest that you begin by setting all options to No and then enable them one by one, creating a new configuration 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. Unfortunately, there is no other way than trial and error to deduce which options may be incompatible with your server.

# 8.1. Basic Security

### Basic security

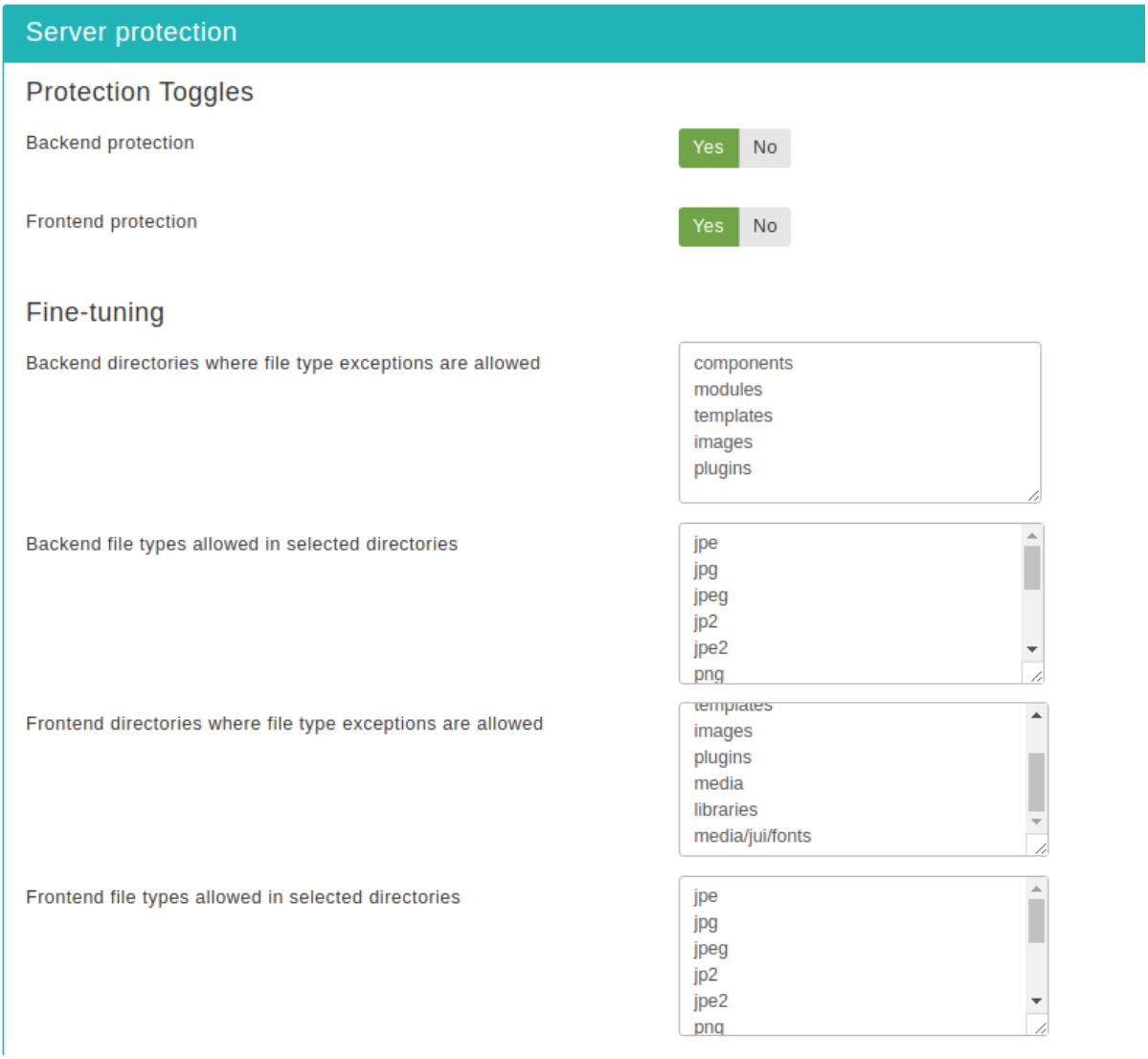



| | |
|---|---|
| Disable directory listings (recommended) | When disabled, your web server might list the files and subdirectories of any directory on your site if there is no index.html file inside it. This can pose a security risk, so you should always enable this option to avoid this from happening. |
| 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 gallery components use them. In this case you are recommended to use the RFIShield (Remote File Inclusion protection) in the Web Application Firewall and turn this web.config Maker option OFF. |
| Disable PHP Easter Eggs | 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.<br><br>Note: You are advised to also set *expose_php* to `Off` in your `php.ini` file to prevent accidental leaks of your PHP version. |
| Block access to configuration.php-dist and htaccess.txt | These two files are left behind after any Joomla! installation or upgrade and can be directly accessed from the web. They are used by attackers to tell the Joomla! version you are using, so that they can tailor an attack targeting your specific Joomla! 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. This option also hides the web.config.txt file included in Joomla! 3 and later for use with the IIS server. |
| 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. |
| 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 Joomla!, it is a server-level protection feature kicking in. Just avoid including the word Wget and you should be out of harm's way. |
| Block common exploits | Enabling this option will include a set of options recommended by Joomla! to protect against (obsolete) common exploits which no longer have any effect on Joomla! 2.5 and later. It's still a good idea to enable this option. |

# 8.2. Server protection

### Server protection




This is the most coveted feature of our software, offering a near-inclusive protection against the vast majority of known threats when enabled. This feature's mission statement can be summed up with a single phrase: nothing executes on your site unless you allowed it to. By blocking access to front-end and back-end 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 INI files, which are usually used by attackers to find out which version of Joomla! you are running on your site to tailor an attack to your site. On the downside, you have to explicitly enable access to some extensions' PHP files which are designed to be called directly from the web and not through Joomla!'s 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, such as RokGZipper. In our humble opinion the security risk of having your site unprotected outweighs the benefits of such solutions by a dramatic factor. As a result, we strongly suggest disabling RokGZipper and other similar software using similarly questionable security practices.

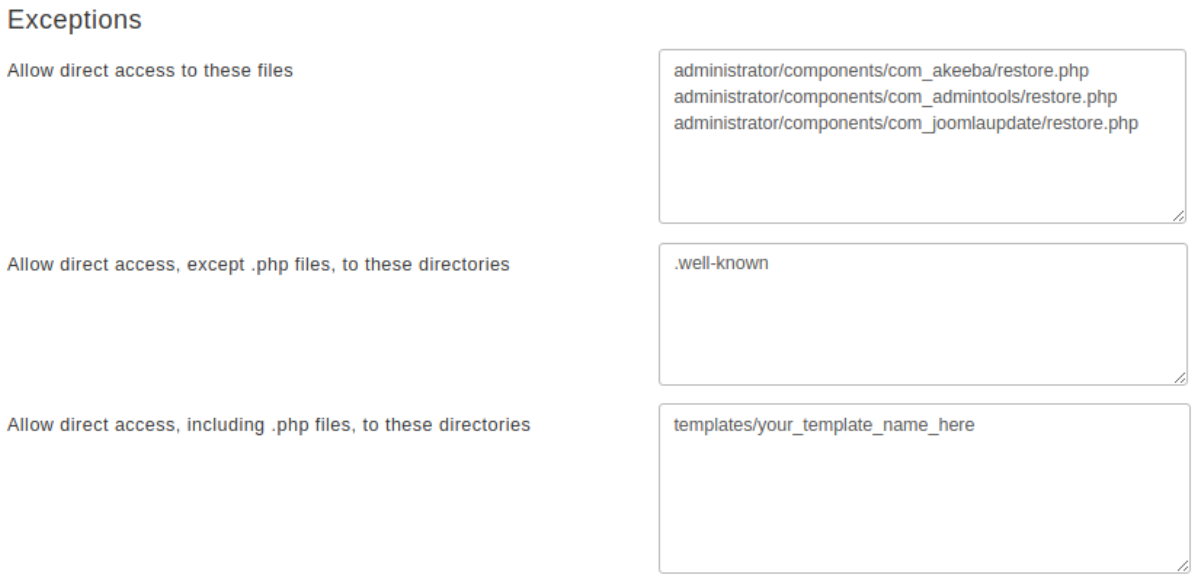
There are three sections of configuration settings controlling the functionality of the Server Protection feature. The first one is the Protection Toggles which allows you to enable or disable the four main aspects of protection:

| | |
|---|---|
| Back-end protection | Disables direct access to most back-end resources, except those in the exceptions lists. It is generally recommended to turn it on to enhance the protection of your site, unless you have enabled the administrator password protection feature. In the latter case this option is redundant and we recommend turning it off. |
| Front-end protection | Disables direct access to most front-end resources, except those in the exceptions lists. It is generally recommended to turn it on to enhance the protection of your site. |

The next section is called Fine-tuning and contains the necessary options to tweak the protection's behaviour to suit your site. Before describing what each option does, a small explanation of how the protection works is in order. The protection code in the generated `web.config` file blocks direct web access to all files. Joomla!'s standard "entry point" or "main" files, `index.php` and `index2.php`, are 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 Joomla! 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.

| | |
|---|---|
| Back-end directories where file type exceptions are allowed | This is a list of back-end directories (that is, subdirectories of your site's administrator directory) where you expect media files to be present. Place one directory on each line. Subdirectories of those directories are automatically added to the exceptions list without having to explicitly list them here. |
| Back-end file types allowed in selected directories | The extensions of back-end files which allowed to pass through the server protection filter, as long as the files with those extensions are in the list above. 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" (without the quotes) 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. |
| Front-end directories where file type exceptions are allowed | This is a list of front-end directories (that is, directories in your site's root) where you expect media files to be present. Place one directory on each line. Subdirectories of those directories are automatically added to the exceptions list without having to explicitly list them here. |
| Front-end file types allowed in selected directories | The extensions of front-end files which allowed to pass through the server protection filter, as long as the files with those extensions are in the list above. 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" (without the quotes) 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. |

## Exceptions




Finally, we have the Exceptions section. 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, some extensions need to directly access PHP files, without passing them through Joomla!'s main files. 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. Other prime examples are CSS and Javscript minifiers, either included in your template or installed on top of your site. Forum attachments are also part of the same problem, as they tend to create a dedicated directory for their attachments, avatar icons and so forth. Moreover, some extensions place PHP files inside your site's `tmp` and `cache` directories and expect them to be directly accessible from the web. While this is a stupid behaviour, contrary to the design goals of Joomla! itself, you still need a way to work around them and we have to provide it. Finally, you may have a third party script (e.g. Coppermine gallery, phpBB forum, WordPress blog, or even another Joomla! site in a subdirectory) which doesn't install as a Joomla! extension. 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:

Allow direct access to these files
: Place one file per line which should be exempt from filtering, therefore accessible directly from the web. The default settings include Akeeba Backup Professional and, of course, Admin Tools itself.

Allow direct access, except .php files, to these directories
: Direct access to all files (except for .php files) will be granted if they are inside any of the directories in this list. Normally you should only need to add your forum's attachments, avatars and image galleries directories, or other directories where you only intend to store media files. The example is Agora forum's user files directory. As with all similar options, add one directory per line, without a trailing slash.

Allow direct access, including .php files, to these directories
: 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 Joomla!, WordPress, phpBB, Coppermine gallery 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 templates and template frameworks may wrap their CSS and Javscript 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 extensions do something silly: they place files inside your site's `tmp` or `cache` directories and expect them to be directly accessible from the web. This is plain wrong because these directories are designed to be protected system directories where direct access should not be allowed, most notably because they might contain sensitive information. However, if you have such extensions —most notably certain Javascript and CSS minifiers— you need a way to allow direct access to those directories.

  If you decide that convenience is better than security we can't stop you. Add tmp and cache to this list and wish for the best. You are opening a security hole on your site and you do it at your own risk and potential peril.

While it might seem very tempting to put several Joomla! system directories in here, like components and templates, don't. That's right. Do not do that. It is like using a tactical weapon to kill a mosquito in the same room as you. The mosquito will hardly ever survive, but you will go down with it. Or, in computing terms, you allow potential hackers to use any security vulnerabilities you haven't had the chance to fix yet in order to upload and *execute* malicious code. You killed the mosquito (the access problems you had with an extension) but you accidentally helped to take down your site. Ouch! Even if the chance of this happening is about one in ten thousand, are you willing to take that risk *on your own site*?

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

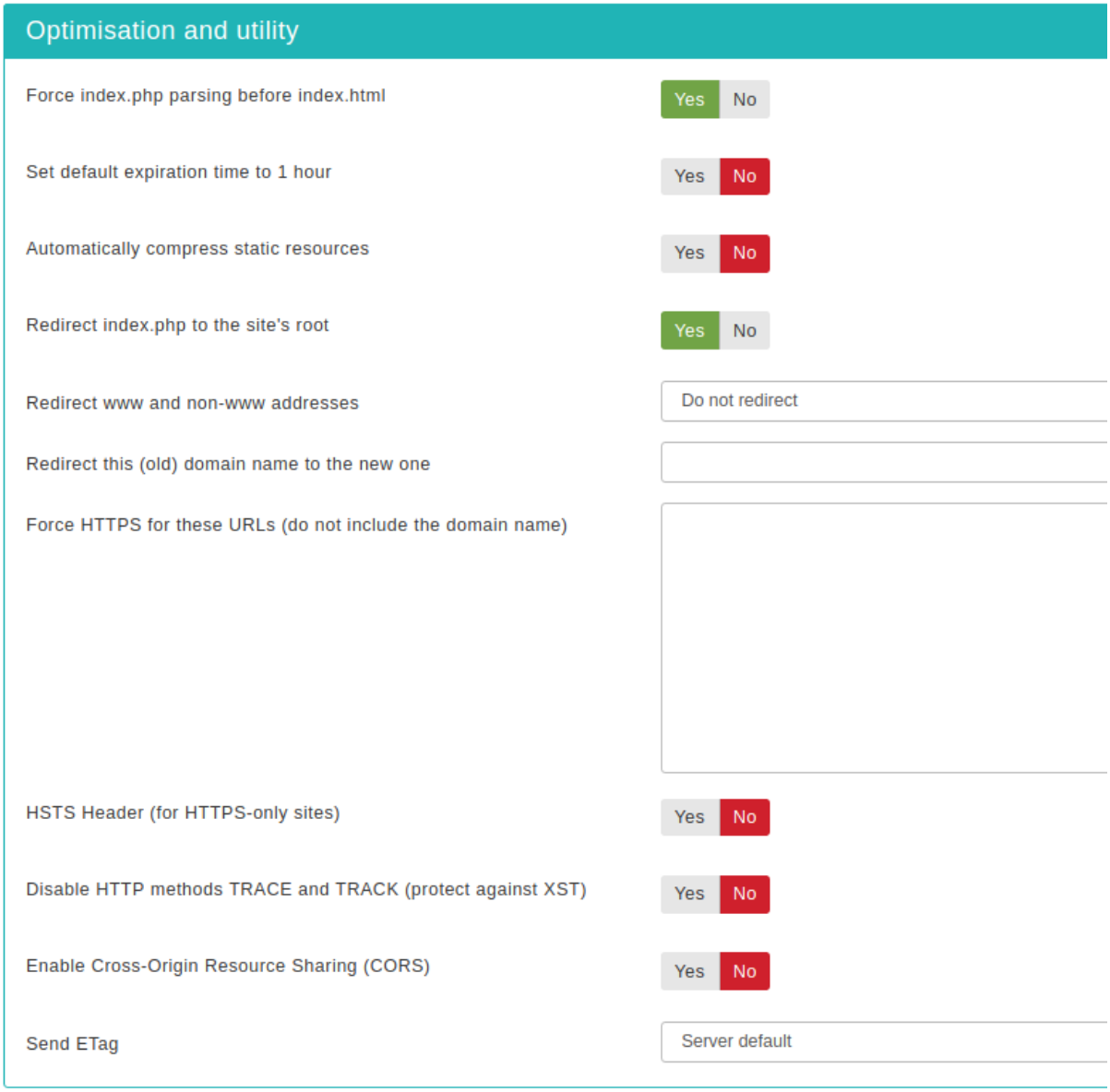
Windows users beware! *Do not* use Windows' path separator (the backslash - \) to separate directories! We are talking about directories as they appear in URLs, so you should always use the URL path separator (forward slash - /) in those settings. In other words `some/long/path` is correct, `some\long\path`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

## 8.2.1. How to determine which exceptions are required

Please refer to the section on determining exceptions under the .htaccess Maker documentation. The exact same process applies. The only difference is that you enter the exceptions in the web.config Maker instead of the .htaccess Maker.

# 8.3. Optimisation and utility

### Optimisation and utility




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 Joomla! 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. Note: some files types have a higher expiration time of 1 week or 1 month.

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. We do add a directive which instructs NginX to not compress the output when accessed by IE6 but all bets are off with a browser that hasn't been updated for over a decade...

Redirect www and non-www adresses

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 on 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, as we did migrating from joomlapack.net to akeebabackup.com. 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, sending to the darkest hole of search engine results. Not good! 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:

```
joomlapack.net, www.joomlapack.net
```

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

HSTS Header (for HTTP-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. Joomla! offers a Global Configuration setting to force SSL throughout the entire site, but this is merely a workaround: if it sees a request coming through HTTP it will forward it to HTTPS. There are two privacy implications for your users:

- If you have not enabled the SSL option in Global Configuration a man-in-the-middle attack known as "SSL Stripping" is possible. 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 Joomla! forwards your user to HTTPS 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 an 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]. |
| 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. |
| 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 it 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 | 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).<br><br>This is a commonly used method used by attackers to compromise web sites, especially when a zero-day XSS vulnerability is discovered in popular Joomla! extensions or Joomla! 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.<br><br>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 Javscript 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!<br><br>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]. |
| 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]

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.
- **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!

## Note

The lack of other options is intentional and has to do with an IIS limitation. IIS, unlike Apache, only offers a binary switch for ETags: you either send them or you don't.

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>` elelements.

- **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 |
|---|---|---|
| https://www.yoursite.com/url1 | http://www.yoursite.com/url2 | NULL |
| https://www.yoursite.com/url1 | https://www.yoursite.com/url2 | https://www.yoursite.com/url1 |
| http://www.yoursite.com/url1 | http://www.yoursite.com/url2 | http://www.yoursite.com/url1 |
| http://www.yoursite.com/url1 | http://www.example.com | http://www.yoursite.com/url1 |
| http://www.yoursite.com/url1 | https://www.example.com | http://www.yoursite.com/url1 |
| https://www.yoursite.com/url1 | http://www.example.com | 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 |
|---|---|---|
| https://www.yoursite.com/url1 | https://www.yoursite.com/url2 | https://www.yoursite.com/url1 |
| https://www.yoursite.com/url1 | http://www.yoursite.com/url2 | NULL |
| https://www.yoursite.com/url1 | http://www.example.com | NULL |
| https://www.yoursite.com/url1 | https://www.example.com | 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 |
|---|---|---|
| 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/ |

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

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

# 8.4. 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.

### System Configuration


This final section contains all the options which let the NginX Configuration 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 and path to your site. For example, if the address is `https://www.example.com/joomla` then type in `www.example.com/joomla`.

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 and path to your site. For example, if the address to your site's root is `http://www.example.com/joomla` then type in `www.example.com/joomla`.

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

# 9. Web Application Firewall

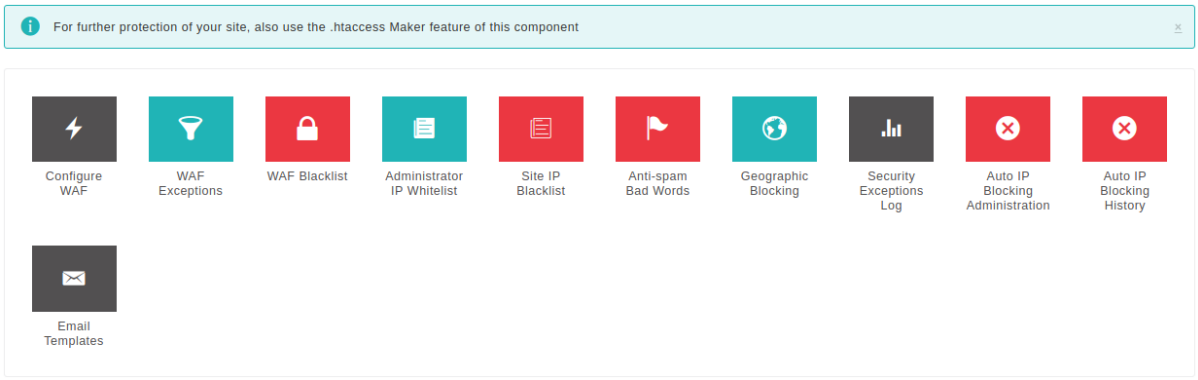
## Note

This feature is 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 fingerprinting attacks, used by attackers to deduce information about your site in order to tailor an attack to it, and the most common attacks. The real-time protection is performed by the "System - Admin Tools" plugin (`plg_admintools`). Before configuring Admin Tools' WAF you have to make sure that the plugin is published and it's the first to run, i.e. it should appear first in the ordering menu. These conditions are automatically applied when you install the Admin Tools bundle. However, if you have installed more system plugins make sure that plg_admintools is published before all other system plugins. If not, the protection offered will not be thorough.

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

### The Web Application Firewall page




Clicking on any icon will launch the respective sub-tool. The Back button on the upper right-hand corner will get you back to the Control Panel page.

# 9.1. Configure

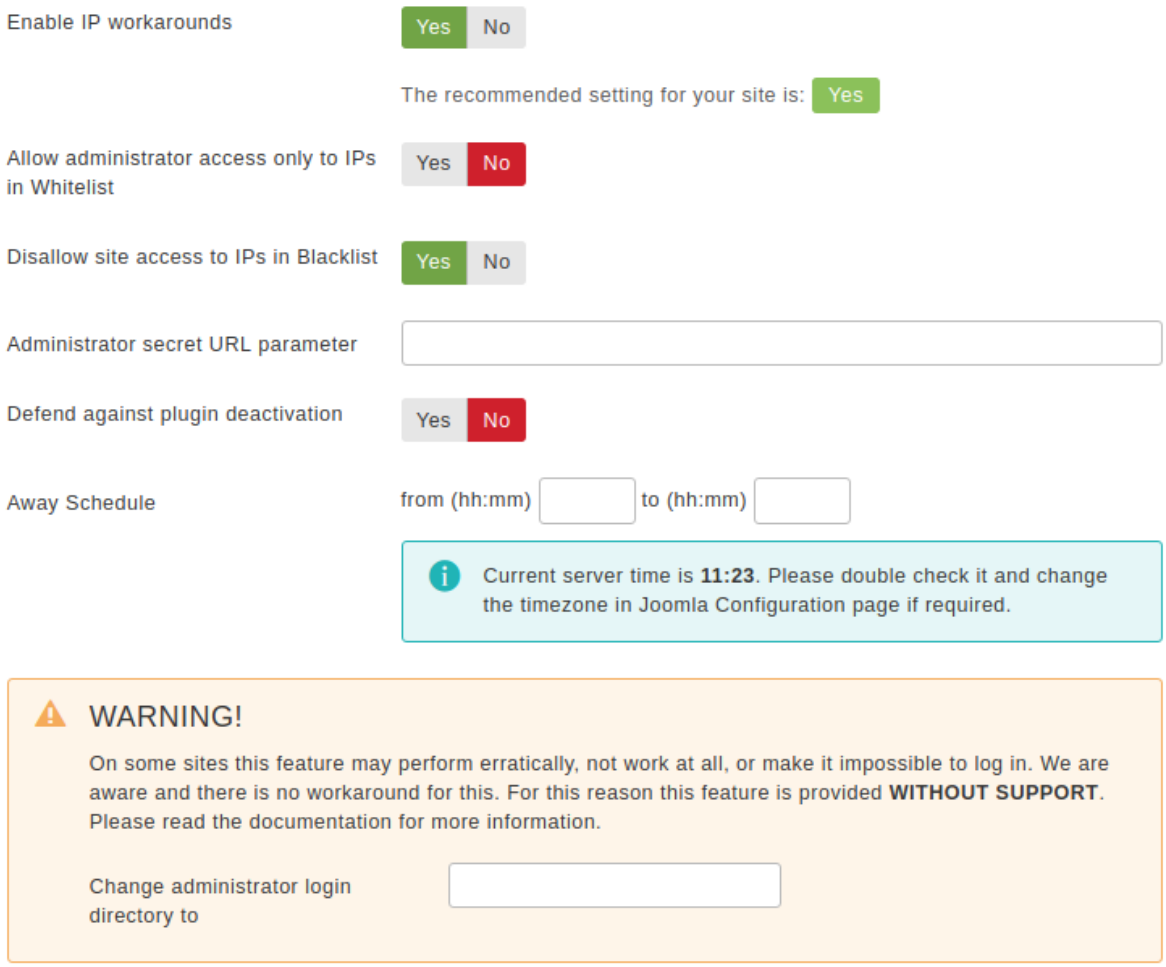
This sub-tool is where all the configuration fine-tuning of the firewall takes place. By default, none of these options are enabled during installation. You will have to enable them manually. Once you are content with your options click on Save to save the changes and return to the WAF panel page, or 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 section 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.

## 9.1.1. Basic Features

### WAF: Basic Features




The Basic 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.

Administrator secret URL parameter

Normally, you can access your site's administrator area using a URL similar to `http://www.example.com/administrator`. 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 an administrator area exists to deduce that your site is running Joomla! and attack it. By entering a word here, you are required to include it 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 with `http://www.example.com/administrator?test` due to their configuration. You may want to try using `http://www.example.com/administrator/?test` (add a slash right before the question mark) or `http://www.example.com/administrator/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 one (`http://www.example.com/administrator?test`) works on 95% of servers and that's what we recommend trying out first.

Defend against plugin deactivation

When enabled, Admin Tools will prevent back-end users from trying to disable (unpublish) the plugin. This means that you will also be unable to unpublish the plugin until you disable this option!

Change administrator login directory to

THIS FEATURE IS PROVIDED WITHOUT SUPPORT. We had completely removed this feature in version 3.5.0. It was only restored at the insistence of some clients. Since we cannot guarantee its correct operation, we offer no support for it. Please note that many servers are severely misconfigured and will not process the redirection to /administrator correctly. This may cause this feature to perform erratically or even prevent you from logging in to your site. Use at your own risk and keep in mind that NO SUPPORT will be provided for it. We recommend using Administrator Directory Password Protection instead. It's more secure and doesn't cause the problems the "Change administrator login directory" feature does.

As explained in the option above, you can normally access your site's administrator area using a URL similar to `http://www.example.com/administrator` 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 `foobar` 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/administrator` 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/foobar` they will see the administrator login page.

A few important notices regarding this feature:

- It REQUIRES Search Engine Friendly URLs and Use URL Rewriting to be set to `Yes` in your Joomla! Global Configuration page.
- You MUST NOT have any menu item with an alias which is the same as this option. If you do you will lose access to that menu item from the front-end of your site.
- This setting works by setting a session variable. After the first time you visit the cloaked login URL (e.g. `http://www.example.com/foobar`) you will then be able to access the regular administrator URL (`http://www.example.com/administrator`) until your back-end session expires. Session expiration is controlled by the Session Lifetime value you have set in your Joomla! Global Configuration page. This behaviour is not a bug, it is how it is intended to function.
- By using this option you are NOT renaming the administrator directory. Doing so is not supported by Joomla! and its extensions and would lead to grave issues with 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 indeed!
- You CAN combine it with the Administrator secret URL parameter feature. In this case you need to access the login page as `http://www.example.com/foobar?test` where

"foobar" 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, we suggest that you enable all three administrator login protection features on your site: password-protect administrator, secret URL parameter and change administrator login directory. Combined with two-factor authentication (either Admin Tools' or the one shipped with Joomla! 3.2) you will have a quintuple protection before anyone can access your administrator area. That's paranoia level protection.

Away Schedule

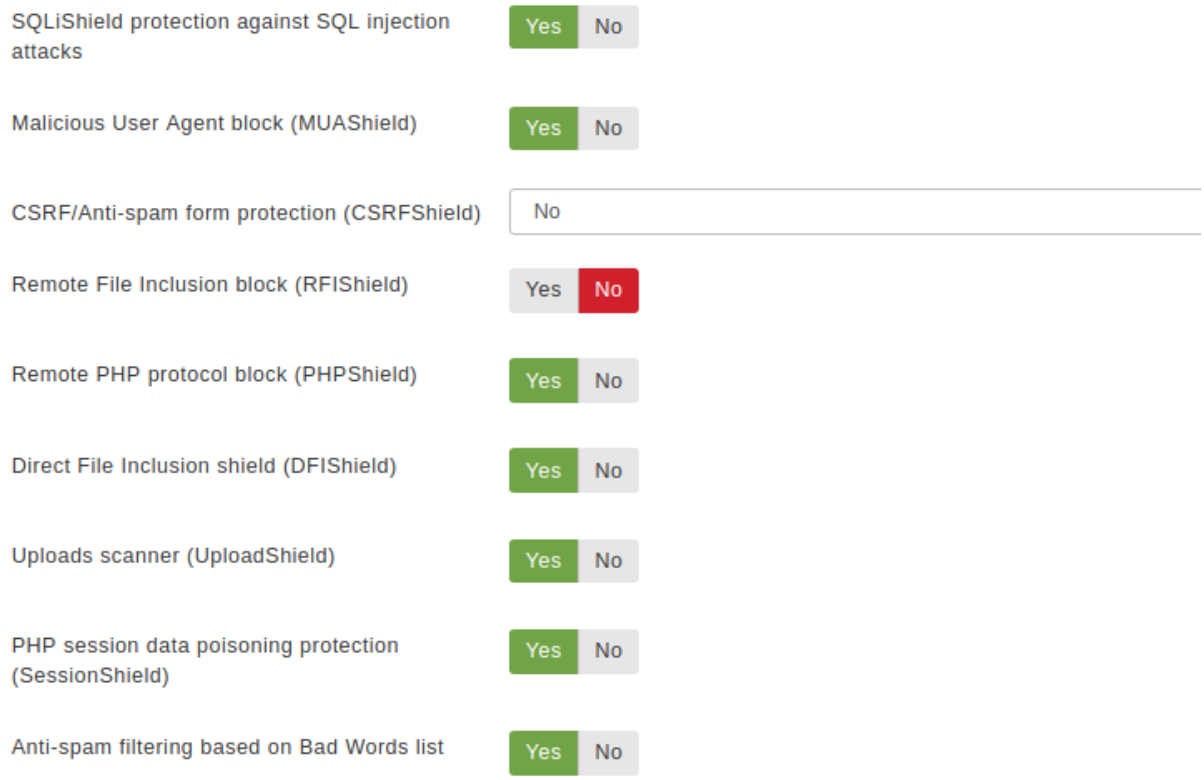
By default, Joomla! allows users with back-end access to log in to the site any time of the day. On smaller sites which have only a handful, or even just one, administrators on the same zone this means that someone can try to log in with a stolen username / password while you are fast asleep and unable to respond to the unexpected login. This where the Away Schedule comes into play. If a user with back-end login privileges tries to log in to the front- or back-end of your sute between the "from" and "to" hour of the day they will be denied login. Moreover, if someone tries to access the administrator login page during that time they will be redirected to the front-end 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 belonging to a group with the *Admin Login* privilege. You can check which groups have that privilege by clicking on the System, Global Configuration menu of your site and visiting the Permissions tab.

The From and To time has to 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.

## 9.1.2. Request Filtering

### WAF: Request Filtering




The Request Filtering section contains the options which are the heart and soul of the Web Application Firewall. Admin Tools will monitor incoming requests and their variables, 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.

But what is a SQLi attack? A few Joomla extension developers are hobbyists, without experience and / or security training; or mistakes do happen, as Joomla itself has found out the hard way. 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 Super 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.

Malicious User Agent block (MUAShield)

Many hackers will try to access your site using a browser configured to send malicious PHP code in its user agent string (a small piece of text used to describe the browser to your server). The idea is that buggy log processing software will parse it and allow the hacker to gain control of your website. When enabled, this feature allows Admin Tools to detect such attacks and block the request.

CSRF/Anti-spam form protection (CSRFShield)

One of the major concerns regarding web forms –like login forms, contact forms, etc– is that they can be exploited by automated scripts (bots). This is usually performed to send spam messages or brute-force passwords. Admin Tools has two methods to prevent such abuse, depending on the setting of this option:

- `No`. Turns off this feature.
- `Basic`. Performs basic referer filtering. If the browser of the visitor reports that the previous page was not one belonging to your site, Admin Tools will block processing of the form. This is enough to thwart script kiddies and unsophisticated spam bots, but will do nothing for more serious attacks.
- `Advanced`. On top of the basic protection, Admin Tools will automatically inject a hidden field on all forms. Spambots will usually try to fill all fields on a form, including the hidden one. WHen this happens, Admin Tools will block the request. This is a better method, but it's much slower and not recommended for high-traffic (several dozen of thousands of visitors per day) websites.

## Warning

If you expect external sites to be performing POST requests to your site, e.g. PayPal posting back IPN notifications, please DISABLE this feature or use the WAF Exceptions to work around it, otherwise all such requests will be marked as security exceptions. Alternatively, if you expect such requests to come only from specific IP addresses (e.g. PayPal), then please add these IPs in the Never block this IPs whitelist.

Remote File Inclusion block (RFIShield)

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.

## 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.

Remote PHP protocol block (PHPShield)

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)

Some hackers try to trick vulnerable components into loading arbitrary files. Depending on the vulnerable component, the file will either be output verbatim or parsed as a PHP file. This allows attackers to disclose sensitive information about your site or run malicious code uploaded to your site through another vulnerable vector, e.g. an unfiltered upload of executable PHP code. 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.

## Important

This feature does NOT prevent dumping of non-PHP files, e.g. the `/etc/passwd` file of Linux servers.

Uploads scanner (UploadShield)

When this option is enabled, Admin Tools will proactively scan all files which are uploaded through Joomla!. If any of these files is found to contain even a single line of 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 COMPONENTS ALLOW ADMIN TOOLS TO SCAN THEIR UPLOADS**! Some components do not use Joomla!'s index.php entry point file. Instead, they use their own. Since these uploads do not pass through the Joomla! application, Admin Tools' code doesn't run and these uploaded files are not scanned. In this case, if that component is found vulnerable, your site will still be at risk. We suggest avoiding such components. How can you tell? It's simple. If you use the front-end protection feature of .htaccess / NginX Configuration Maker and you had to add an exception for a component, it doesn't use Joomla!'s index.php and is potentially vulnerable to this kind of code upload attacks.

## Note

As of Joomla! 3.4.1, our UploadShield code is included in Joomla! itself and is always enabled. As a result we recommend that our clients keep this feature turned off on Joomla! 3.4.1 and later.

PHP session data poisoning protection (SessionShield)

Prevents malicious input data which can be used to trick PHP's internal session handler into executing arbitrary code when it's restoring the user session.

The PHP session unserializer has a major bug which makes it misinterpret stored session data if they contain specific character combinations, overwriting the legitimate session data with the attacker-defined contents. Combined with some other features of PHP this can lead to the execution of arbitrary PHP code. **In short, attackers can send malicious data in one page load and get arbitrary code to execute in the next page load**. This feature of Admin Tools detects and blocks this kind of malicious data. CAUTION: It may block some legitimate requests as well.

## Warning

This attack vector is NOT unique to Joomla!. It is a low level PHP bug / vulnerability which was fixed only in PHP 5.5.4 and later versions. Furthermore, default PHP settings even in newer versions of PHP use the old, vulnerable setting, putting all sites using session data at risk! We **VERY STRONGLY** recommend that all our clients use PHP 5.5.4 or later and edit their php.ini to modify this line:

```
session.serialize_handler = php
```

to

```
session.serialize_handler = php_serialize
```

This is the ONLY guaranteed way to fix this low level PHP vulnerability across all possible attack vectors, including those yet undiscovered.

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.

| | |
|---|---|
| Disable creating / editing backend users from the frontend | Yes / No |
| Monitor Global Configuration | Yes / No |
| Monitor component configuration | Yes / No |
| Action for configuration monitoring | Email |
| Monitor Critical Files | Yes / No |
| Monitor these files for changes | test.txt |
| Monitor Super User accounts | Yes / No |
| Disable Joomla!'s Two-Factor Authentication on password reset | Yes / No |
| Forbid frontend Super Administrator login | Yes / No |
| Treat failed logins as security exceptions | Yes / No |
| Deactivate user after | 0 failed logins in 1 da |
| Warn about self XSS | Yes / No |
| Filter user registration by email | Allow / Block |
| Email domains | |

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

Warn about use of well-known passwords

When this option is enabled, Admin Tools will connect to the Have I Been Pwned database [https://haveibeenpwned.com/API/v2#PwnedPasswords] and check if the hash of the current password is known. If a match is found, the user will be blocked from using an insecure password.

## Wait, are you sharing my password? Is that service secure?

First of all, **we do not share your password**. We're only sending *a fraction* (only first 5 chars) of the *hash* of your password. This method is called k-anonymity [https://en.wikipedia.org/wiki/K-anonymity] and it's a very secure way to share sensitive date anonymously. So, don't worry, your password is secure, if you want to read the whole details of this implementation, you can take a look at this page [https://www.troyhunt.com/ive-just-launched-pwned-passwords-version-2/].

Regarding the external service, it is powered by two well known figures: Troy Hunt (a security research) and CloudFlare (leader in Content Deliver System services).

User groups to check for well-known passwords

Most likely you want to enable this feature only for specific groups: Admin Tools will check for well-known passwords only users belonging to those groups (default to Super Users)

Disable editing backend users' properties

When enabled, trying to modify the settings of an existing or create a new Manager, Administrator or Super User will fail.

Disable creating / editing backend users from the frontend

You should normally be unable to create a new user with administrative backend login privileges from the public frontend. When this option is enabled it will treat attempts to create this kind of accounts as hacking attempts and block them from executing. This addresses some of the most notorious zero day attacks in Joomla! which took place between 2015 and 2016 and we recommend having it turned on at all times. If you need to disable it we STRONGLY recommend rethinking whatever leads you to disable this setting because it's creating a gaping security hole on your site.

Monitor Global Configuration

When this is enabled and someone tries to change the Global Configuration of Joomla!, either from the back-end or the front-end, you will either be notified or they will get blocked (depending on your settings below). This feature is designed to protect you against sly hackers or malicious administrators who subtly change your site's configuration for nefarious purposes, e.g. by elevating the global privileges of user groups.

Monitor component configuration

When this is enabled and someone tries to change the configuration of any core Joomla! or third party component (what you see when you click Options in a component's toolbar) from the back-end of your site you will either be notified or they will get blocked (depending on your settings below). This feature is designed to protect you against sly hackers or malicious administrators who subtly change your components' configuration for nefarious purposes, e.g. by elevating the privileges of user groups with regards to a particular component.

Action for configuration monitoring

This option works in conjunction with the two above. You define what do you want to do when either global or component configuration is enabled and a change is detected in the configuration.

- *Email* will simply send a warning email to the email addresses you've configured to receive security exception emails and only if you have configured such email addresses. The changes in configuration will go through. This is the recommended setting for most sites.
- *Block* will treat any such changes as security exceptions. The changes in configuration will NOT go through. This setting should only be used on "locked down" sites where

configuration changes are not expected (or will only be performed by an administrator who has adequate access to modify Admin Tools' configuration).

Monitor Critical Files

Critical files commonly modified by hackers (index.php, administrator/index.php and the index.php, error.php and component.php of all templates installed on the site) will be monitored for changes on every page load. If a change is detected you will be notified by email. This usually lets you get an ahead warning in case of a successful hacking attempt.

Monitor these files for changes

Monitor the following files (one per line) for changes. If a change is detected you will be notified by email.

Monitor Super User accounts

Admin Tools will keep track of the user accounts with Super User access. If a new Super User is added outside of Joomla's Users page you will be notified by email. Moreover, the detected new Super User accounts will be automatically blocked. The idea is that these Super Users are most likely create as the result of a hack or rogue code.

Please note that users created or added by other Super Users in the backend of the site using Joomla's Users page will NOT be blocked by this feature. If you wish to disable this please use the Disable editing backend users' properties feature.

Disable Joomla!'s Two-Factor Authentication on password reset

When enabled, Admin Tools will disable the Joomla! Two Factor Authentication configuration for a user when they are resetting their password.

Joomla! 3.2 or later allows every user of the site to enable Two Factor Authentication (TFA) for their user account. In case the user misplace their TFA device or is otherwise unable to use TFA they are given emergency one time passwords. However, many people forget to note them down or do not understand how to use them. Every time they cannot use TFA they have to contact an administrator of the site to disable TFA on their account. Even worse, when the user is an Administrator themselves they have no way to disable TFA without renaming files – and knowing which files to rename. This is where this Admin Tools feature comes in handy.

The workflow is the following: The locked out user starts by using the "Forgot your password?" link in Joomla! to request a password reset. The receive an email with instructions. They follow the link which takes them back to the site where they enter their username and the password reset authorisation code found in the email. Now they enter their new password. When the password changes, the "Disable Joomla!'s Two-Factor Authentication on password reset" feature of Admin Tools kicks in and disables Two Factor Authentication on this user's account. The user can now log in to the site using just their username and password.

## Important

Please remember that this only applies to the two factor authentication feature built in Joomla! 3.2 or later.

Forbid front-end Super Administrator login

When enabled, it will not be possible for Super Administrators to log in to your site's front-end. This is a security precaution against password brute forcing. One common method is an attacker trying to login to the front-end of your site as a Super Administrator, trying different password until he finds the correct one. When this option is enabled, he will not be able to log in as a Super Administrator in the front-end of the site, crippling this brute forcing method of determining the Super Administrator password.

Treat failed logins as security exceptions

When enabled, failed login attempts of any kind of user (even simple registered 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.

Deactivate user after

Admin Tools can optionally deactivate existing user accounts when there are multiple failed attempts to log in using their username, protecting user accounts from brute force attacks.

In here you can specify the number of failed logins and the time period these have to occur before the user is deactivated, e.g. 3 failed logins in 1 minute.

In order for this feature to work you must have enabled the Treat failed logins as security exceptions option above and NOT include `Login failure` in the Do not log these reasons option in the Logging And Reporting area of this configuration page.

The behaviour of this feature depends on the user registration setup of your site, as defined in Users, User Manager, Options in your site's back-end. When Allow User Registration is set to `No` this Admin Tools feature does not do anything at all! When Allow User Registration is set to `Yes` there are three possible behaviours depending on the setting of the New User Account Activation option:

- `Self`: The user is deactivated and an activation email is sent to them by Admin Tools using the `User re-activation` email template.
- `Admin`: The user is deactivated and an activation email is sent to all of your site's Super Users by Admin Tools using the `User re-activation` email template.
- `None`: This Admin Tools feature does absolutely nothing at all. The user is not deactivated.

Warn about self XSS

Display a message in browser console to warn the user to avoid running any command inside it. This can lead to hacking yourself (a.k.a. Self XSS attacks [https://en.wikipedia.org/wiki/Self-XSS]) and steal your account data.

Filter user registration by email

Admin Tools can block user registration based on the email domain they are using (listed in the field below):

- **Allow** Will allow registration only if the email domain is contained inside the list. A typical use case is to allow registration only from site company addresses or student of a campus
- **Block** Registration will be blocked if the user tries to use a domain contain in the list. This is usually useful if you want to block people from using temporary or disposable email accounts.

Email domains

Enter one domain for each line, leave empty to disable the filter during user registration

Below that you will find the Forgotten backend users section. This feature lets you automatically block or force a password reset for users with backend access who have not logged into the site for a very long time. This feature was inspired by a tweet by Jeff Atwood [https://twitter.com/codinghorror/status/1084583084035661826?s=21] (of DIscourse fame) and our observations by logging into real world sites when our clients request us to do so.

The idea is that privileged user accounts who have not logged into the site for a very long time are probably left over user accounts the site owner forgot to disable when the person stopped having a reason to log into the site's administrator backend. The password of the forgotten user account may have been compromised in the meantime. For example, the user may have reused their password on a different site which got hacked; or they may had used an easy to guess password. If Two Factor Authentication isn't enabled on the account, an attacker who has successfully compromised the password could now log into your site. Since they are using a legitimate user account they do not trigger a security exception and they have full access to your site with everything that entails about your site's integrity.

This Admin Tools feature is designed to prevent this kind of awkward situation. If a user with backend access has not logged in for the configured time period (default: 90 days) they will either be completely blocked from accessing the site or they will be forced to reset their password (default and recommended action). In the first case only another Super User can unblock them, by editing their user account. In the latter case the user will try to log in and Joomla! will immediately force them to reset their password. Password reset requires providing information sent by email. This way an attacker cannot use a compromised password; they cannot read the email sent to the legitimate account holder's email address, therefore they cannot reset the password and log into your site.

For even better protection of your site we recommend that you take two more optional steps. Make sure that all privileged users have Two Factor Authentication set up on their user account. Joomla has Two Factor

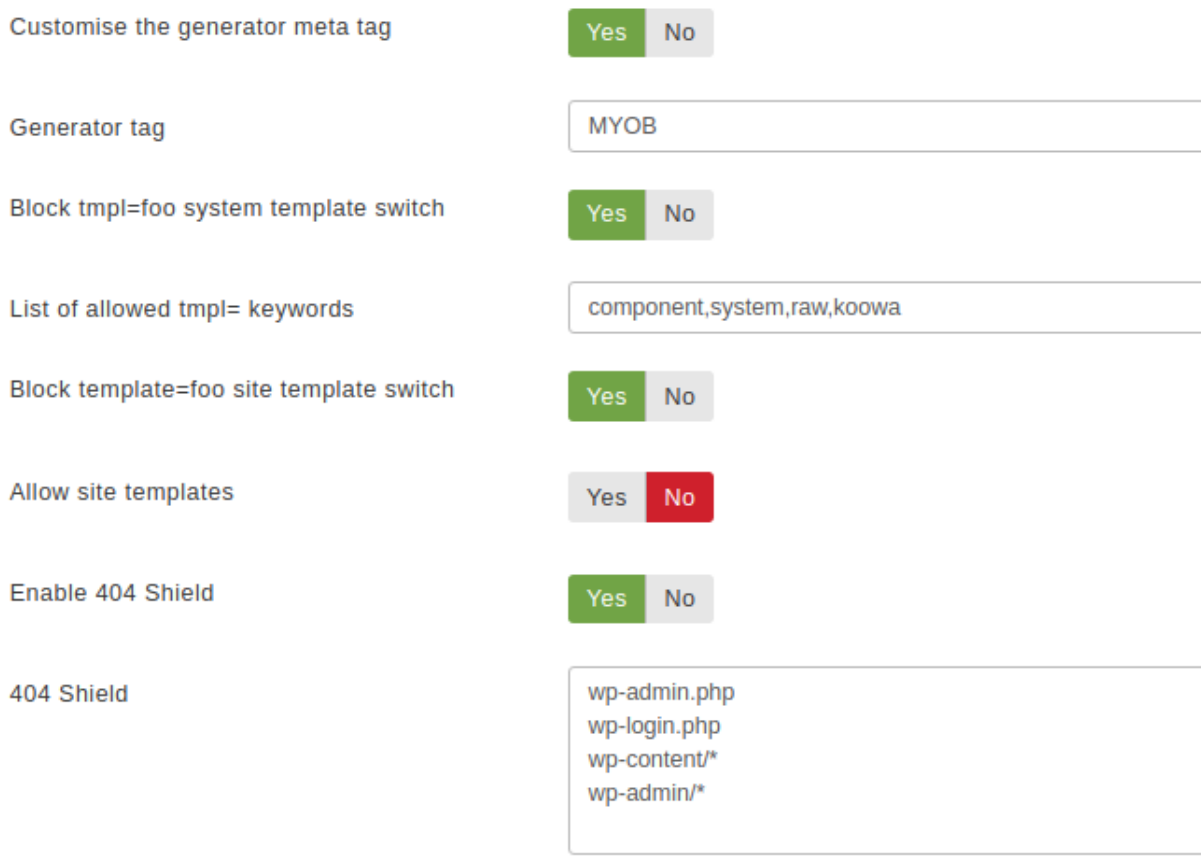
Authentication built in. Alternatively, you can use our more thorough, free of charge Akeeba LoginGuard extension to provide Two Step Verification (it also lets you force certain user groups to enable it). Moreover, it is recommended to have inactive user accounts automatically deleted. This can be done, for example, with our free of charge Akeeba DataCompliance component for Joomla! (however, it will not delete Super User accounts by default to prevent any accidents -- deletion through Akeeba DataCompliance is irreversible by design as it implements the GDPR requirements of Data Minimization and the Right To Be Forgotten).

The following options are available for this feature:

| | |
|---|---|
| Prevent forgotten backend users from logging in | Should this feature be enabled at all? |
| Check every [minutes] | For performance reasons, this feature only runs periodically, checking which backend user accounts are inactive and disabling / forcing a password reset on them. Here you can define how often it will run. The default is 60 minutes which means that it will run *at most* once every 60 minutes. Other useful values are 1440 (at most once a day) and 10080 (at most once a week). |
| Backend user groups | Which user groups this feature should apply to? We recommend choosing at the very least the Administrator and Super User groups. If you have other user groups with backend login we recommend you add them as well.<br><br>If you do not specify any groups, or choose the "Show All Groups" option, Admin Tools will consider users from all user groups which have the Admin Login privilege, as set up in the Global Configuration of your site.<br><br>Even though you can select user groups without backend access they are NOT taken into account. The user groups list is rendered by Joomla! and it does not provide a way to remove user groups which lack backend access. |
| Maximum number of days since last login | Users who have not logged into the site for *at least* this many days will be blocked or forced to reset their password. The default is 90 days (three months). Reasonable values are between 30 and 365 days. If you set this to 0 or leave this blank the feature will effectively be disabled. |
| Login prevention method | What should Admin Tools do with the user accounts which have not logged in for a long time?<br><br>Block means that the user will be completely blocked from accessing the site. This is implemented by setting the Block User to Yes. The blocked users cannot unblock themselves. A Super User will have to do that by editing the user from the Joomla backend Users, Manage menu item.<br><br>Force Password Reset is the recommended and selected by default method. In this case the user account is allowed to log in but they will have to immediately reset their password and log back in before they can do anything on the site. The password reset takes place through Joomla's built in password reset method. It is NOT handled by Admin Tools. |
| Protected users | Any users you select here are not going to be prevented from logging into the site. We recommend that you add the site owner here. Moreover, if you are building a site for a client, you should add your user account as well. This will let you log into the site to provide technical assistant should your client require it.<br><br>It is worth noting that if Login prevention method is set to Block and Protected Users is empty Admin Tools will NOT block ANY Super Users, even if they haven't logged in for a time period longer than the specified maximum number of days. This is a precaution against losing all access to the site by accident (if all Super Users get blocked then nobody is left to unblock you). If you have a site with multiple Super Users and use the Block method you MUST specify at least one Protected User for Admin Tools to provide a sensible level of protection against forgotten user accounts. |

## 9.1.4. Cloaking

### WAF: Cloaking




The next section is called Cloaking and contains options to allow you to modify the way several features in Joomla! which are frequently exploited by attackers to locate Joomla! sites work. The idea is that potential attackers use automated tools to scan thousands of sites, trying to identify which of them run Joomla! in order to attack them. Using these options will allow you to "cloak" your site against such fingerprinting (scanning) attacks.

Hide/customise generator meta tag
: All Joomla! 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 Joomla!. This information is cached by search engines and is exploited by attackers to deduce that your site is running Joomla! when looking for potential targets. Disabling the generator tag normally requires modifying Joomla! core files. Instead, you can enable this option and enter a custom value for the generator tag in the next option. Be inventive! Use something silly, like "A million monkeys with typewriters" or cloud the water by assigning the name of another CMS, like "Drupal" or "WordPress".

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

Block tmpl=foo system template switch
: One of the lesser known Joomla! features are its system templates. Whenever an error occurs or you put your site offline, Joomla! loads the respective system template. Passing the name of the template in the URL by appending, say, `?tmpl=offline` allows you to test those templates without having to actually produce an error or put your site off-line. Do note that tmpl=system and tmpl=component must be permitted (see next option), as they are required by some extensions to work.

List of allowed tmpl= keywords
: The list of tmpl keywords which should be allowed of your site, as a comma separated list. At the very least you MUST include system and component, otherwise Joomla! will not work properly. Default value: `component,system,raw,koow`

### Tip

On many sites you have to set this to `component,system,raw,koowa` for your third party components to work.

### Note

The koowa keyword is only required when you run components based on Nooku Framework a.k.a. Koowa, for example DOCman. According to the Koowa developers' email we received on January 2015 there are two reasons for the use of the koowa keyword:

- The modals which contain full page JavaScript "applications", like the multi file uploader, was breaking on some templates out there because they do weird stuff in their JavaScript. No matter the precautions taken by Koowa there is at least one template out there removing the JavaScript files from the page output because they "looked like JavaScript".
- Frontend edit forms. The Koowa developers also had a lot of problems by using tmpl=component or the normal template in frontend forms. Templates re-define Bootstrap rules, use Bootstrap 3, add weird JavaScript to "enhance" the page that has no job in the component output and so on.

So, basically, they added the custom "koowa" tmpl keyword to work around restrictions imposed by templates.

Block template=foo site template switch

Another Joomla! hidden feature is the ability to switch between installed templates by passing a special URL parameter called "template". Enabling this option will turn off this hidden Joomla! feature.

Allow site templates

Enabling this option partially overrides the previous option (the blocking of template=foo in the URL). If the template= URL query parameter specifies the name of a template which exists in your template directory, then it will be allowed without raising a security exception.

### Important

If you are using the "Send this page by email" icon in your articles and/or multiple templates on your site, you MUST enable this option.

You MUST enable this option if you want your site visitors to be able to use Joomla!'s com_mailto component, i.e. the "Send this page by email" icon in your articles.

Moreover, you must use it on sites which are using more than one template at the same time. What we mean by that is that you can go to Joomla!'s back-end, go to Extensions, Templates and assign any of the installed templates to any number of menu items. When you do that, several components need to append template=*`yourDefaultTemplateName`* to the URL. This would cause your site to throw security exceptions. By enabling this option you prevent such unwanted security exceptions from being raised.

Enable 404 Shield

Whether the 404 Shield feature should be enabled or not.

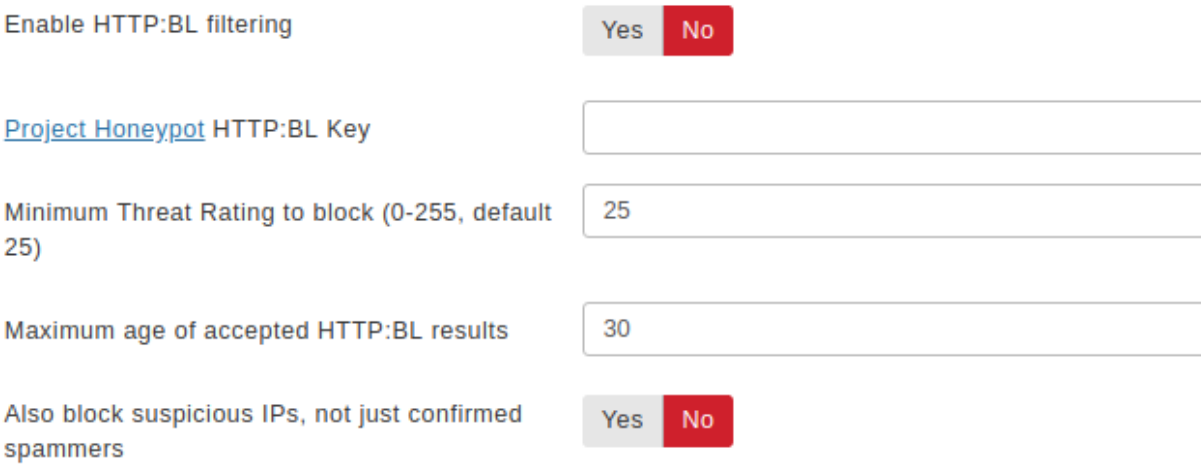
404Shield

This feature 404 will block irregular "Page not found" requests which typically indicate that your site is being targeted by an automatic vulnerability scanner or hacking tool. For example, someone trying to access the folder `wp-admin` on your Joomla site is irregular since that folder is the administration area of WordPress. Since your site is running Joomla it means that the request to your site was very likely malicious, e.g. an automated tool (bot) trying to guess your access credentials by trying various common combinations of usernames and passwords. In this light, the request has to be treated as a security exception.

The default list of URLs to be blocked by 404Shield consists of known WordPress-only paths. That's because we know that these URLs cannot be found on a Joomla site and are typically used by automated hacking tools, therefore minimising the possibility of false positives. You can always add more if you want to.

## 9.1.5. Project Honeypot

### WAF: Project Honeypot

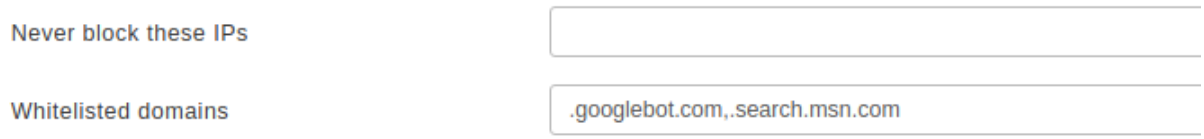



Project Honeypot allows you to integrate with Project Honeypot's spam fighting services. Project Honeypot is a collective effort to detect spammers, email harversters and crackers. Its HTTP:BL service allows participants to query the IP addresses of their visitors and figure out if it is a malicious 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 him. You have the following options:

| | |
|---|---|
| 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! |

## 9.1.6. Exceptions

### WAF: Exceptions




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 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.

Finally, you may enter a dynamic IP 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 you can enter `@example.dyndns.info` to whitelist your dynamic IP 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

Since Admin Tools 2.1.7, 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).

## 9.1.7. Auto-ban

### WAF: Auto-ban


You can easily Auto-ban. This feature allows you to automatically ban IPs triggering security exceptions. This can be prove to be an effective measure against malicious users who try to probe your site for vulnerabilities. You MUST enable logging of security exceptions for this feature to work. You can set the following options to define how Admin Tools will behave in those cases:

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

Email this address if an IP is auto banned
: 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.

> **Note**
>
> In order for the country and continent to show up in your email, you must download the GeoIP plugin as instructed in the Control Panel page.

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

Block after
: 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
: 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.

Permanently blacklist IP after
: 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.

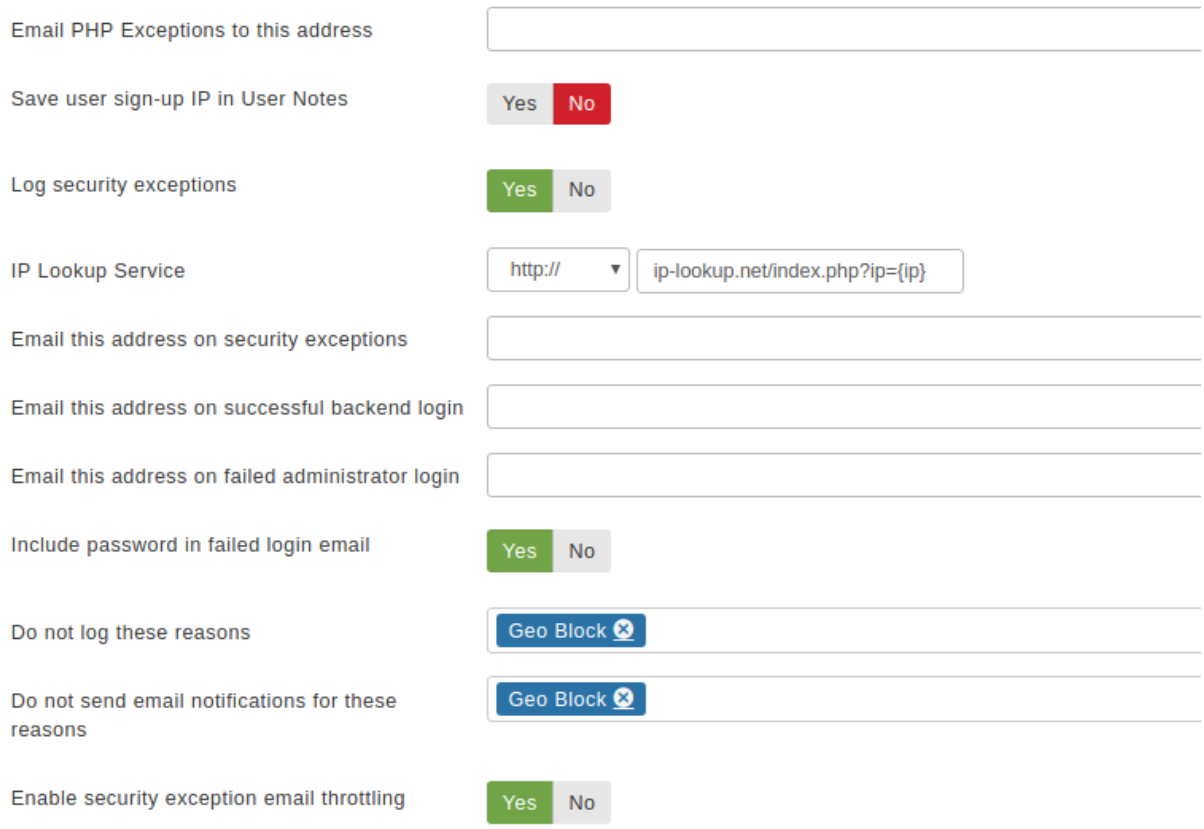
Show this message to blocked IPs

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.

## 9.1.8. Logging & reporting

### WAF: Logging & reporting




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.

Email PHP Exceptions to this address

Whenever an unhandled PHP exception is raised (ie an error on a database query), Admin Tools will send an email containing all the details (time, file and line raising the exception) for later debugging.

Save user sign-up IP in User Notes

When enabled, the IP new users signed up from will be stored as User Notes.

#### Important

This feature is guaranteed to work only when a user registers to your site using the front-end user registration form provided by Joomla!. Users created through the back-end will not have their IP saved as a User Note 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

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. This is required for the automatic IP blocking feature to work.

Please note that turning off this feature will also disable the debug log file, even if the option below is set to Yes.

## 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.

Keep a debug log file

It is suggested to keep this option disabled unless you are troubleshooting.

When enabled, Admin Tools will create a file named `admintools_breaches.php` in your site's `administrator/logs` directory (or wherever you have configured your logs directory to be). This contains all the information sent in the request that Admin Tools blocked. This may include sensitive information such as usernames, passwords and personally identifiable information. For this reason you must only enable this feature for a limited amount of time when troubleshooting. We may ask you to do this, and send us a copy of the log file, if you ask us for support.

When you disable that option, the existing log files will be removed once you visit Admin Tools' Control Panel page again.

Do note that your logs directory MUST be writable for the log file to be generated.

## Important

Some servers use automated file scanners which will mistakenly flag Admin Tools' log file as a security threat. Because of that they might issue an automated warning to you that your site is hacked, rename / delete the file or prevent web access to your site (put it offline). This is a mistake and does not reflect the truth. Our log file does have an executable extension (.php) and does contain the signatures of hacking attempts (the hacking attempts it stopped from hacking your site!) BUT the hacking attempts signature themselves are NOT executable. In fact, the only reason this is a .php file is so that we can put a PHP die() statement at the top of the file to prevent it from being executable over the web. This information is also printed at the top of the file, in its header. If your host is giving you grief about the log file please show them this documentation page or ask them to actually review the file and read its header. If they still insist that they have to block your site please go to a different host that understands how PHP works and, by extent, is a much safer choice. In the meantime, just disable the Keep a debug log file option.

## Important

By default the Joomla! `log` directory is readable over the web. We *VERY STRONGLY* advise you to either choose a log directory outside your web root or protect this directory against web access. The former can be performed through your site's Global Configuration page; please consult Joomla!'s documentation. The latter can be achieved through the directory password protection feature of your hosting control panel or by adding a .htaccess file (Apache web server) or web.config file (Microsoft Internet Information Services -IIS- server). If you are using a different server, such as NginX, the only way to protect the logs directory against unauthorised web access is using a directory outside your web server's root. Please consult your host if you are not sure how you can do this.

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.

## Note

In order for the country and continent to show up in your email, you must download the GeoIP plugin as instructed in the Control Panel page.

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 back-end login

Enter an email address which will get notified whenever someone successfully logs in to your site's administrator back-end. 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 administrator 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. `alice@example.com, bob@example.net`. 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.

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 Extensions, 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 Super 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.

## Note

In order for the country and continent to show up in your email, you must download the GeoIP plugin as instructed in the Control Panel page.

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

Email this address on failed administrator login

Enter an email address which will get notified whenever someone tries to log in to your site's administrator back-end but is denied access. If you do not wish to use this feature, leave this field blank. If you enter an email address, every time someone unsuccessfully tries to log in to the administrator 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. `alice@example.com, bob@example.net`. 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.

This allows you to get instant notification of unexpected administrator area login attempts 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 Extensions, 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 a potentially compromised Super 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.

> **Note**
>
> In order for the country and continent to show up in your email, you must download the GeoIP plugin as instructed in the Control Panel page.

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

Include password in failed login email
: 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.

  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.

  The default setting is `GeoBlock` (Geographic IP blocking)

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".

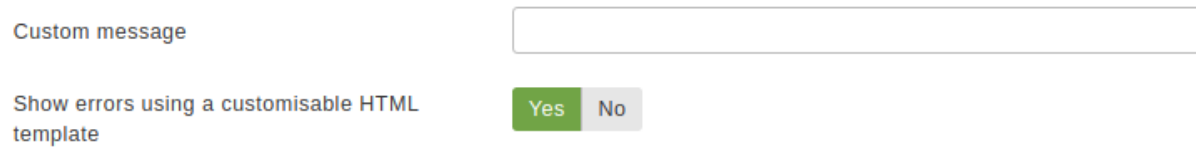
  For a list of what each reason means please consult the list of WAF log reasons. You can start typing or click on on the field to show the list of reasons.

  The default setting is `GeoBlock` (Geographic IP blocking)

Enable security exception email throttling
: 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.

## 9.1.9. Customisation

### WAF: Customisation




The Security exception message 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
: By default, Admin Tools uses a generic message ("Are you feeling lucky?") when a security exception occurs. Considering that this may not be exactly the kind of message you want your visitors to see, we allow you to customise it. Just type in the message to be shown to site

Exceptions message

visitors when a security exception occurs, e.g. "We have detected a possible security violation caused by your request. Please go back to the previous page and try again."

Show errors using a customisable HTML template

By default, the Security Exceptions Message will be shown using Joomla!'s standard error message page. This is not always desirable, as that page lacks proper styling and admittedly looks very cheesy. When this option is enabled, however, Admin Tools will use a customisable HTML template.

The default HTML template file is located in the `components/com_admintools/View/Blocks/tmpl/default.php` file. **DO NOT MODIFY THIS FILE DIRECTLY**! It will be overwritten on each upgrade. Instead, you will have to do a template override, as per the following instructions.

Locate the directory of your front-end template. For example, this could be `templates/protostar` if you are using the default template in Joomla!. Inside it there's a directory called `html`. Create a new directory named `com_admintools` and inside it yet another new directory called `Blocks`. In our example, you should now have a directory `templates/protostar/html/com_admintools/Blocks`. Copy the `default.php` file from `components/com_admintools/View/Blocks/tmpl` to `templates/protostar/html/com_admintools/Blocks`. Edit that file and customise it to your heart's desire. Do note that unlike other Joomla! template files this is a full HTML page, including the opening and closing `<html>` tags.

For more information regarding template overrides, please consult Joomla!'s documentation wiki page [http://docs.joomla.org/How_to_override_the_output_from_the_Joomla!_core] on the subject.

Send troubleshooting email on administrative functions

Some Admin Tools administrative functions have the potential to make your site behave in a way you didn't expect or even lock you out of your site. This can happen because of a misunderstanding of what a security feature does, a misconfiguration or –more rearely– a browser or server mangling the configuration you are submitting to Admin Tools. We understand that this leads to frustration and occasional panic as you have no idea what happened and how to fix it.

For this reason Admin Tools will automatically send you an email with troubleshooting instructions every time you take any administrative action which might result in getting locked out of your site or your site not working properly. These actions include applying the initial configuration with the Quick Setup Wizard, changing the Web Application Firewall configuration, applying administrator password protection or saving a new .htaccess, web.config or NginX configuration file through the relevant Admin Tools features.

The email explains what change took place and includes links to our troubleshooter documentation which can help you get your site back to a working state. Moreover, it has a reminder about getting support from us if all else fails.

The email is sent only to the email address recorded on the user account logged into Joomla who initiated this change. It is not sent to other Super Users, Administrators or, in general, any other email address. Also note that if you have set Receive system email to No in your Joomla! user profile you will not receive this email.

This option can be used to turn off this feature for all administrator users with access to Admin Tools, regardless of their Receive system email status. We recommend leaving this option enabled unless you are absolutely sure you know what you're doing and you're confident you can find your way to the troubleshooter documentation on your own.

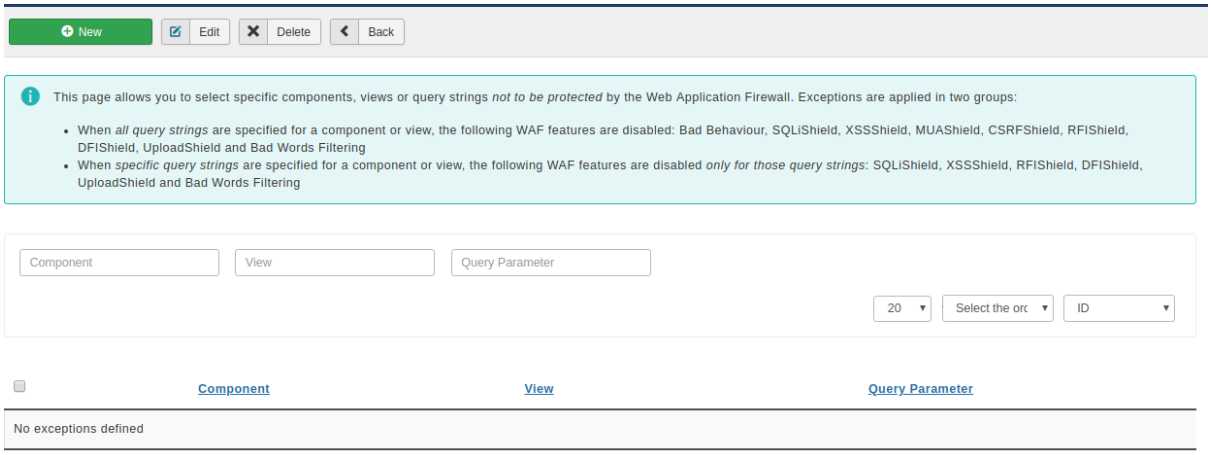
## 9.1.10. Troubleshooting (I got locked out of my site)

It's possible to accidentally lock yourself out of the administrator area, especially when using the IP whitelisting or IP blacklisting options of the Web Application Firewall. The easiest way to work around this issue is using an FTP application or your hosting control panel's File Manager to rename a file.

Go inside the `plugins/system/admintools/admintools` directory on your site. You will see a file named `main.php`. Rename it to `main-disable.php`. This will turn disable the Web Application Firewall from executing and you can access your site's back-end again. After you have fixed the cause of your issue remember to rename `main-disable.php` back to `main.php`, otherwise your site will remain unprotected!

# 9.2. WAF Exceptions

### WAF Exceptions

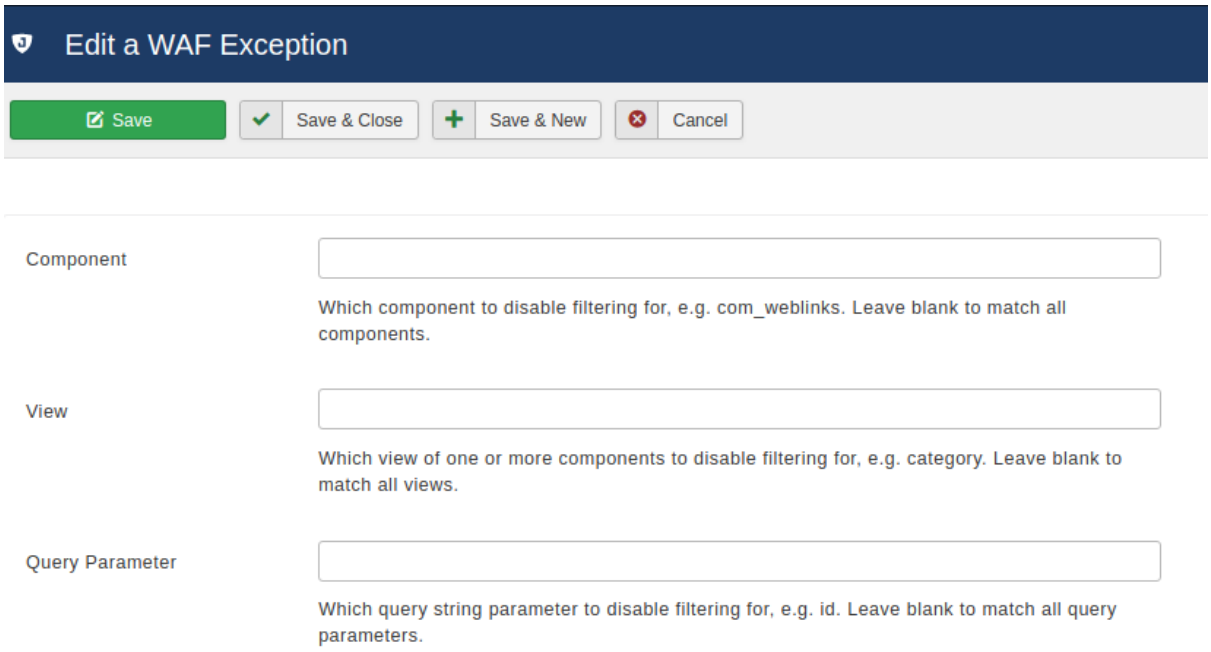



This page allows you to configure exceptions to the WAF filtering rules. Why you need that? Some components are designed to properly and safely parse and use data which triggers WAF protection rules. Most usually, a component accepts an absolute path to files on your server or can parse complex data which normally trigger WAF's filters. Without any exceptions set, these components 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 components, views and query parameters 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.

### WAF Exception




#### Important

You create a new WAF Exception by clicking on the green New button at the toolbar which is located at the top of the page. The fields under the toolbar are filters: you can use them to filter the display of WAF Exception rules. They will NOT create a new WAF Exception. As a rule of thumb, which applies to all Joomla! components, if you don't see a Save & Close button at the top of the page you need to press the green New button before being able to create something.

WAF Exceptions are defined by specifying a combination of three things:

- *Component*. Which component the exception applies to. For example, if you want to disable filtering for a query parameter in JCE you will have to set this to `com_jce`. If you want to apply the exception to all components, no matter what, leave this blank.
- *View*. Each component has one or several views. When you turn off SEF you see something like `index.php?option=com_foobar&view=example&id=1`. Note the view=example part in this URL; this tells Joomla! that the view name (i.e. the area of the component we want to use) is *example*. As you might have guessed, the View option in a WAF Exception allows you to target the exception to exactly one view. If you leave it blank, the exception will match all views.

  Components using the classic Joomla! MVC might use a different notation, like `index.php?option=com_foobar&task=item.edit&id=1` . Note the `task=item.edit` part; its value (item.edit) is a composition. The part to the left of the dot (item) is the View you need to use in the WAF Exception. Support for this Joomla! feature was added in Admin Tools 4.3.1; earlier versions cannot define WAF exceptions for components using this notation.

#### Important

Due to the way Joomla! works, if you are using Joomla!'s SEF URLs it is possible that WAF Exceptions will not work with some components. In this case, change the ordering of the System - Admin Tools and your SEF router plugins so that the SEF router plugin is published BEFORE Admin Tools' plugin. This way Admin Tools will not be able to protect your site against potential vulnerabilities in your SEF component, but it will be able to apply WAF Exceptions even when SEF URLs are turned on.

- *Query Parameter*. Everything after the question mark in a non-SEF URL is called the URL query. You will see a lot of key/value pairs, like `id=1`, `category=1:test` and so on. The word at the left hand side of the equals sign is called the *Query Parameter*. The same-named parameter in WAF Exceptions allows you to target a very specific query parameter. If you leave it blank, all query parameters will be matched.

### Warning

You can not leave all three options blank. That would match all components, all views and all query strings or, in other words, EVERY PAGE you access. This would imply that WAF would be effectively turned off. Admin Tools detects an attempt to do that and won't allow you to perform such a change.

## Understanding WAF exceptions

The best way to understand WAF exceptions is by some practical examples.

**Whole-component exception**. Set component to `com_jce`, leave view and query parameter empty. This tells WAF that if it sees a request for JCE's utility component (com_jce) is should turn off WAF no matter which view or which query parameters are set. Essentially, WAF is turned off for the entire JCE component.

**Excepting a single component's view**. Let's say we want to disable WAF for all front-end logins to avoid a complex password throwing a 403 error to our users. Front-end logins are handled by com_user's login view. So just set component to `com_user`, view to `login` and leave the query parameter blank. WAF is now disabled for the login/logout page of your site.

**Excepting a query parameter of a specific component and view**. Let's say we have a com_foobar component whose test view accepts a pass parameter. Strong passwords may accidentally trigger WAF. Just create a new exception where component is `com_foobar`, view is `test` and query parameter is `pass`. WAF will not deal with that specific query parameter on that specific component and view, but will be triggered by unsafe content passed in any other query parameter on that particular view.

**Excepting a query parameter across all components and views**. Let's say that you see a lot of 403s in your site because various components use a password query parameter to accept passwords and, as we mentioned above, complex passwords can trigger WAF. Instead of hunting down all the views across all components, you can simply leave component and view empty and set the query parameter to `password`. From now on, when WAF sees a password parameter coming into Joomla! it will not try to apply its protection filters against it. If other query parameters come in with the user request they will be filtered and, if they contain unsafe content, the request will still be blocked.

# 9.3. WAF Blacklist

Sometimes vulnerabilities in older versions of Joomla! and its extensions do not rely on maliciously crafted data but holes in the validation of perfectly normal, innocent-looking data. For example, a well-known e-commerce extension for Joomla! had a vulnerability in 2014 which would allow an attacker to create a Super Administrator account by passing an undocumented (and unfiltered) parameter in the new client account creation form. The only way to protect against this kind of attacks is being able to block requests which contain the sort of key-value pairs involved in these vulnerabilities. This can be accomplished with the WAF Blacklist.

### Important

You create a new WAF Blacklist rule by clicking on the green New button at the toolbar which is located at the top of the page. The fields under the toolbar are filters: you can use them to filter the display of WAF Blacklist rules. They will NOT create a new WAF Blacklist rule. As a rule of thumb, which applies to all Joomla! components, if you don't see a Save & Close button at the top of the page you need to press the green New button before being able to create something.

WAF Blacklist rules are defined by specifying a combination of a few things.

In order to better explain this, please consider the sample URL `http://www.example.com/index.php?option=com_example&view=foo&task=bar&badidea=oops` Let's consider that we want to block the

badidea=oops, badidea=oops1 and so on because if the value of the "badidea" parameter begins with "oops" the component com_example will do something dangerous, e.g. give the attacker access to all our data.

- **Enabled**. If you want to temporarily disable a blacklist rule when troubleshooting your site you can simply set the Enabled field to No.
- **Application**. Joomla! has two applications, the public frontend (the site your visitors see) and the administrator backend (where you manage your site). By default, WAF Blacklist rules apply only to the frontend of your site. You can choose to apply them in the backend of your site as well, or both.
- **Verb**. The HTTP verb applicable to the request. The most common are GET (access a URL) and POST (submit a form). If you're not sure leave the empty option (three dashes) to have the rule apply to all verbs.
- **Component**. The component which will be filtered. This is required. In a non-SEF Joomla! URL this is the value of the *option* query parameter (and before the first ampersand following it, if any). For example, in the sample URL this is `com_example`
- **View**. The view of the component which will be filtered. If left blank the rule will apply to all views of the component specified in the rule. In a non-SEF Joomla! URL this is the value of the *view* query parameter (and before the first ampersand following it, if any). For example, in the sample URL this is `foo`

  Components using the classic Joomla! MVC might use a different notation, like `index.php?option=com_foobar&task=foo.bar&badidea=oops` instead of the example URL we noted before. Note the `task=foo.bar` part; its value (foo.bar) is a composition. The part to the left of the dot (item) is the View and the value to the right is the Task.
- **Task**. The task of the component which will be filtered. If left blank the rule will apply to all tasks of the component and view specified in the rule. In a non-SEF Joomla! URL this is the value of the *task* query parameter (and before the first ampersand following it, if any). For example, in the sample URL this is `bar`

  The note about components using the classic Joomla! MVC applies here as well. If the task has a dot in it then the part to the left of the dot MUST be placed in the View field and the part to the right of the dot MUST be placed in the Task field.
- **Query Parameter**. Here you can specify the name of the query parameter which will be blocked. This is the name of the parameter after the ampersand and before the equals sign. In our sample URL it is `badidea` You have three ways to define it:
  - **Exact**. What you enter is the exact name of the query parameter. If you enter `badidea` the rule will filter badidea but not badidea1, badideamister or thisisabadidea.
  - **Partial**. What you enter is part of the name of the query parameter. If you enter `badidea` the rule will filter badidea, badidea1, badideamister and thisisabadidea.
  - **Regular Expression**. What you enter is a Regular Expression. For example, if you enter `/idea$/` the rule will filter badidea and thisisabadidea but NOT badidea1 or badideamister.
- **RegEx for query content**. Enter a regular expression which will be used to match the value of the query parameter, i.e. what follows the equals sign after the query parameter name and before the first ampersand after it. In our example we'd need to use `/^oops/` to filter all values beginning with "oops". If you leave it empty than any value will be matched by this rule.

## Warning

It is a very bad idea using a Query Parameter which contains the text option, view, task and Itemid as these are Joomla! reserved keywords. If you create such a rule we can't guarantee what the results will be. You have been warned!

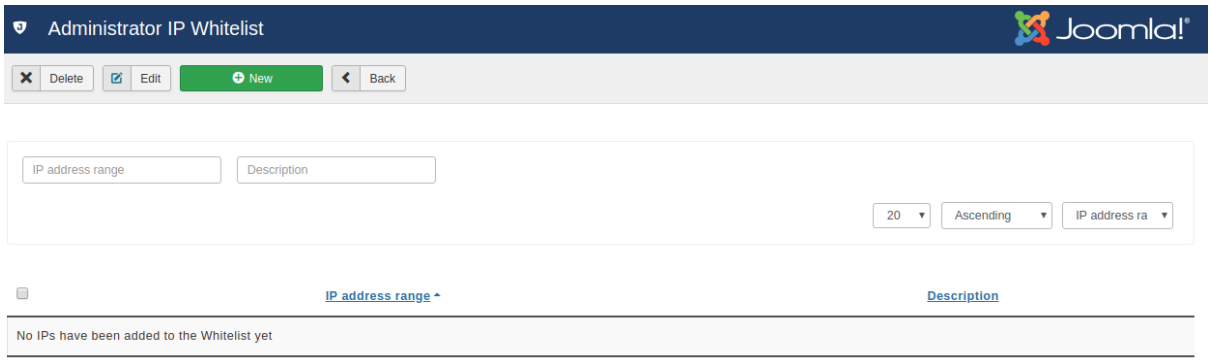
## Warning

When using Partial and Regular Expression matches be very careful not to filter innocent query parameters. For example, a partial match on id will also block Itemid which is a reserved Joomla! keyword

that's internally appended to all URLs of your site. If you still didn't understand this: doing a partial match on id and an empty RegEx for query content will block everyone from accessing any page on your site! If this happens you can rename the plugins/system/admintools folder to admintools-noload (this will prevent Joomla! from loading the System - Admin Tools plugin, therefore disabling Admin Tools' protection), go back to Admin Tools, fix your rule and rename the folder back to admintools to re-activate Admin Tools protection.

# 9.4. Administrator IP Whitelist

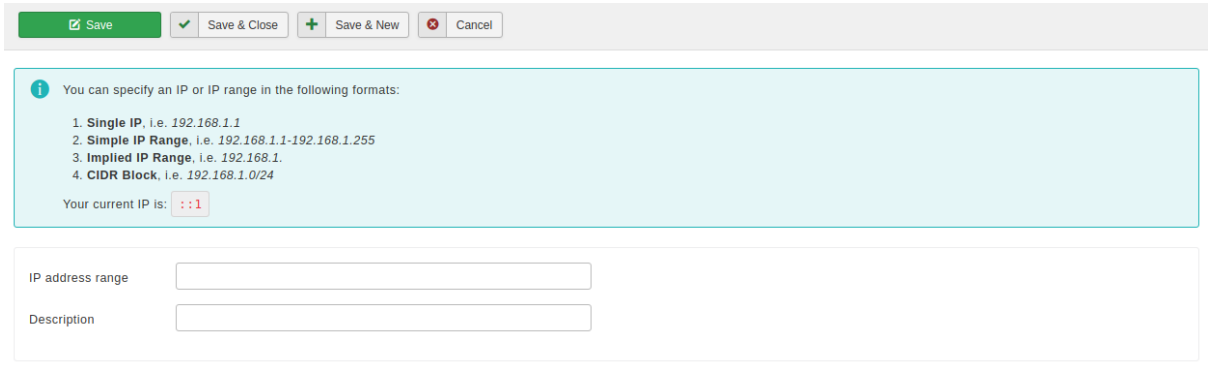
### The Whitelist management page




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 management is done using the standard Joomla! toolbar buttons. Clicking on an entry, or checking its box and clicking on Edit will allow you to edit the entry. Clicking on the New button allows you to add an IP/IP range. Checking one or several items in the list and clicking on Delete will remove them from the list.

The Edit/Add page looks like this:

### The Whitelist editor page




## Tip

You 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 IP 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 you can enter `@example.dyndns.info` to whitelist your dynamic IP 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. Furthermore, this method ONLY works with IPv4 addresses. Dynamic IP domain lookups do not take into account the IPv6 address. 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). However, IPv6 will not work with the Dynamic IP Domain Name entries.

### Tip

You can use the Save & New to quickly add multiple entries without having to go back to the administration page and click on New all the time.

## 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 5.2.0 and later make 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 access the administrator login page while logged out of the administrator 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.

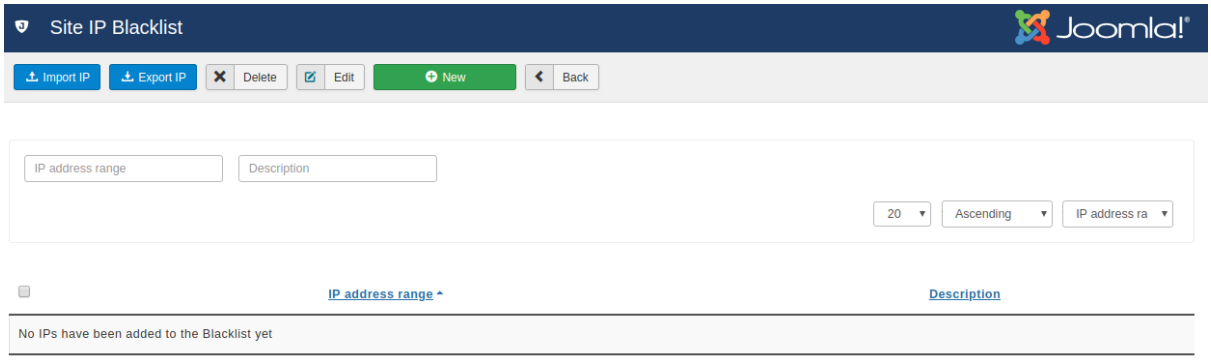
Furthermore, all dynamic IP providers have a default timeout for the dynamic DNS entries varying from 1 minute to 1 hour. If your IP changes within that period your server might be "blind" to the change. The same thing can happen if your dynamic IP updater (typically running in your router or NAS firmware) 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 updater 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 have to access your administrator area 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. The management is done using the standard Joomla! toolbar buttons. Clicking on an entry, or checking its box and clicking on Edit will allow you to edit the entry. Clicking on the New button allows you to add an IP/IP range. Checking one or several items in the list and clicking on Delete will remove them from the list.

## 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.

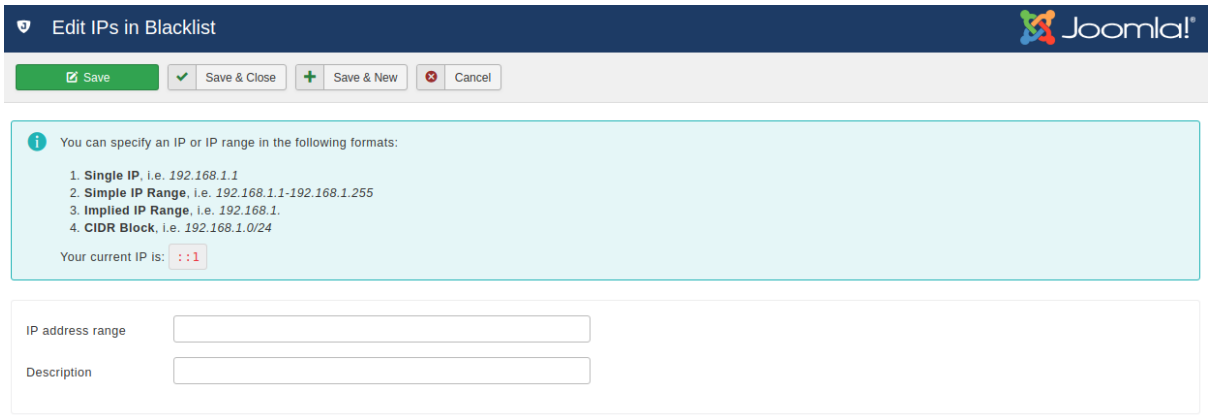
There is a small, but large enough to be annoying, percentage of attacks originating from wanna-be hackers who use the same IP address to attack you over and over again. Usually they're running a dumb script with no error handling. Therefore even when Admin Tools blocks them automatically they keep trying 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

You 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).

#### Tip

You can use the Save & New to quickly add multiple entries without having to go back to the administration page and click on New all the time.

### 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

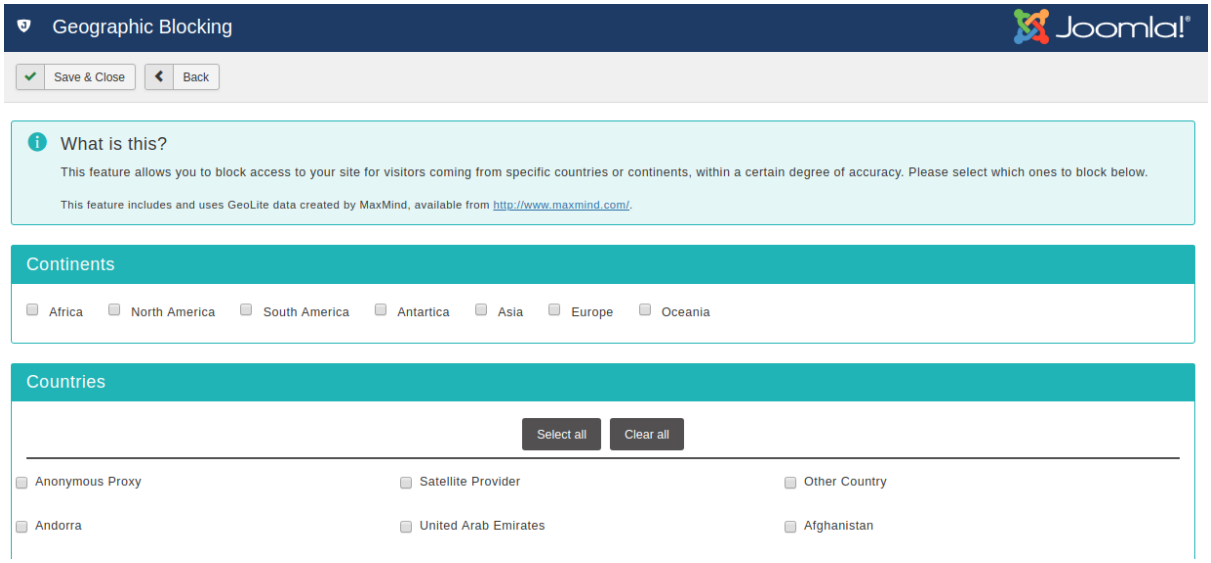

This page allows you to manage the list of Bad Words. Their use will be forbidden on the site. If a query contains one of those words, it will result in a 403 error and it will optionally be logged in your Security Exceptions Log. You can use the standard Joomla! toolbar buttons to administer the list. 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. Geographic blocking

### Geographic blocking



Several users have asked for a consistent way to block visitors coming from specific countries or continents. While this adds no security –a clever cracker would just hide behind an anonymizing proxy– it may still be useful for inherently regional sites, such as e-shops able to deal with a handful of countries only.

The interface page of Admin Tools' Geographic Blocking feature allows you to select which countries and/or which continents you want to block. If it's checked, it will be blocked. When you're done selecting the continents or countries you want to block, click on Save.

## Should I use this feature?

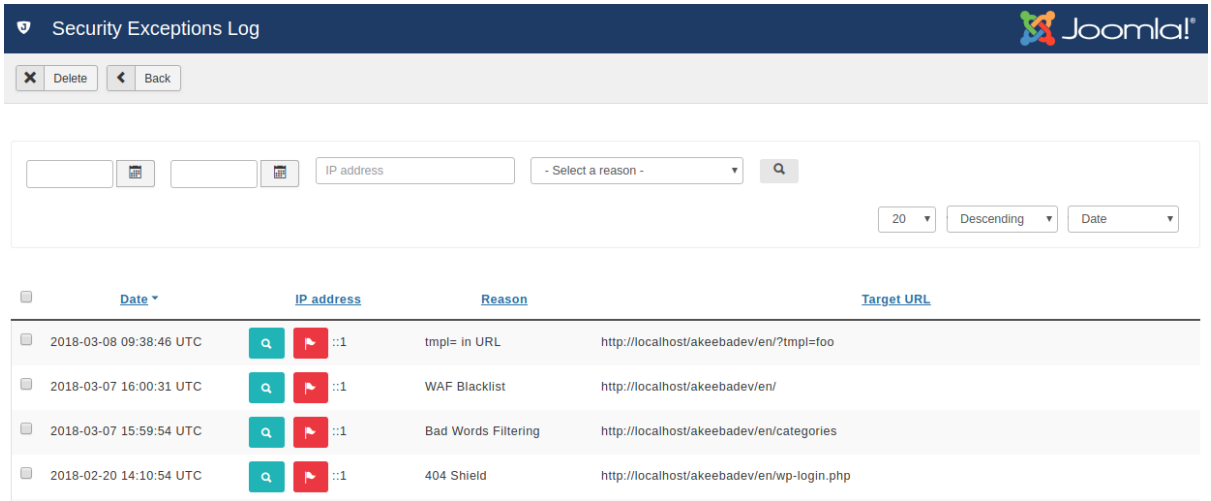
We strongly believe that geographic blocking doesn't add anything to the security of your website. Most people think "cool, I can block those Russian spammers". Nothing could be further from truth than that. The intelligent spammers and crackers do not use a single computer in their country to launch their attacks on other sites. They are usually in control of a botnet, a collection of compromised computers around the world which do what they are told to. Using such a botnet, they can launch a spam operation whose traffic comes from different countries around the globe - even the country you live in. Clever crackers will also never use their real IP address to attack you. They usually use an anonymizing proxy or the TOR network. The immediate effect is that the traffic seemingly comes from another country or from a variety of different countries.

Then, there is the accuracy factor. MaxMind claims a 99% accuracy. On a site with 10,000 visitors per day this translates to 100 visitors every day reported as coming from a different country than they really do. This might not sound such a big deal, but imagine having an e-shop and losing those potential clients. It suddenly becomes quite a big deal.

All and all, we recommend common sense. IP filtering is like the bouncer at the door. You wouldn't expect to find a bouncer standing next to your bakery's door. Likewise, don't overdo it with geo blocking. Use it sparingly.

# 9.8. Security Exceptions Log

### The Security Exceptions Log viewer page




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.

## 9.8.1. 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.

404 Shield — Code: `404shield`

See the Configure WAF page, 404 Shield. The request was blocked by Admin Tools.

Admin Query String — Code: `ipwl`

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.

tp=1 in URL — Code: not applicable

Only for Joomla! 1.5, see the respective option in the Configure WAF page. The attack was blocked by Admin Tools.

tmpl= in URL — Code: `tmpl`

See the Configure WAF page, Block tmpl=foo system template switch. The attack was blocked by Admin Tools.

template= in URL — Code: `template`

See the Configure WAF page, Block template=foo site template switch. The attack was blocked by Admin Tools.

MUA Shield — Code: `muashield`

See the Configure WAF page, Malicious User Agent block (MUAShield). The attack was blocked by Admin Tools.

CSRF Shield — Code: `csrfshield`

See the Configure WAF page, CSRF/Anti-spam form protection (CSRFShield) . The attack was blocked by Admin Tools.

Bad Behaviour — Code: not applicable

See the Configure WAF page, Bad Behaviour integration. The attack was blocked by Admin Tools. NO LONGER PRESENT SINCE ADMIN TOOLS 2.5.3

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.

XSSShield — Code: `xssshield`

(Only on older sites) Cross Site Scripting block (XSSShield). The attack was blocked by Admin Tools. This has been removed in Admin Tools 3.6.7 as it was throwing too many false positives (legitimate requests being blocked).

Geo Block — Code: `geoblocking`

Someone tried to access your site's front- or back-end but his IP belonged to a forbidden country or region as definite in the Geographical Blocking feature of Admin Tools.

Spammer (via HTTP:BL) — Code: `httpbl`

See the Configure WAF page, SQLiShield protection against SQL injection attacks. 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.

Two-factor Auth Fail — Code: `securitycode`

Someone tried to log in the back-end of your site but provided the wrong Two Factor Authentication code. Please note that this feature has been removed since Admin Tools 3.5.0. If you see it, it probaby comes from an old version of Admin Tools.

Backend 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 belong in one or more User Groups that gives them backend login privileges. In a default Joomla! installation these are the users belonging to the Manager, Administrator and Super User groups.

Frontend Edit Admin User — Code: `nonewfrontendadmins`

Someone tried to create or edit an administrator user from the frontend of your site. In this context "administrator user" means any user who belong in one or more User Groups that gives

them backend login privileges. In a default Joomla! installation these are the users belonging to the Manager, Administrator and Super User groups.

Configuration Editing

Code: `configmonitor`

Someone tried to change either the Global Configuration of Joomla! itself or the configuration (Options) of a component. Please consult the additional information saved with this security exception to understand which configuration was attempted to be changed. The change may have originated from the backend or the frontend of your site.

# 9.9. Auto IP Blocking Administration

### Auto IP Blocking Administration


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.

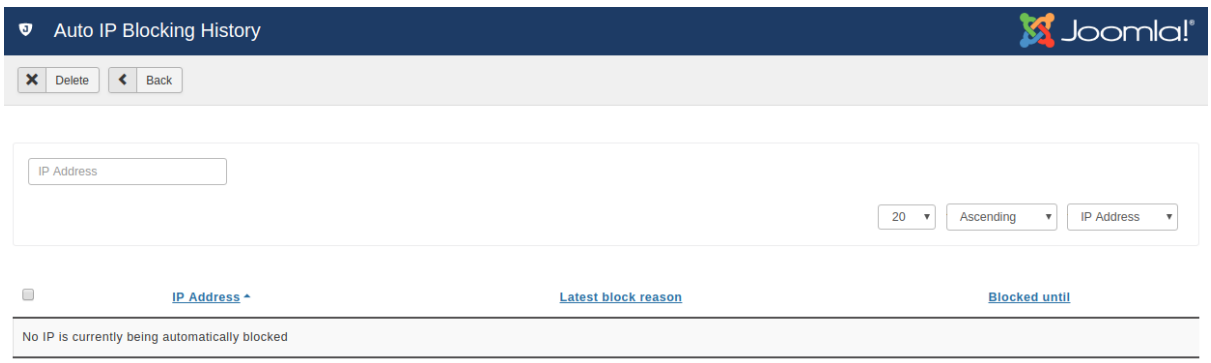
Please remember that this page only lists the automatic bans currently in effect. For a list of automatic IP bans which have been lifted please consult the "Auto IP Blocking History" page.

#### 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.

# 9.10. Auto IP Blocking History

### Auto IP Blocking History




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.

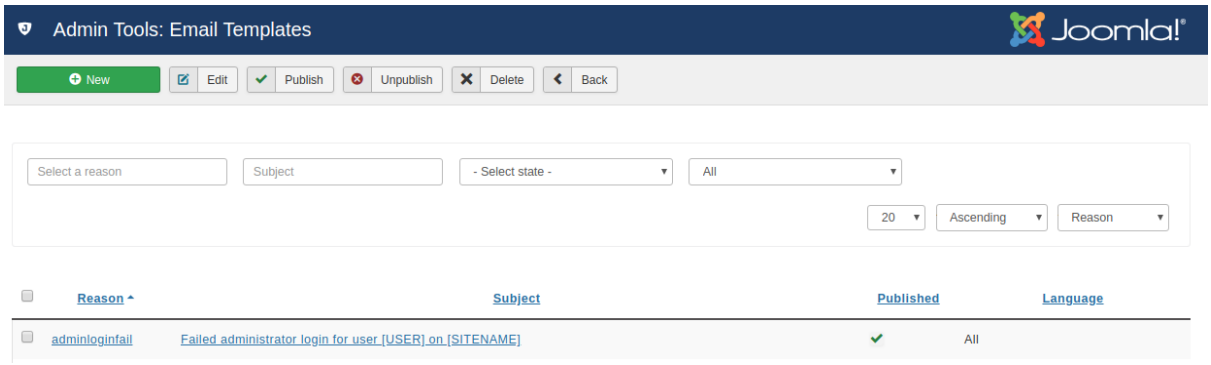
The contents of this page are used by Admin Tools together with the "IP blacklisting of persistent offenders" option in the Configure WAF page to determine which IPs of repeat offenders should be automatically added in the permanent IP blacklist.

### 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.

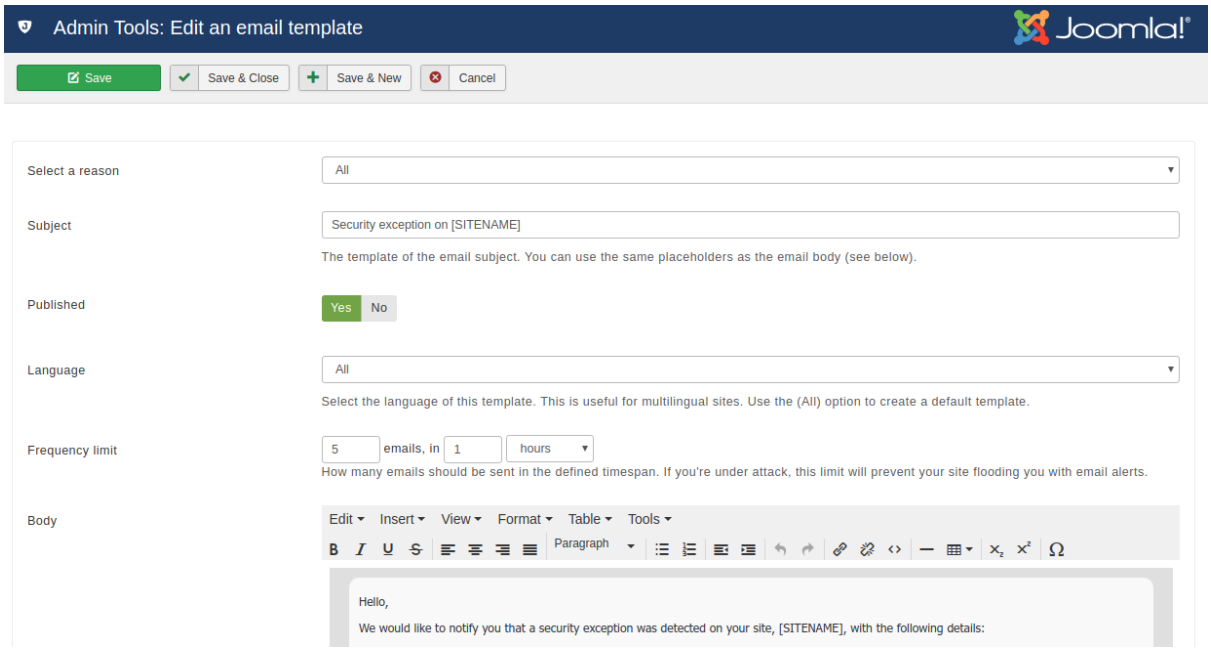
# 9.11. Email templates

## Email templates




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




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. |
| Language | Select the language of the email template. If an email template is not found for the currently active site's language when an email is about to be sent out Admin Tools will use the one with its language set to "All". If such a template is not found, Admin Tools will look for a template with its language set to "English (United Kingdom)". |
| 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)
- [COUNTRY] Country of the attacker (you need the Akeeba GeoIP plugin enabled)
- [CONTINENT] Continent of the attacker (you need the Akeeba GeoIP plugin enabled)
- [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. Database tools

## Warning

These features are only available on sites using the MySQL database server.

Do note that these tools can be both found in Admin Tools' Control Panel page since Admin Tools 1.0 Stable. Previous versions used to have them in a separate page.

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. One table notorious for becoming very fragmented too fast is the sessions table. In fact, every time a guest user visits your site or a user logs in and logs out from your site this table starts becoming bloated until, one day, nobody can log in to your site, not even yourself. This is a very common issue, especially on high-traffic sites.

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!

There are three tools available:

- 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 Joomla! sessions table is so bloated that PHP times out waiting for your database server to optimise this table.
- Purge Sessions will purge (completely empty) and optimize only the sessions table. Doing so will log everybody out of the site, including yourself. Use this option sparingly and only when you observe severe problem when users are trying to log into the site.
- **Change Database Collation** will let you change the character encoding for your database data. See the Information on Database Collation below for details.

A cut-down version of the optimisation process, addressing only the sessions table, can be scheduled to run on a timely basis by using the parameters of the "System - Admin Tools" plugin of the Professional release.

# Information on Database Collation

## What is the collation and why you need to change it?

Joomla! stores all your data, including your articles, tags and third party extensions' data, in the database. The database needs to know what the raw binary data represents in order to do basic operations such as searching for information, ordering information and so on. This is called the *collation* of the database.

Joomla! is optimally designed to use the UTF-8 character set with a "generic" (multilingual) collation. In short, the UTF-8 character set allows you to store the characters of most written languages on the planet. Technically, UTF-8 is an *encoding* format for Unicode, the universal character representation format supported by all modern software and operating systems. UTF-8 can store each character in one to three bytes. For instance English characters are typically stored using one byte, Greek and Cyrillic characters using two bytes each, Simplified Chinese and Japanese Hiragana and Katakana characters with three bytes. Most database servers are configured to use UTF-8 by default and Joomla! will work trouble-free on them.

However, some database servers are configured to use a different collation, latin1_swedish_ci. This may sound strange, but it's the default setting of MySQL. Basically, some server administrators were too lazy to change a single line in a single configuration file before putting the server on-line. This could lead to problems running Joomla!, e.g. accented or non-latin characters (Cyrillic, Greek, Hindu, ...) could end up as garbled text or question marks. The solution to this problem is using the Change Database Collation feature of Admin Tools to change the collation of your database to UTF-8.

## Different UTF-8 collations, multibyte characters (Emoji, Chinese, ...) and security

The default UTF-8 collation used by Joomla! can only store characters consisting of up to three bytes each. This means that some characters cannot be represented at all. The most frequently used 4-byte characters are Emoji (the faces and symbols you get on your iPhone!), and some of the less often used Traditional Chinese and Japanese Kanji characters.

At the time of this writing (May 2016) Joomla! only supports 4-byte characters in Joomla! 3.5.0 and later. Earlier versions do not. If you try to enter a 4-byte character, e.g. an Emoji, all text following this character *will be silently lost*. This is both a nuisance and a security issue. Since the text following a 4-byte character is lost you can end up with corrupt HTML. This corruption takes place after the data has been sanitised by Joomla!'s code, essentially tricking Joomla! into inserting invalid and possibly dangerous data into the database. While no exploit is known at the time of this writing this issue is very similar to a WordPress security flaw affecting all WordPress releases up to and including 4.2.0. Therefore we consider the lack of 4-byte character support as a POTENTIAL security issue. Please note that this is a POTENTIAL and UNPROVEN security issue. There may actually not be a security issue at all. But since the possibility exists we provide you with a way to work around it.

Using the Change Database Collation change your database's collation to UTF-8 Multibyte. This uses the utf8mb4_general_ci collation which tells MySQL to add support for 4-byte characters. On top of that, the System - Admin Tools plugin tells Joomla!'s database driver to add support for 4-byte characters.

### Warning

If you enable the UTF-8 Multibyte collation you MUST have the System - Admin Tools plugin enabled. Otherwise the 4-byte characters (e.g. Emoji) will be saved and displayed as a series of four question marks, like this: ???? This will no longer be necessary if Joomla! itself adds support for multibyte characters anytime in the future.

### Things to keep in mind when changing the collation

Always take a backup BEFORE changing the collation. This process actively modifies all your database content. Such an operation has an inherent risk, in that MySQL may corrupt your data in the process. While rare, it's not unheard of. A fresh, locally kept, tested backup is the only thing standing between you and a catastrophic failure.

Though not strictly necessary, we've found that on some servers you MAY have to use the Repair & Optimise feature in Admin Tools right after changing the database collation. This is especially true if you have tables with several thousands of rows or more.

Depending on your database server privileges and the nature of the extensions you have installed you MAY have to repeat the change collation process after installing new extensions or updating existing ones. How can you know? It's simple. If you get funny looking characters, truncated text or question marks instead of text you know you need to redo the Change Database Collation process.

Also note that changing the collation MAY result in a blank page if you have too many and / or too big tables. This is simply PHP timing out while MySQL processes large sets of data. Don't panic. Repeating the process a few more times will eventually let it complete successfully.

# 11. The PHP File Scanner

### Note

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

We have introduced a very powerful feature in Admin Tools Professional 2.2.a1 called PHP File Change Scanner. This feature can be used to perform a security scan of the PHP files included inside 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.

The PHP File Change Scanner doesn't stop at scanning. Coupled with an array of handy features such as 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 standard CRON job (available for Joomla! 1.7 and later only), making sure that you always know what's going on with your site.

### Warning

Only files with a lowercase .php extension are scanned. Non-PHP files or PHP files whose extension is different (e.g. .PHP in capitals, .php4, .php5, .php.inc, .inc, .phps and so on) 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.

Moreover, not all hacking scripts are written in PHP. Some of them may be written in PERL, Python, Ruby, shell scripting 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.

# 11.1. 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 Joomla! site for PHP files and comparing them to their last known state 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 Joomla! 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 Joomla 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 a lowercase .php extension are scanned. Non-PHP files or PHP files whose extension is different (e.g. .PHP in capitals, .php4, .php5, .php.inc, .inc, .phps and so on) 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.

**Directories automatically skipped**. Admin Tools Professional will automatically skip scanning the following directories: `tmp`, `cache`, `administrator/cache`, `log`. These files contain temporary files, logs disguised as PHP files or cache files disguised as PHP files. The contents of neither of those directories is supposed to be directly accessible over the web – and that's why Joomla! allows you to relocate them to off-site locations. If you run across an extension which references files in those directories from a frontend or backend page, uninstall it a.s.a.p. as this is a sign of a developer not knowing what he's doing. Would you trust that developer with your site? I wouldn't.

## Note

Regarding the tmp and log directories, Admin Tools Professional will actually take a look at your Global Configuration settings and exclude the directory for temp-files and directory for log files specified in there. Usually these are the tmp and log directories respectively, hence the reference to those directories in the paragraph above.

**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. 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 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. 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. An average site contains about 3,000 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 very big strain on your server, similar to what you get when you're backing up your site.

**Requirement for a writable temp-file directory**. In order for this feature to work, we need to keep a temporary file in your site's temp-files directory (configurable in the Global Configuration page, usually it's `tmp` under your site's root). For this to be possible, your tmp directory has to be writable. Depending on your file ownership and permissions, your tmp directory may be unwritable. In this case, you have to perform a trick to make it writable without compromising the security of your site. First, give that directory 0777 permissions. Then, upload (using FTP) a .htaccess file in your temp-files directory with the following contents:

```
<IfModule !mod_authz_core.c>
Order deny,allow
Deny from all
</IfModule>
<IfModule mod_authz_core.c>
<RequireAll>
Require all denied
</RequireAll>
</IfModule>
```

Give the .htaccess file you just uploaded 0444 permissions.

Remember to use Admin Tools' Permissions Configuration to set up the permissions of the directory to 777, otherwise the folder will become unwritable as soon as you use Admin Tools' Fix Permissions feature. The trick outlined above makes the temporary directory world-writable (anyone with access to the server can write to it). This is normally unsafe. However, it is unsafe only if anyone could access the files in that directory over the web, essentaily being able to execute arbitrary PHP code. By uploading the .htaccess we mentioned, you made the directory inaccessible from the web. This means that a potential attacker could write arbitrary PHP files in this directory, but not execute them, therefore no longer posing a security risk. By changing the permissions of the .htaccess file to 0444 we made it read-only, so that a potential attacker can not override it, unless he has FTP access to your site (in which case your site is already hacked, so you shouldn't worry about the temp-files directory any more...).

**Using with Akeeba Backup 3.3.6 or earlier**. Akeeba Backup 3.0.a1 up to and including 3.3.6 would use your site's temp-files directory to store its temporary "memory" files (later versions use the backup output directory, which is a different directory). Admin Tools' PHP File Change Scanner feature is based on Akeeba Engine, the same engine used by Akeeba Backup, and also uses the site's temp-files directory to store its own "memory" files. However, the names of the temporary "memory" files of both Akeeba Backup and Admin Tools are the same. This means that if both a backup and a PHP file scan operation are running at the same time, both of them could crash or there could be other, unknown consequences. The solution is simple: do not run both a scan and a backup at the same time. Run first one of them, e.g. the backup, wait for it to complete, then launch the other one, e.g. the scan. If you have Akeeba Backup 3.3.7 or later this should not be a problem and you could run both a backup and a scan operation at the same time, albeit this is not recommended due to server resource usage concerns.

**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 more performant / higher-quality host.

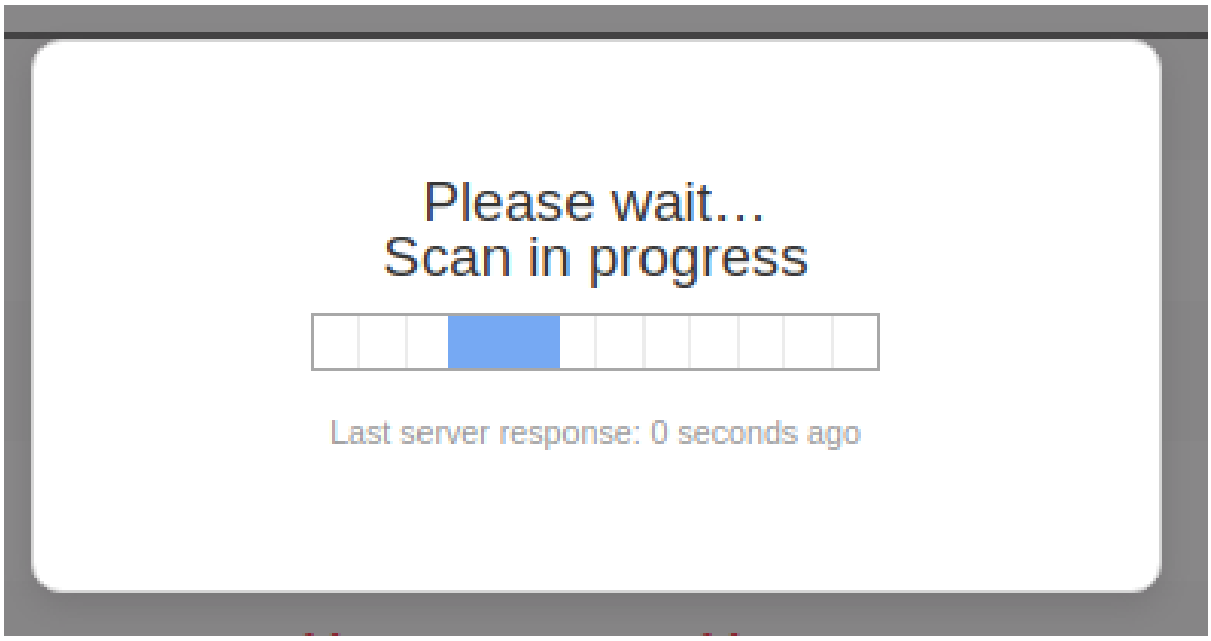
# 11.2. Configuration

You can configure the PHP File Change Scanner from the standard Joomla! component Options page. Just go to your site's back-end and click on Components, Admin Tools. Then click on the Options button to open the Options page. The settings for the file scanner can be be found in the File Scanner tab.

# 11.3. Scanning and administering scans

## Performing a new scan

### PHP File Scanner: Running a scan



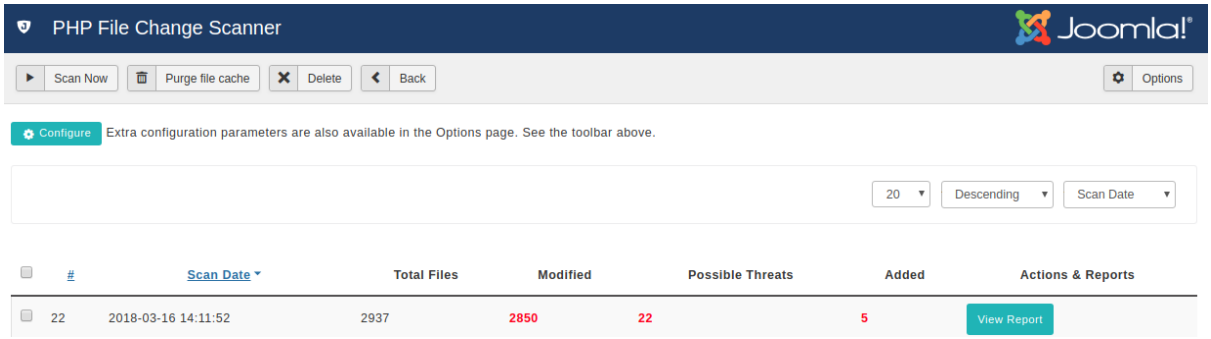

Performing a scan is a very simple process. Just go to your site's backend, Components, Admin Tools and click on PHP File Change Scanner. On that page, simply click on Scan Now to initiate the scan. A modal dialog is displayed.

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

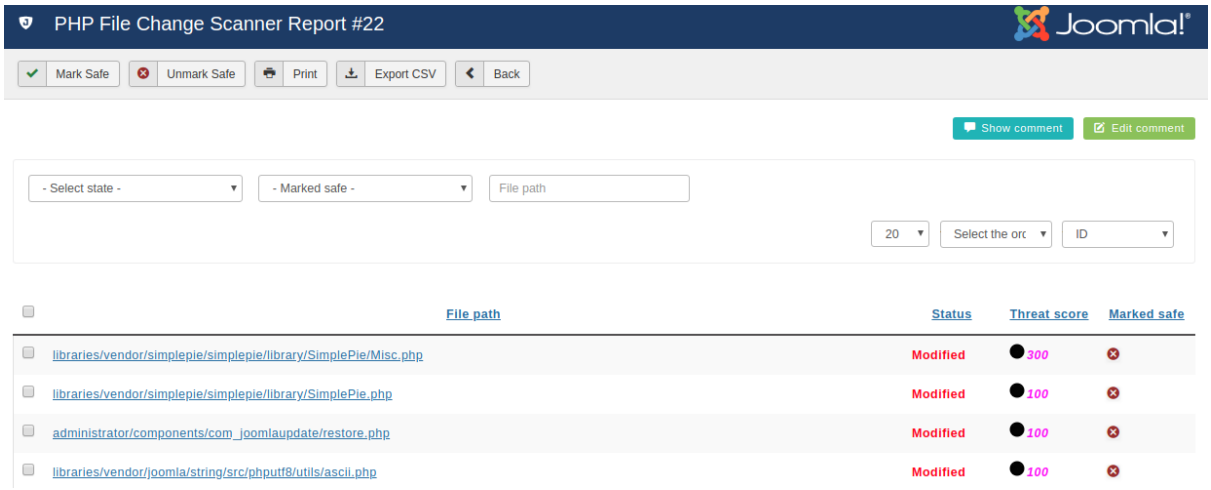



The main page of the PHP File Change Scanner feature gives you an overview of the scan operations. From left to right, you see the following columns on each row:

- **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.

# 11.4. Reading the reports

### PHP File Scanner: Reading the reports




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, several Joomla! core files, several Akeeba Subscriptions plugins and several K2 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 Joomla! and the extension this file belongs to. For example, let's say that you get a high threat score for the `administrator/components/com_k2/lib/elfinder/elFinderVolumeDriver.class.php` file. From the file path you can understand that it's part of the K2 component. Install a new Joomla! site on a local server and install K2 on it. Find the `administrator/components/com_k2/lib/elfinder/elFinderVolumeDriver.class.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. I have my favourites for Mac OS X, but since they're all commercial I'd rather not suggest any of them. 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.

## Tip

A quick way to see if a file is compromised is to quickly scan its top and bottom 20 lines. The vast majority of hacking scripts adds the hack code either at the top or at the bottom of the file. If no suspicious code is seen in there, your file is *most likely* safe. If you want to be certain beyond a shred of doubt use the full file comparison method I described above.

## Tip

It's a good idea to filter the list by threat score. Just click on the Threat Score header twice. This will place the highest rated files (therefore more likely to be malicious) at the top of the list.

- **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 them 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 fie has since been deleted, you will see an empty pane.

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.

## 11.5. Automating the scans (CRON jobs)

#### Tip

Consult the PHP File Change Scanner Scheduling page 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 `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/cli/admintools-filescanner.php
```

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.

## 11.6. Automating the scans (front-end scheduling URL)

#### Tip

Consult the PHP File Change Scanner Scheduling page 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 **cron** 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 Options button. Find the option titled Enable front-end scheduling 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*/index.php?option=com_admintools&**

**view=filescanner&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*/index.php?option=com_admintools&**

**view=filescanner&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.

# 12. SEO and Link Tools

This section of Admin Tools includes useful tools to improve your improve your site's SEO and handle your site's links. The list of features in this section is going to expand over time.

# Link migration

### SEO and Link Tools: Link migration


When you move your site across hosts, you may end up with broken intra-site links. Most of the times, this is caused by either putting absolute links or moving the site into a different directory name than it used to be.

In the first case, let's say you move your site from `www.example.com` to `www.example.org`. If you copied links from your browser's address bar and pasted them into your content or menus you're stuck with a bunch of links referencing the www.example.com domain name, i.e. `http://www.example.com/somepage.html`. Finding and changing those links is a mighty task, especially if you have thousands of content items.

In the latter case, which is the most common, the typical scenario goes like this. You develop your site locally, accessing it as `http://localhost/mysite`. Then you move your site to a live server with an address like `http://www.example.com`. Suddenly, all of your links and images are broken! Why? All WYSIWYG Joomla! editors create relative URLs. For example, linking to `images/stories/image.jpg` creates a link like `/mysite/images/stories/image.jpg` in your content's HTML source code. If you take a good look at this URL, you'll immediately notice the /mysite prefix. This works perfectly on your local server, as your site is inside the /mysite directory of your web root, but breaks on the live site as you are restoring to the web root itself! Again, finding all those references and changing them is a mighty task.

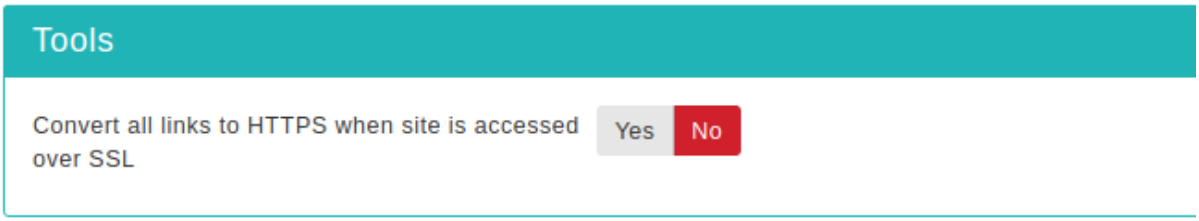
Might task it isn't anymore! Admin Tools Link Migration feature comes to your rescue. First, set the Enable link migration option to Yes in order to enable the feature. In the Old locations text area you will have to enter the domain names or subdirectories where your site used to live, one on each line. For example, if your site was hosted on `http://www.example.com`, you have to enter `www.example.com` on one line (that is, without the http:// or https:// prefix!). If you want to work around relative URLs, enter both the full URL and directory, one at each line, i.e. `http://localhost/mysite` on one line and `/mysite` on another line. Admin Tools will work its magic, migrating your URLs to point to your new site, on-the-fly as Joomla! is generating your site's pages.

## Important

Please remember to clear your Joomla! cache and your browser's cache after enabling this feature in order to see the changes in your browser when you reload your site's pages.

# Tools

### SEO and Link Tools: 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 extension 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.

#### 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.

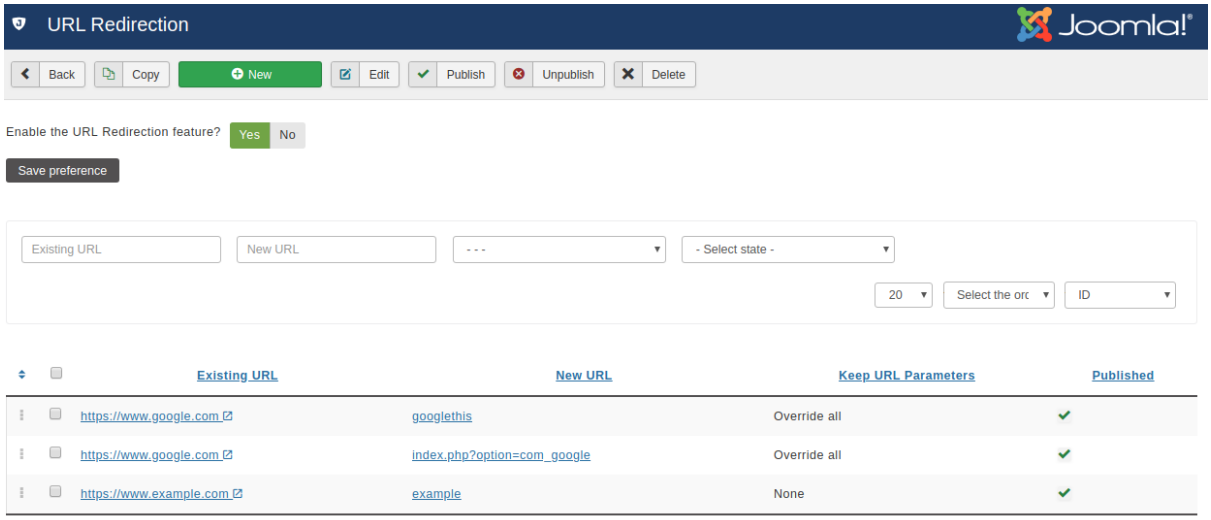
# 13. URL Redirection

#### 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 which Joomla!'s co-founder Brian Teeman calls PEF (Pub Ear Friendly). Arguably, telling someone to visit `http://www.example.com/downloads` is much easier than telling them to visit `http://www.example.com/index.php?option=com_downloads&view=repository&task=list` or even `http://www.example.com/site-resources/download.html`. 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

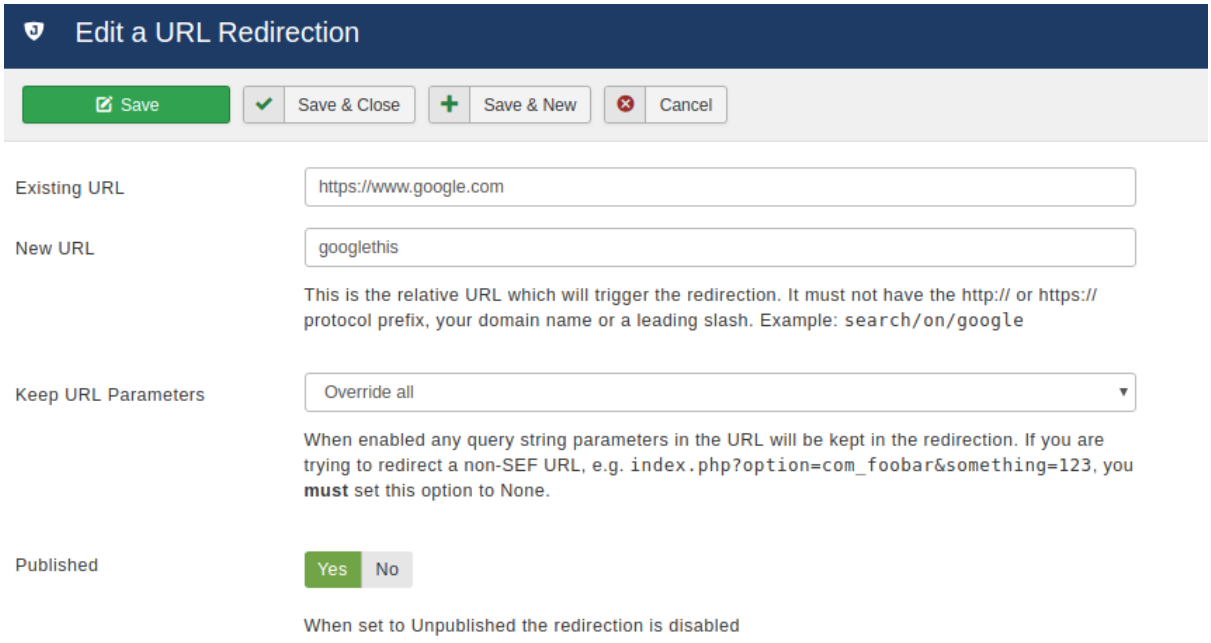



The main administration page shows you a list of the custom URL redirections defined on your sites. Each entry consists of the following information:

- 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/joomla` and this field reads `search/google`, then all requests to `http://www.example.com/joomla/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.
- Order. The order with which the custom redirections will be processed.
- 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




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. For example, putting `index.php?option=com_frontpage` is sufficient to display the front-end component. You can use either an index.php URL or a SEF URL (as long as you have SEF URLs turned on in your Global Configuration!).

  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/joomla`, entering `google` in this field will cause the URL `http://www.example.com/joomla/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`.

  Since Admin Tools 3.3.0 you can redirect internal URLs, which contain index.php. For example you can use `index.php?option=com_foobar&view=abc` to redirect this URL to somewhere else. Pitfalls: you must NOT put your site's URL in front of index.php. Moreover, if someone uses the URL `index.php?option=com_foobar&view=abc&something=else` (additional parameters) or `index.php?view=abc&option=com_foobar` (different parameter order) to access your site the URL redirection will NOT take place.

  If you want to allow additional parameters in an internal URL you can use the form `index.php?option=com_foobar&view=abc%` (note the percent sign at the end) to allow any URL beginning with this text to be redirected. The pitfall is that if you use the format above the URL `index.php?option=com_foobar&view=abcdef` will also be redirected which may not be what you want. In this case you may want to try `index.php?option=com_foobar&view=abc&%` to redirect only URLs which have

view=abc followed by other parameters. You can even place one or more % anywhere in the URL to redirect, for example `index.php?option=com_foobar&view=abc&task=%&%` to redirect URLs of the com_foobar component, abc view and any task followed by zero or more parameters.

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.

If you are trying to redirect a non-SEF URL (a URL with index.php inside it), e.g. index.php?option=com_foobar&something=123, you must set this option to either None or Add New. Otherwise you might end up with a redirection loop. This is not a bug, it's perfectly reasonable. When you allow Overide All and try to redirect from one component (option=com_something) to another (option=com_another) the redirection URL will have its option parameter (com_another) overridden with the old option parameter (com_something). Since you are trying to redirect com_something you end up in a redirection loop which will cause the browser to complain.

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.

Use the Save button to save the changes and go back to the administration page, Save & New to save the changes and start entering the information for a new redirection, Apply to save the changes and return to this editor page and Cancel to discard all changes and return th the administration page.

# 14. Cleaning your temporary files directory

Your Temporary Files directory (called *Temp-directory* in your site's Global Configuration page) is the directory where Joomla! and its extensions put all transient files when installing software or performing other kinds of file manipulation activities. One problem with that directory is that sometimes files can get stuck in it, for example after a failed update. This not only causes a space problem —as these files take up valuable disk space— but can also compromise your site's security as these files may contain potentially sensitive information, or may be executable PHP files. While the latter issue can be usually worked around by using the front-end protection mode in the .htaccess Maker feature of Admin Tools Professional, the proper solution is to periodically clean the contents of that directory.

Admin Tools Core and Admin Tools Professional include the Clean Temp-directory feature which will do that for you with a single click! More specifically, it will automatically remove all files and directories from your Temp-directory except `index.html` and `.htaccess`, if any of those files exists.

### Important

Admin Tools asks Joomla! to tell it where the temporary directory is located and then asks Joomla! to delete its contents. This has a couple of pitfalls:

- Your temporary directory is what you have configured in your site's Global Configuration page, in the Temp-directory option. If you see something like `tmp` or `/tmp` in there please note that it is NOT the

same as the directory inside your site named `tmp`. The directory inside your site is a full path which usually looks like `/home/myuser/public_html/tmp`.

- If your temporary directory is outside your site's root or contains double dots (e.g. `../tmp`) Joomla! will *REFUSE* to delete its contents. This is not a bug in Admin Tools, it's how Joomla! itself is designed to work.

- Being able to delete the contents of the directory depends largely on its permissions. If Joomla! doesn't have browse permissions to this directory it can create temporary files just fine and delete them when it still knows their name (right after creating them), but not when Admin Tools asks it to delete the contents of the temp-directory. The reason is quite technical: Joomla! can't list the contents of the directory, therefore it can't know which files / folders it contains and as a result doesn't know what it has to delete. This is how filesystems work, not a bug in Admin Tools.

- On some servers you may need to use Joomla!'s FTP layer to delete the contents of the temp-directory. We consider this a major indicator of a critically bad server security model. If you are hosted on such a server we strongly advise you to move to a different host or, at the very least, express your concerns to your host. Each site should run under its own user and never, ever, require the FTP layer.

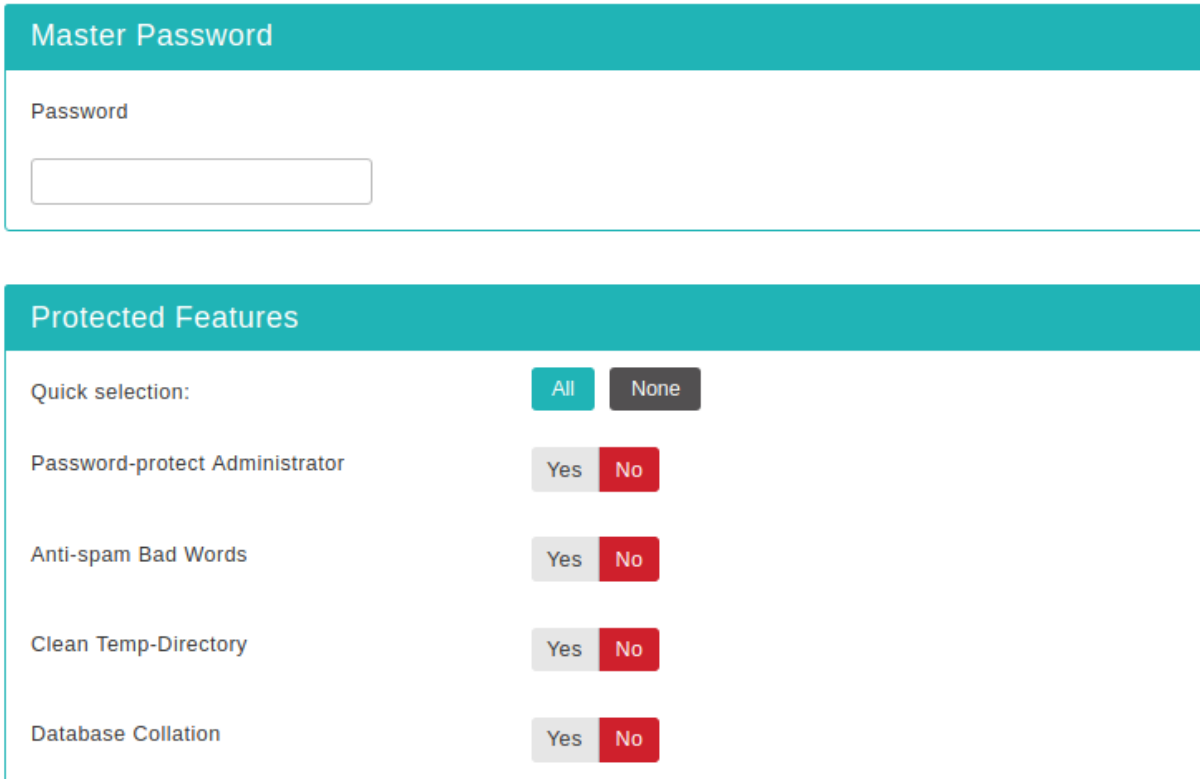
# 15. Protecting Admin Tools with a password

## 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 that could break their own site. THIS FEATURE IS NOT DESIGNED TO PREVENT A MALICIOUS AND/OR KNOWLEDGABLE PERSON 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 back-end access to be able to modify Admin Tool's settings. Instead of giving you the traditional "all or nothing" access control imposed by Joomla! user groups, 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, he has 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 protections, 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 button. Features marked as "No" will be accessible by all back-end users (Managers, Administrators and Super Administrators). Featured marked with "Yes" will only be available to users who enter a valid password in the Control Panel page. This means that even Super 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 jos_admintools_storage table (where *jos_* 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.

# 16. 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

Since Admin Tools 3.1.0 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, .htaccess Maker and NginX Configuration Maker pages |
| IP Blacklist | The permanently blacklisted IP addresses from the IP Blacklist page |
| IP Whitelist | The whitelisted administrator IP addresses from the IP Whitelist page |
| Email templates | All email templates from the Email Templates page |

After selecting what you want to export click on the Export settings button in the toolbar. 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 in the toolbar. The imported settings will overwrite your existing settings.

# 17. Access Control

Joomla! 1.6 and later comes with a very powerful and somewhat complex ACL system on its own. Admin Tools is designed to make full use of it. In order to access the ACL setup, go to Components, Admin Tools and click on the Options button in the toolbar. Then, click on the Permissions tab. Each group can be setup with the following privileges:

| | |
|---|---|
| Configure (the one on top) | Allows access to Component Parameters button. This is a core Joomla! privilege. |
| Access Component | Self explanatory. If a user doesn't have this privilege, he won't be able to access the component! This is a core Joomla! privilege. |
| Utility | The user can use the utility features of Admin Tools. The features affected are: cleaning the temporary directory, component access (Control Panel), Emergency Off-Line Mode, fixing and configuring permissions, URL redirections, SEO and link tools. |
| Maintenance | The user can use the database maintenance features of Admin Tools. The features affected are: session cleanup and table optimization. |
| Security | The user can use the security features of Admin Tools. The features affected are: access control, administrator password protection, Web Application Firewall setup and associated tools (anti-spam bad words filtering, geo blocking, IP white and black list, log view), .htaccess Maker and Master Password. |

We won't go into more details regarding the ACL setup on Joomla! 1.6 and later. If you want more information about how the ACL system works in Joomla! 1.6 and later please consult its documentation or ask on the Joomla! forums.

# 18. The "System - Admin Tools" plugin

## Note

The scheduling features of this plugin are only available in the Professional release. The Core release does need the plugin to be enabled for the SEO and Link Tools features to work.

The "System - Admin Tools" plugin, or `plg_admintools` for short, has a dual role for the Professional release of Admin Tools. On one hand it is necessary for the correct operation of the Web Application Firewall and URL Redirections features of Admin Tools. On the other hand it allows you to schedule various aspects of your site's maintenance.

You can access the plugin's configuration parameters by going to your back-end's Extensions, Plugin Manager menu item. Then find the item System - Admin Tools on the list and click on it. The standard Joomla! plug-in configuration page opens.

On the left-hand side of the administrator area you can find the standard Joomla! controls. First, make sure that Enabled is set to Yes. Then, in order for the plugin to be published in the correct order, select 0 - First from the Order drop-down list.

The plugin options is where all the important functionality can be scheduled. You have the following options:

Rescue URL (Joomla! 3.6 or later only)
: When enabled (default) the Rescue Mode feature is enabled, allowing Super Users with blocked IPs to request a temporary Rescue URL which lets them log into the site and lift the block. We recommend leaving this feature enabled unless you know what you are doing. See the Rescue Mode section for more information.

  ### Important

  You will only receive the email to activate Rescue Mode if your IP is being blocked by Admin Tools. If your IP is NOT blocked by Admin Tools you will NOT receive any email. This is by design. It doesn't make sense to temporarily unblock yourself with Rescue Mode when you are not blocked!

Rescue duration (minutes)
: How long is the Rescue Mode active. This controls two things:

  1. The maximum amount of time between requesting a Rescue URL and visiting it.
  2. The maximum amount of time between visiting the Rescue URL and the end of Rescue Mode.

  We recommend leaving this setting to 15 minutes. Lower values tend to be very impractical.

Email language
: Admin Tools will send you emails to notify you of security exceptions when you enter an email address in WAF Configuration. By default, the current user's language (or your site's default language, if no user is currently logged in) is being loaded, which means that these emails will be sent out in this language. If you have a multilingual website it means that you may receive an email in any language available in your site. This can lead to confusion and makes it nigh impossible to set up any email filters. Therefore we give you this option. You can enter the language tag of the language in which you wish those security exception emails to be sent. For example, typing `en-GB` in this field will cause all emails to be sent out in English. If left blank (default) the current language loaded by Joomla! will be used.

Enable Session Optimizer
: When enabled, the Session Optimizer will be scheduled to run automatically. This feature will repair and optimize Joomla!'s sessions table.

| | |
|---|---|
| Run every X minutes | How often to run the Session Optimizer feature, in minutes |
| Enable Session Cleaner | When enabled, the Session Cleaner will be scheduled to run automatically. This feature will purge (completely empty) and optimize Joomla!'s sessions table. Watch out! This will automatically log all users out of your site! You should only use it on sites where you don't expect to have logged in users at all, e.g. a company presentation site. |
| Run every X minutes | How often to run the Session Cleaner feature, in minutes |
| Enable Cache Cleaner | When enabled, the Cache Cleaner will be scheduled to run automatically. This feature will try to purge (completely empty) Joomla!'s cache. This is not possible on occasions, especially if you are using a cache adapter which doesn't support purging. |
| Run every X minutes | How often to run the Cache Cleaner feature, in minutes |
| Enable Cache Auto-expiration | When enabled, the Cache Auto-expiration will be scheduled to run automatically. This feature will try to expire and delete stale items in Joomla!'s cache. Unlike the Joomla! built-in feature, it will try to run this operation across all caches. This is not possible on occasions, especially if you are using a cache adapter which doesn't support automatic expiration control. |
| Run every X minutes | How often to run the Cache Auto-expiration feature, in minutes |
| Delete inactive users | When this option is enabled, the Admin Tools plugin will automatically delete inactive users, i.e. users who registered on the site but never logged in. On each page load, up to five inactive users will be deleted, to avoid slowing down your site. There are four different options: |

| | |
|---|---|
| Never | Disables this feature |
| Only if they haven't activated their account | Users who have never activated their account will be removed. If they have activated their account they will not be removed. |
| Only if they activated, but never logged in | Users who have activated their account but never logged in will be removed. If they haven't activated their account yet, they will not be removed. |
| Activated or not, as long as they haven't logged in | Any user who hasn't logged in for the number of days specified in the next option will be removed from the site, no matter if he has activated his account or not. |

| | |
|---|---|
| Delete after this many days | How many days must elapse between the registration date of an inactive user and its deletion. For example, if this option is set to 7 then if a user registers on your site on the 1st of the month and has not logged in at least once by the eighth of the month, his user account will be removed. |
| Maximum security exceptions log entries | 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.

All expiration options are best-effort scheduled. This means that they will try to run every X minutes, but only as long as there is visitor traffic to trigger them. In any other case they will defer their execution for when there is visitor traffic.

# 19. Rescue Mode

## Overview

Sometimes an overzealous Admin Tools configuration can result in accidentally blocking yourself, a Super User, from the site. Normally that would require you to rename the `main.php` file of Admin Tools' system plugin to unblock yourself. This can be rather daunting for novice site administrators.

The Rescue URL feature works around that problem in a secure and elegant manner. First you visit a special URL, including your Super User email address. An email is sent to you with a "magic" link called the Rescue URL. Clicking on that link lets you log in to your site's administrator area without Admin Tools' protections getting in your way. You can then unblock yourself and / or modify the Admin Tools configuration which caused your IP address to be blocked in the first place.

## How to use the Rescue Mode

### Important

Rescue Mode is only available on sites running Joomla! 3.6.0 and later and Admin Tools 4.3.0 or later. Also note that if you are not the only Super User on your site, or if you used another company / freelancer to build your site, it's possible that they have turned off Rescue Mode. If these instructions don't work you should assume Rescue Mode is not available or disabled on your site.

Assuming that your site's URL is *`http://www.example.com`* and your Super User email address is *`you@example.com`* you need to visit the following URL to request a Rescue URL to be sent to you:

*`http://www.example.com`*`/administrator/index.php?`
`admintools_rescue=`*`you@example.com`*

You will see the message "Check your email for Rescue URL information" printed on your screen.

Check your email. You will receive an email from your site with a Rescue URL.

### Important

You will only receive the email to activate Rescue Mode if your IP is being blocked by Admin Tools. If your IP is NOT blocked by Admin Tools you will NOT receive any email. This is by design. It doesn't make sense to temporarily unblock yourself with Rescue Mode when you are not blocked!

The Rescue URL looks like this:

*`http://www.example.com`*/administrator/index.php?
admintools_rescue_token=4vJPFH8pkpFdVkjz0Ej7VUi6gUt39lmkMS36sjmQV6hCTZZ36b2snqWVY6PrxqHdvyb4B3DI8VSUy

Do note that the part after admintools_rescue_token is very long and completely random. Also note that it's only valid for use from the SAME browser and IP address that you requested a Rescue URL to be sent to you. The link is only valid for a short period of time (default: 15 minutes). All of that is done for security reasons!

Visit the Rescue URL either by clicking on it or by copying it and pasting it to your browser's address bar. If all goes well you will see your site's administrator backend login page or the Joomla! administrator control panel. If you see the login page just log in with the Super User account which corresponds to the email you used when requesting a Rescue URL to be sent to you.

### Tip

If you were logged in as a different Super User account you will still be blocked. You will need to repeat this process using the email address of the Super User account you were logged in with on your site. Alternatively, use your browser's Private Browsing mode to request and visit the Rescue URL.

Now you can go to Components, Admin Tools and unblock yourself. Remember that you have a limited period of time (default: 15 minutes) for security reasons!

### Tip

Don't know how to unblock yourself? No problem! Going to Components, Admin Tools you'll see a message with a link to step by step instructions.

# Rescue Mode and security

Rescue Mode was designed with security in mind. There's no point having a security extension if there's an easy backdoor to it! We have ensured security by taking several measures.

First and foremost, the Rescue Mode only applies to the administrator backend. The frontend of your site is not affected. This means that nobody can abuse it to subvert Admin Tools' protection of your public site.

When you are requesting a Rescue URL you must be already blocked from accessing the backend of the site and know the Super User's email address. If your backend login page is protected by a .htaccess password (a.k.a. Administrator Password Protection) you will need to supply that before the request has any effect.

A very long (96 random alphanumeric character), single use, limited validity time (default: 15 minutes) token is generated when you make the request. This has about 160 bits of randomness which means that there are more than 1,460,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 possible combinations. This is practically impossible to guess. Moreover, it's stored hashed using the same technology as your Joomla Super User password to prevent side-channel attacks, i.e. an attacker using a possible vulnerability in any part of your site / server to perform an unauthorized read of database information.

The token itself can only be used by the same browser and IP address that requested the Rescue URL. This means that phishing attacks wouldn't work. An attacker cannot fool you into opening a backdoor to your site for them. In fact, a potential attacker would need full access to your email to pull of an attack. Of course if they have full access to your email account they can do far more dangerous things, like having your hosting company hand over control of the domain to them, i.e. you'd be thoroughly hacked. Therefore the email portion of Rescue Mode does not constitute a viable attack vector.

When you visit the Rescue URL the token is immediately invalidated (it cannot be used again) and data is written to your session. This data is what acts as a temporary key to disable Admin Tools' protections only for you and only for the site's administrator. Furthermore you MUST log in, or already be logged in, with the same Super User as the one whose email you used when requesting a Rescue URL. If you try to log in with a different user the Rescue Mode is immediately canceled.

The Rescue Mode only temporarily disables Admin Tools' security checks. It does not remove Joomla's own security checks or any third party extensions. Therefore if you are using Two Factor Authentication / Two Step Authentication to verify your login it will still be required for you to log in to your site. This means that even in the unlikely event of you being fully compromised (including control of your email account AND your Super User username and password) the attacker would still be stumped by Two Factor Authentication.

Furthermore, the Rescue Mode is only active for a limited amount of time (default: 15 minutes) since you access the Rescue URL. This means that even if you use a loaner computer you won't end up with a browser that has a backdoor to your site's login page. We also include a button in the Admin Tools control panel page to immediately end Rescue Mode -even if it's not expired- for additional control and security.

Finally, Rescue Mode is opt-out. This means that you can disable it by editing the System - Admin Tools plugin options and setting the Rescue URL option to No.

# Discoverability and message customization

Features like this are useless if they are simply buried in the documentation. Admin Tools displays information about the Rescue URL in three places, **as long as you have not modified the default options**.

First on all, when a security exception is raised the visitors see a message informing them they did something they shouldn't have done. You can customize this in the Configure WAF page, Security Exception Message Customisation tab, Custom Message option. If that option is left blank the default message generated by Admin Tools contains information about unblocking yourself.

The second place where this is displayed is the message shown to blocked IPs. You can customize that in the Configure WAF page, Auto-ban Repeat Offenders tab, Show This Message To Blocked IPs option. If you leave this blank or if you use the default message ("You are a spammer, hacker or an otherwise bad person.") the information about unblocking yourself will be appended to the end of the message.

Moreover, Admin Tools will automatically append the information about unblocking yourself to the default content of the security exception and IP auto-ban emails (i.e. reasons `all` and `ipautoban`) shipped with Admin Tools. You can customize these emails from the Web Application Firewall, Email Templates page.

If you customize these messages and / or emails you can instruct Admin Tools to include the default Rescue URL information by adding the code [RESCUEINFO] in all caps, including the brackets, anywhere in the two messages or the body of the email templates. The rescue info typically reads something like:

If you are the administrator of this site and have blocked yourself on accident please visit https://www.example.com/administrator/index.php?admintools_rescue=you@example.com where you@example.com is the email address of your (Super User) account.

You can customize this information message by creating a standard Joomla! language override [https://docs.joomla.org/J3.x:Language_Overrides_in_Joomla] for the translation string `ADMINTOOLS_BLOCKED_MESSAGE_RESCUEINFO`.

### Important

For security reasons, we strongly recommend that you change the Custom message and Show This Message To Blocked IPs messages described above to NOT include any reference to Admin Tools and / or the procedure to unblock yourself. You MUST NOT tell the world how you are protecting your site. Not disclosing this information is yet another hurdle for a potential attacker, making it less likely that they will spend time to attack your site.

# 20. Other plugins

## 20.1. The plugins powering the One Click Update feature

### Note

This feature is only available in Admin Tools Professional, the for-a-fee edition of our software

Admin Tools Professional can send you e-mails to remind you of available updates to itself or to the Joomla! CMS. By default, when a new version is detected, it will send an email to all Super Administrators on your site notifying them of the available update. Even better, it goes one step further than simply notifying you of the availability of the new version. Clicking on the link found in the update notification email you are automatically taken to your site and forwarded to the relevant update page (Joomla! Update for Joomla! CMS updates and Admin Tools' Live Update page for Admin Tools updates), which starts installing the new version automatically.

### Important

Since Admin Tools 2.6.1 the update URL does not log you in to your site. You will need to enter your login information in the login page of your site's administrator area before the update proceeds.

If you want you can OPTIONALLY enable the automatic log in feature in the email plugins' parameters. However you are discouraged from doing so as it can be a security risk. In order for the automatic log in feature to work the System - One Click Actions plugin must also be activated.

The update emails are sent by two plugins:

- The System - Admin Tools Update Email plugin will send you e-mails for Admin Tools updates
- The System - Admin Tools Joomla! Update Email plugin will send you e-mails for updates of Joomla! itself

Update checks will be performed periodically, without having you to log in to your site's back-end. These checks will be performed as long as your site receives about page views every day at a minimum.

### Tip

Since Admin Tools Professional 2.4.4 you can specify *just one* Super Administrator to be emailed. In order to do that please go to Extensions, Plug-in Manager and click on the System - Akeeba Backup Update Check entry from the list. You have two options:

| | |
|---|---|
| Email language | On multi-lingual websites this forces the email to be sent in a specific language. Enter the language code you want, e.g. en-GB for English (Great Britain), de-DE for German, fr-FR for French, es-ES for Spanish (Spain) and so on. |
| Super Admin Email | Enter the email address of a Super Administrator. The email you enter must match the email address set up in the user profile of an *existing* Super Administrator on the site. If it's left blank (default) all Super Administrators will be emailed when an update is found. If it's invalid or doesn't belong to an existing Super Administrator then no email will be sent. |

# 21. The CLI update notification and automatic update script

### Note

This feature was removed in May 2017.

The automatic update script was removed in May 2017 due to massive bugs in Joomla! 3.7. These bugs broke all CLI scripts which make direct or indirect use of the JSession package, including simply checking if a user is logged in. This includes the update script. It cannot be fixed because the update script uses the core JUpdater and JInstaller APIs to fetch and install updates. Both of them use JSession which means they cannot be used from a CLI script.

The only thing we can do is remove a feature which can no longer work because Joomla! broke backwards compatibility with itself.

# Appendix A. GNU General Public License version 3

Version 3, 29 June 2007



## 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



## 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. Secondarily, 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.