Step by step guide

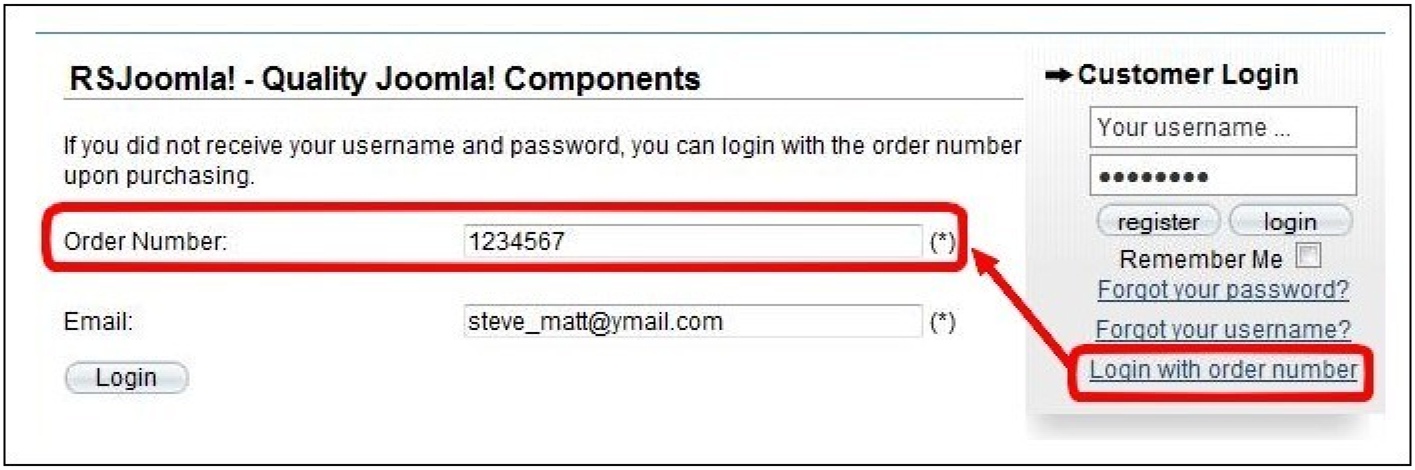
Step 1: Purchasing a RSFirewall! membership

When you purchase a membership for the first time, a **RSJoomla!** account is automatically created for unregistered users, after the purchase has been approved, based on the filled in data. The transaction along with the user details are sent in the registration email.

Upon transaction, users have 2 ways of accessing the www.rsjoomla.com account and download RSFirewall!:

1. Login with the user and password automatically created and sent through email, during the transaction process, using the **Customer Login** form.
2. Login with the order number received on the user email.

Login with the order number



RSJoomla! - Quality Joomla! Components

If you did not receive your username and password, you can login with the order number upon purchasing.

Order Number: 1234567 (*)

Email: steve_matt@ymail.com (*)

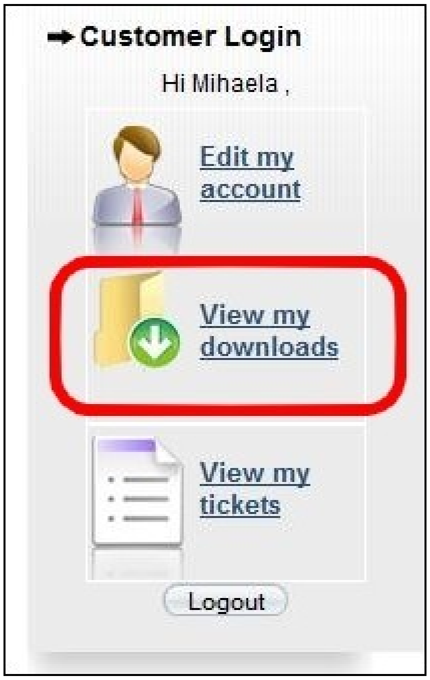
Step 2: Download RSFirewall!

2.1. Download the component

To download RSFirewall! you need to:

Step 1: login on www.rsjoomla.com with the user details or the order number received on email.

Step 2: in the right side, you will find a section dedicated to RSJoomla! customers: **Customer Login.** Click on **View my downloads**



➡ Customer Login

Hi Mihaela ,

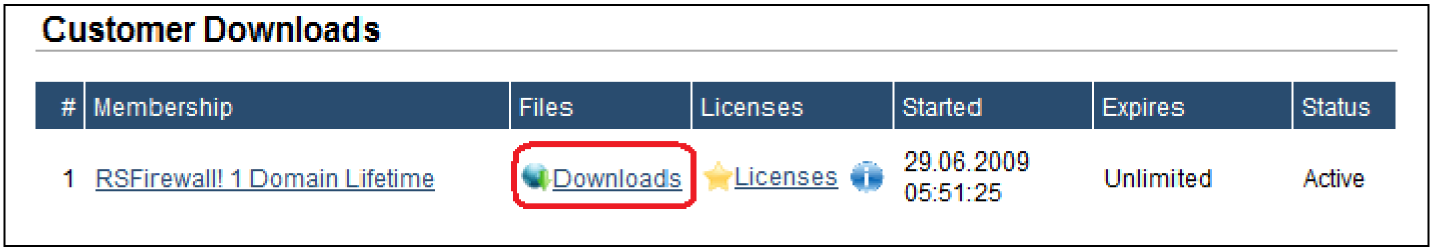
Edit my account

View my downloads

View my tickets

Logout

Step 3: In the **Customer downloads** section are listed all the user's memberships. Click on ***Downloads >> RSFirewall! Files >> Component >> Download RSFirewall! for Joomla! 1.5***

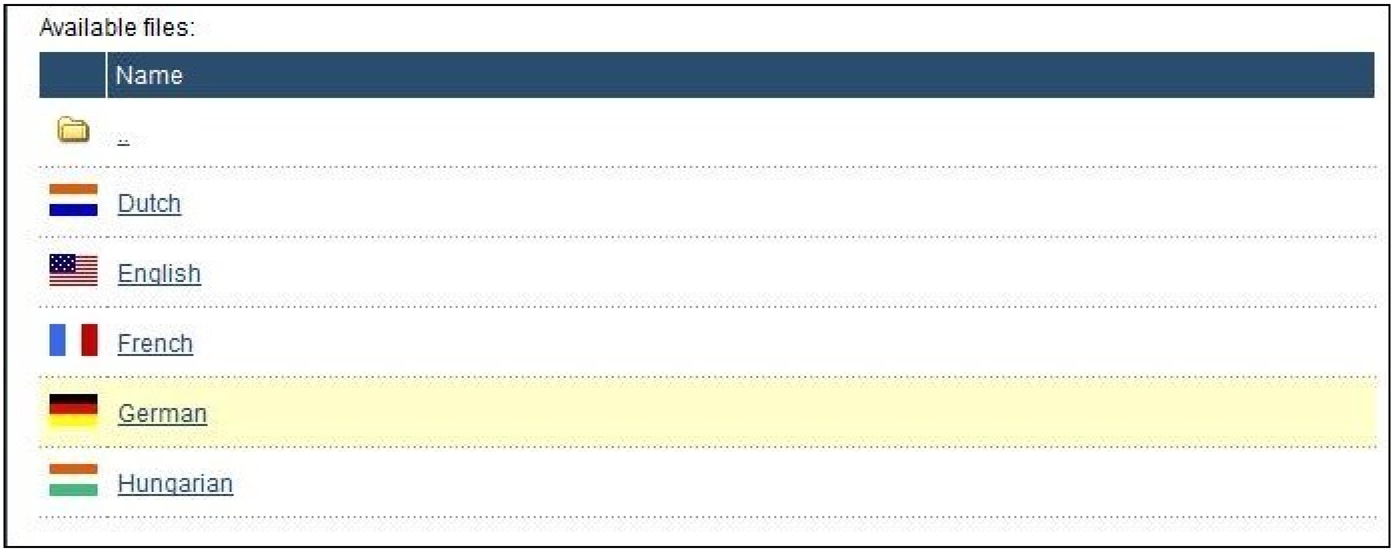


Customer Downloads

#	Membership	Files	Licenses	Started	Expires	Status
1	RSFirewall! 1 Domain Lifetime	Downloads	⭐Licenses ⓘ	29.06.2009 05:51:25	Unlimited	Active

2.2. Download RSFirewall! language files

Additionally, if you need RSFirewall! translated in other languages, you can download the available RSFirewall! language files from ***Customer Downloads >> RSFirewall! Files >> Languages*** or create your own language files



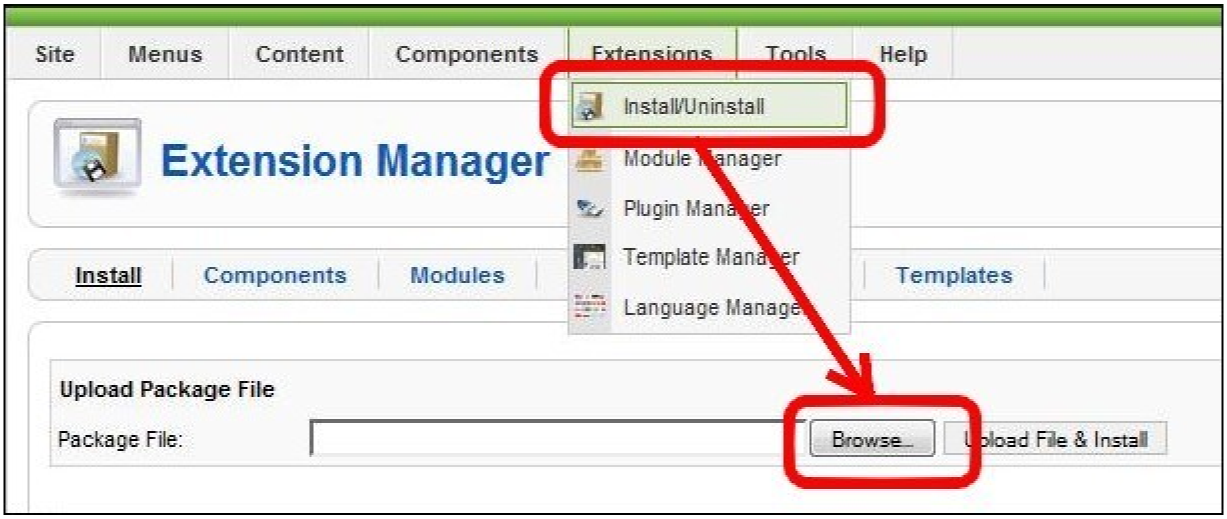
Available files:

	Name
	..
	Dutch
	English
	French
	German
	Hungarian

Step 3: Installing RSFirewall!

3.1. Installing the component

RSFirewall! installs like any other component - trough the default Joomla! installer.
In the backend panel, head to ***Extensions >> Install/Uninstall >> Browse RSFirewall! from your computer >> Upload File & Install.***



3.2. Installing the language files

The language files are installed using the same method as for the component - trough the default Joomla! installer (see the above screenshot), the only condition in order to work is to have previously installed the Joomla! languages pack for frontend and backend.

1. **Install the Joomla! languages pack** (if there aren't already installed): **a.** Head to Joomla! language packs area and choose the desired translation. **b.** Download the corresponding Joomla! languages pack for frontend and backend. **c.** Install the Joomla! languages pack (regular installation trough the Joomla! installer): in the backend panel head to ***Extensions >> Install/Uninstall >> Browse the Joomla! language files >> Upload and Install*** **e.g.** If you want to use RSFirewall! in Dutch, first install the Dutch Joomla! languages pack for frontend and backend, from http://joomlacode.org
   nl-NL_joomla_lang_site.1.5.20.zip
   nl-NL_joomla_lang_admin.1.5.20.zip
2. **Install the RSFirewall! languages pack:** (regular installation trough the Joomla! Installer)

a. Download the RSFirewall! language files from www.rsjoomla.com - Customer Downloads (see **Step 2.2 Download RSFirewall! language files**)
b. In the backend panel, head to ***Extensions >> Install/Uninstall >> Browse the RSFirewall! language files >> Upload***

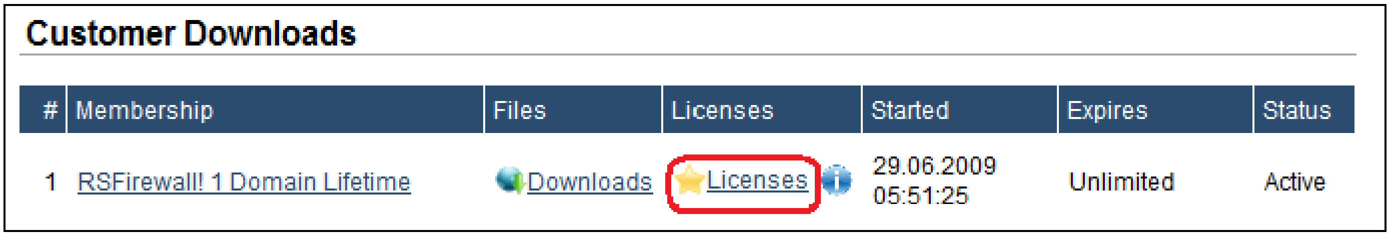
Step 4: Update RSFirewall! to a newer version

RSFirewall! has an *"Updates"* tab, especially designed to smooth the update process.
There are 2 ways to update the RSFirewall! component:

- **4.1 - using the "Updates" tab :**

To be able to receive updates directly in the Joomla! backend panel, you need to enter the RSFirewall! license codes.

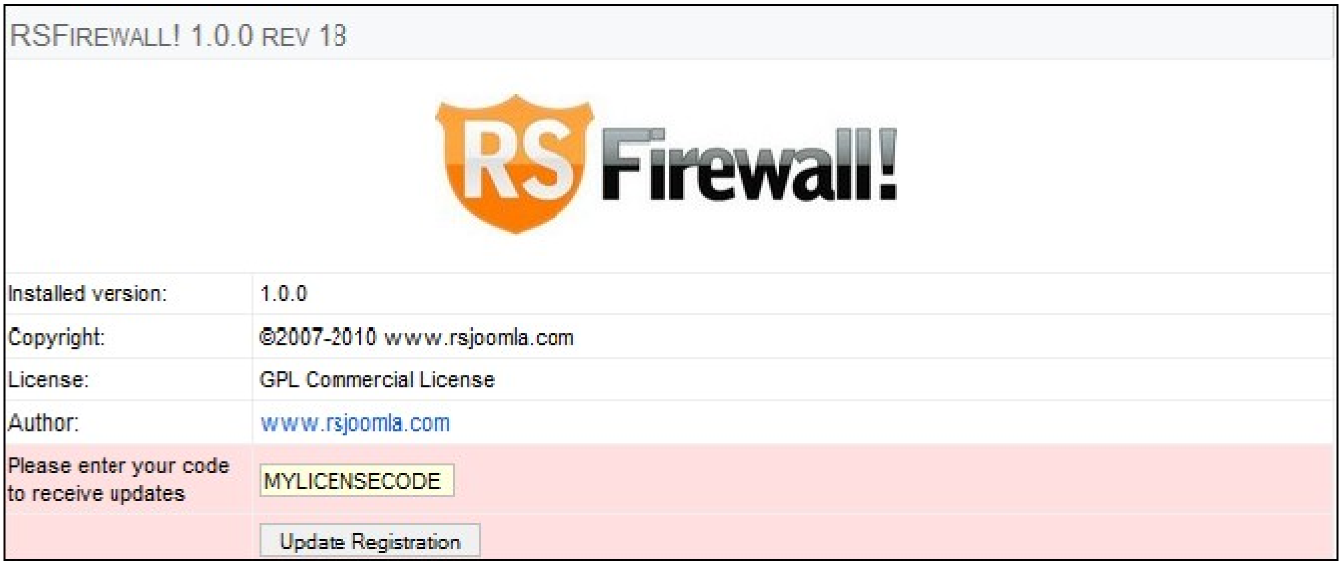
Step 1:
To get this license code, login to your RSJoomla! account and in the Customer Downloads section click on the Licenses link.



Customer Downloads

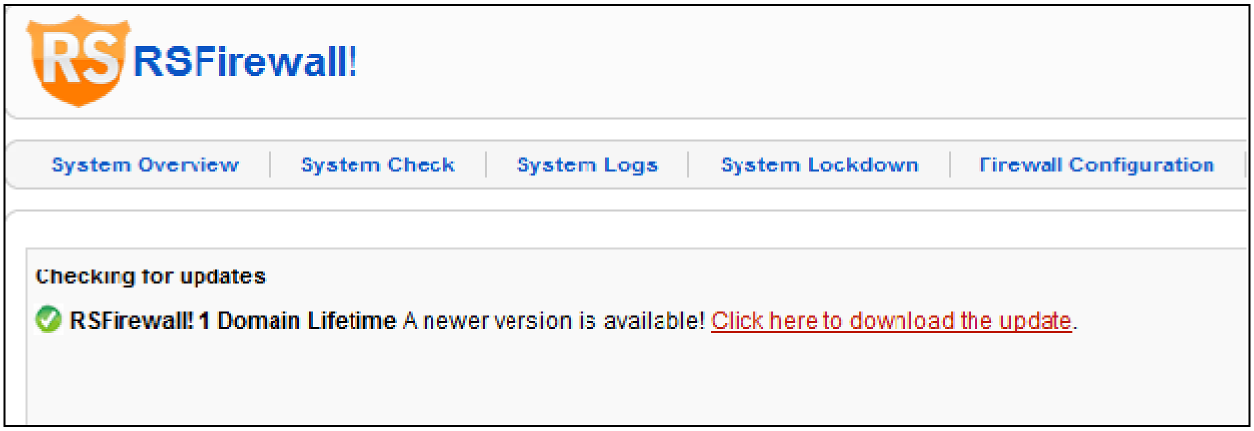
#	Membership	Files	Licenses	Started	Expires	Status
1	RSFirewall! 1 Domain Lifetime	Downloads	Licenses	29.06.2009 05:51:25	Unlimited	Active

Step 2:
After entering the domain name, a license code is generated.
Copy the license code and paste it in the RSFirewall! control panel from the backend Joomla!


RSFIREWALL! 1.0.0 REV 18

Installed version:	1.0.0
Copyright:	©2007-2010 www.rsjoomla.com
License:	GPL Commercial License
Author:	www.rsjoomla.com
Please enter your code to receive updates	MYLICENSECODE

Step 3:
Whenever you want to check new RSFirewall! updates, head to ***Components >> RSFirewal! >> Updates*** and you will be able to download the component directly from the backend.



Checking for updates

✓ **RSFirewall! 1 Domain Lifetime** A newer version is available! Click here to download the update.

- **4.2 – using the default Joomla! installer:** download RSFirewall! from your RSJoomla! account - *View my downloads.*

In the Joomla! backend panel head to ***Extensions >> Install/Uninstall >> Browse the RSFirewall! pack >> Upload.***

⚠ **Notice:**

- To simplify the update process and receive updates, we recommend to enter your license code generated in your RSJoomla! account and then follow the step **4.1 - using the "Updates" tab**.

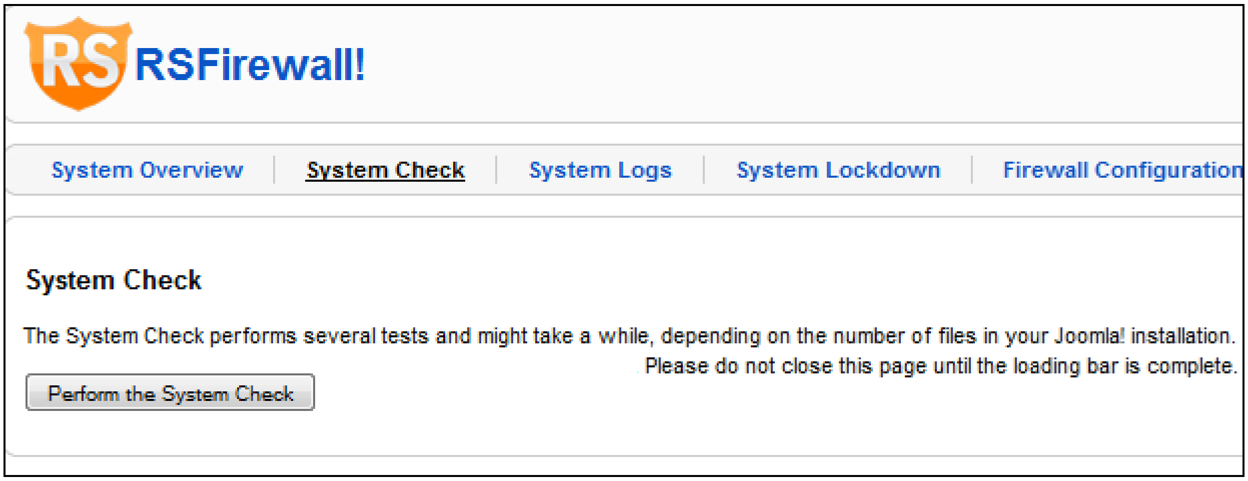
Step 5: Scan the Joomla! installation

5.1 System Check

Path: ***Joomla! backend panel >> Components >> RSFirewall! >> System Check***

5.1.1 The "System Check"

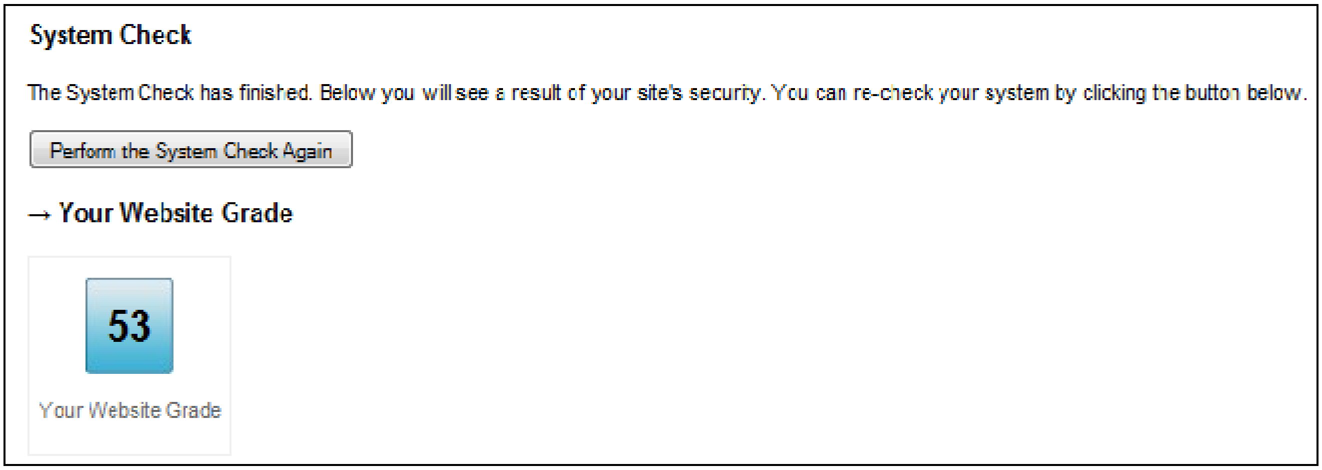
Here you can start the System Check, by clicking on the "Perform System Check" button on the page.



System Check

The System Check performs several tests and might take a while, depending on the number of files in your Joomla! installation. Please do not close this page until the loading bar is complete.

The **System Check** is an on-demand scanner that performs an extensive scan of your Joomla! installation. This scanner verifies the following items: RSFirewall! and Joomla! versions, File integrity, Folder permissions, File permissions, Malware patterns, PHP configuration, User information, Jumi check and Joomla! Configuration.



System Check

The System Check has finished. Below you will see a result of your site's security. You can re-check your system by clicking the button below.

5.1.2 System Version Check

1) Checking if you have the latest version of RSFirewall! installed

It's essential that you have the latest RSFirewall! version installed on your Joomla! website. RSFirewall! alerts you when a new version has been released. You can check this by:

- going to Administrator » Site » Control Panel(you'll see on the right a brief system information which also shows the current RSFirewall! version)
- performing a System Check that will tell you if a new version is available.

“You are using the latest version of RSFirewall!”

If you see this message, then your RSFirewall! version is up to date. We are constantly updating the software and add new vulnerability information etc. We advice you to perform a system check periodically, at least once every two weeks.

“You are using an older version of RSFirewall!”

It's important to have the latest RSFirewall! version installed. The update can be made easily within seconds, so make sure that your RSFirewall! version is always up to date. In order to update the component you can see **Step 4: Update RSFirewall! to a newer version.**

2) Checking if you have the latest version of Joomla! installed

It is best to have the latest version of Joomla! Installed on your site. Keeping your Joomla! Installation always updated to the latest version ensures that you also have the latest Joomla! security updates and also an improved functionality of your site. You can verify this by:

- looking in the top-right corner of your screen where the Joomla! version is usually displayed.

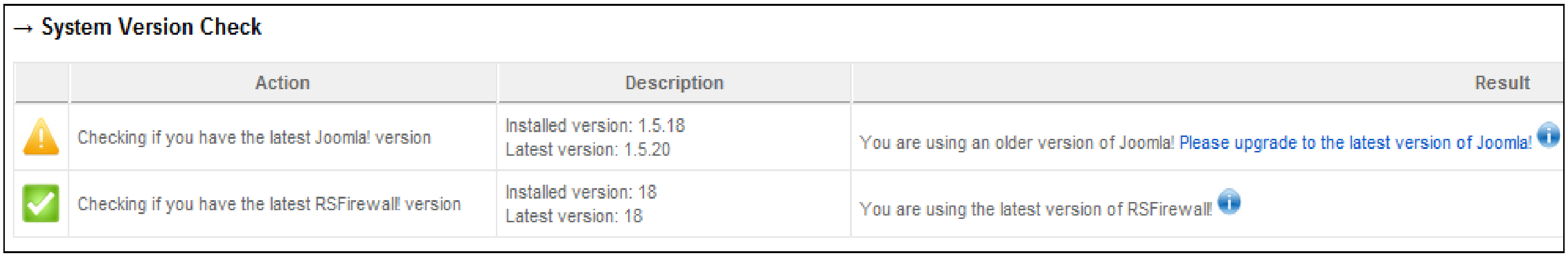
- going to Administrator » Site » Control Panel and verify the RSFirewall! Module.
- performing a System Check that will tell you if a new version is available.
- Going to Help > System Info and the Joomla! Version will be displayed.

“You are using the latest version of Joomla!”

If you see this message, then your Joomla! version is up to date. It is best to constantly verify if new updates are available for Joomla! and apply them as soon as they are available.

“You are using an older version of Joomla!”

It's important to have the latest Joomla! version installed. The update can be made easily within seconds, so make sure that your RSFirewall! version is always up to date. In order to update Joomla! you can see http://docs.joomla.org/Upgrade_Instructionse.



→ System Version Check

	Action	Description	Result
⚠	Checking if you have the latest Joomla! version	Installed version: 1.5.18 Latest version: 1.5.20	You are using an older version of Joomla! Please upgrade to the latest version of Joomla! ⓘ
✓	Checking if you have the latest RSFirewall! version	Installed version: 18 Latest version: 18	You are using the latest version of RSFirewall! ⓘ

5.1.3 File Integrity Check

The RSFirewall! System Check does a complete Joomla! file system scan. The File Integrity Check verifies if the core Joomla! files from your installation are either modified or missing. It is best to do not modify any core Joomla! files as this will increase the time needed to update your installation. If you however wish to modify the core then it will be recommended to keep track of the modifications in order to know which changes to accept and which to not.

The file has been modified

The scanner checks if each Joomla! file is intact. If a file has been changed it will be listed in the **File Integrity Check** report with the *The file has been modified* error message. You can download the original file from the Joomla! installation package and replace the modified files if you are unaware of the changes.

Tip:

- Never download Joomla! files and packages from untrusted websites. They may contain malware that compromise your website security.
- You shouldn't modify the Joomla! core files. It takes much more time to update your website when a new Joomla! version is out. You should use modules, plugins and templates to customize the looks and functionality of your Joomla!.
- If you have just updated your Joomla! installation and RSFirewall! points out that many Joomla! files are modified then please make sure

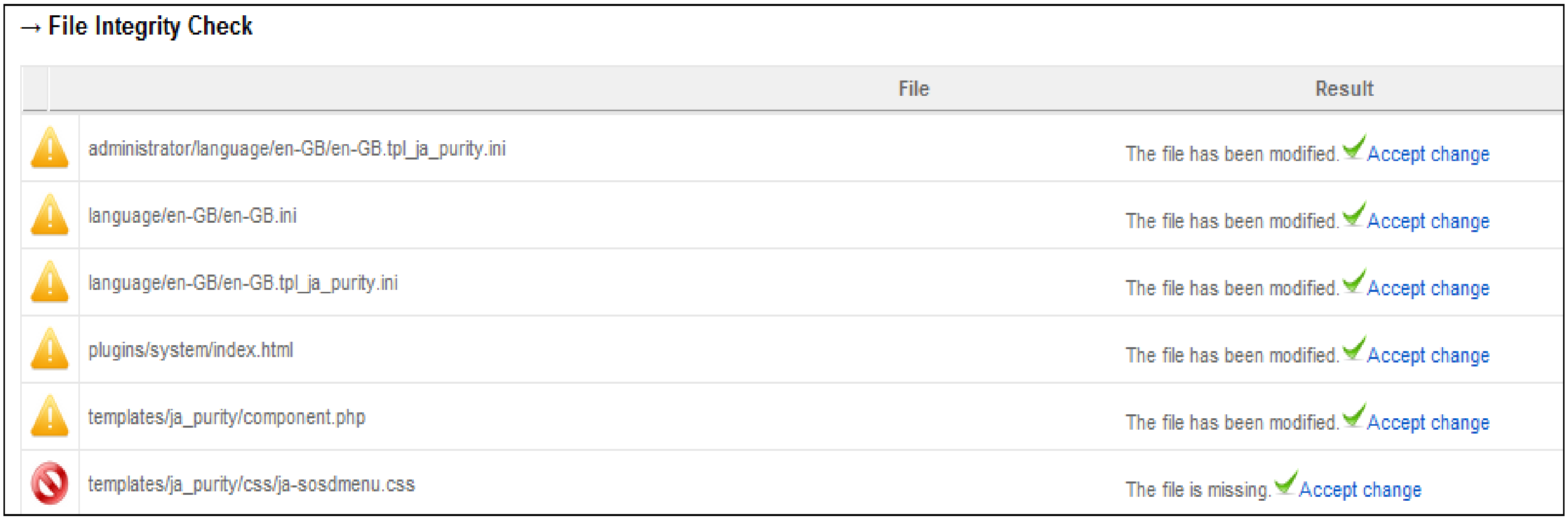
The file is missing

Missing files can compromise your Joomla! website so it's essential that you have them all. RSFirewall! scans all your Joomla! files for changes. If a file is not found it will be added in the **File Integrity Check** report. You are able to see a list of missing and corrupt files.

Tip:

- Never download Joomla! files and packages from untrusted websites. They may contain malware that compromise your website security.

RSFirewall! also gives you the possibility of downloading a copy of the missing/modified file from our server directly. You will have to upload it manually on your Joomla! Installation.



→ File Integrity Check

	File	Result
⚠	administrator/language/en-GB/en-GB.tpl_ja_purity.ini	The file has been modified. ✓ Accept change
⚠	language/en-GB/en-GB.ini	The file has been modified. ✓ Accept change
⚠	language/en-GB/en-GB.tpl_ja_purity.ini	The file has been modified. ✓ Accept change
⚠	plugins/system/index.html	The file has been modified. ✓ Accept change
⚠	templates/ja_purity/component.php	The file has been modified. ✓ Accept change
⛔	templates/ja_purity/css/ja-sosdmenu.css	The file is missing. ✓ Accept change

5.1.4 File and Folder Permissions Check

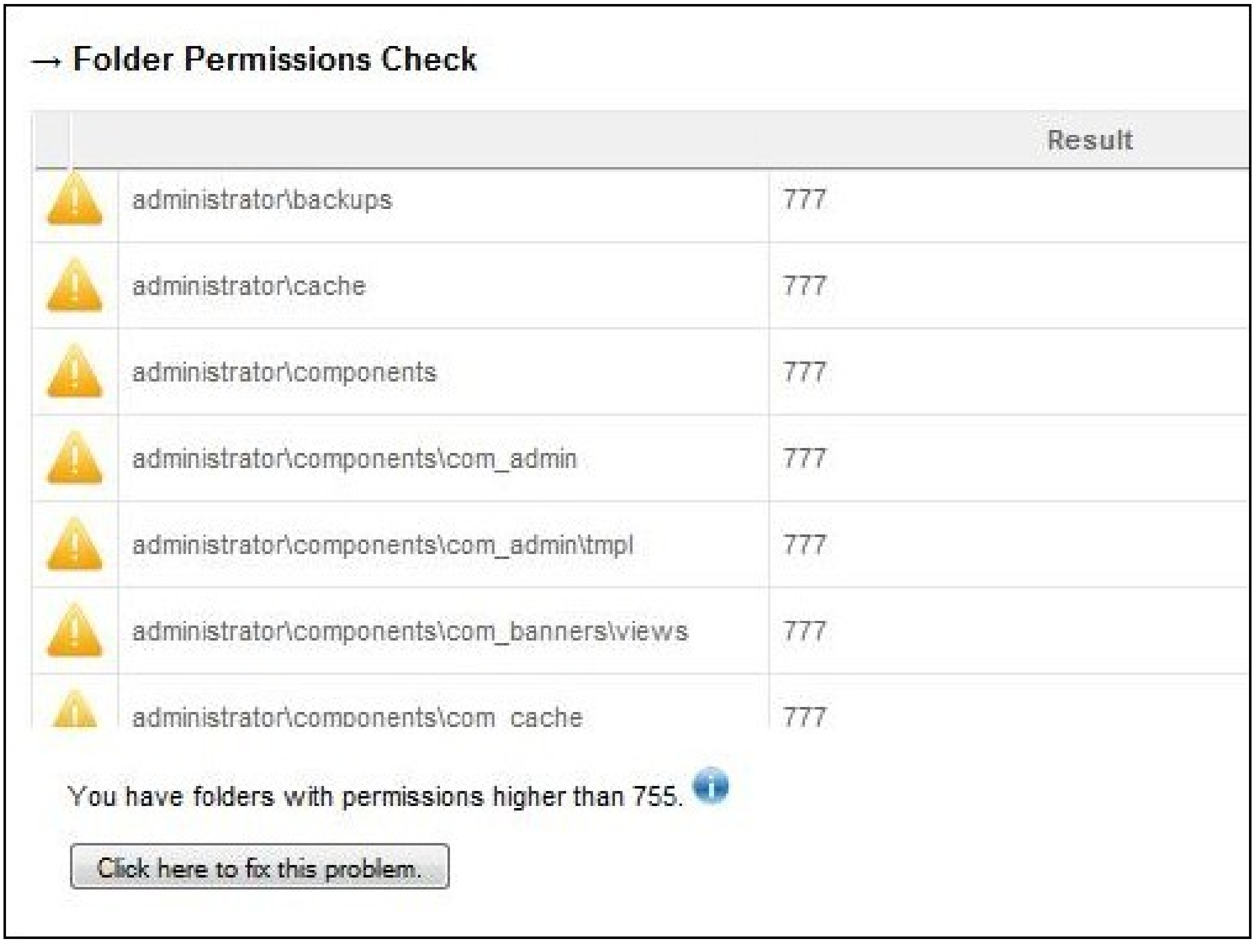
The Permissions Check will verify if you have secure permission for all your files and folders.

Folder Permissions Check - You have folders with permissions higher than 755

The **Folder Permissions Check** will alert you which folders in your Joomla! installation have permissions greater than 755. Folders should have 755 permissions and not 777(writable by anyone) in order to deny any attempt of creating new files or modifying the existing ones.

It's common practice in Joomla! to set folder permissions to 777 (maybe because you want to install something, or simply want to upload some files) and forget to turn them back to 755.

This tool will help you identify the folders that you need to fix.



→ Folder Permissions Check

		Result
⚠	administrator\backups	777
⚠	administrator\cache	777
⚠	administrator\components	777
⚠	administrator\components\com_admin	777
⚠	administrator\components\com_admin\tmpl	777
⚠	administrator\components\com_banners\views	777
⚠	administrator\components\com_cache	777

You have folders with permissions higher than 755.

Tip:

- RSFirewall! offers the possibility to automatically change folder permissions to 755. Please note that this function will work only on servers that allow changing permissions.

File Permissions Check - You have files with permissions higher than 644

The **File Permissions Check** scans all your Joomla! files and checks that they have the appropriate permissions. If you get the *You have files with permissions higher than 644* message, then the listed files permissions must be fixed.

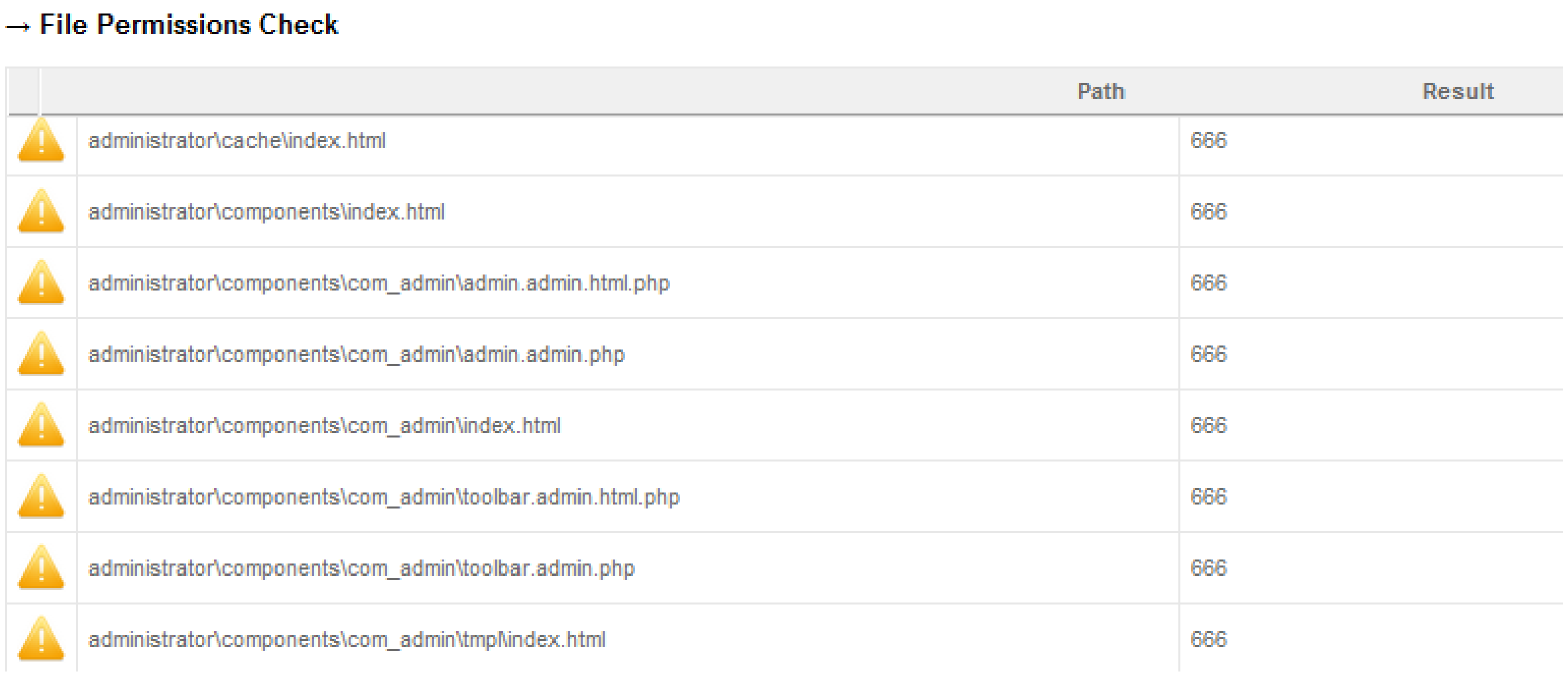
How to change permissions to files?

RSFirewall! has a button *Click here to fix this problem* that will change file permissions automatically. However this feature will not work on servers that do not allow changing permissions

If your server doesn't allow it, you should use your FTP client to change the permissions. Most FTP clients have this feature. All you have to do is to right click on the file and look for Change Permissions or something like that.

Notice:

- This tool is very useful because it gives you all the files that have wrong permissions on your site.
- Leaving writable permissions to files and folders allow hackers to create, modify and upload files to your server. Fixing the file and folder permissions will help reducing the risk of your site being hacked.

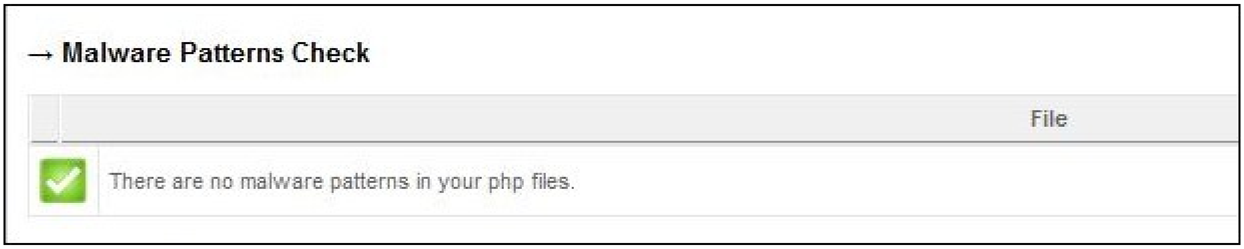


→ File Permissions Check

	Path	Result
⚠	administrator\cache\index.html	666
⚠	administrator\components\index.html	666
⚠	administrator\components\com_admin\admin.admin.html.php	666
⚠	administrator\components\com_admin\admin.admin.php	666
⚠	administrator\components\com_admin\index.html	666
⚠	administrator\components\com_admin\toolbar.admin.html.php	666
⚠	administrator\components\com_admin\toolbar.admin.php	666
⚠	administrator\components\com_admin\tmpl\index.html	666

5.1.5 Malware Patterns Check

The malware scripts are common php scripts that tend to exploit your installation. Once a hacker has managed to upload this type of file on your server, it can gain complete control of the server withing seconds.



→ Malware Patterns Check

	File
✓	There are no malware patterns in your php files.

There are no malware patterns in your php files

This message indicates that no dangerous scripts have been found on your server. However we advice you to periodically check your Joomla! using the System Check.

You have malware patterns in your files

If you see this message, your server is probably been hacked and you need to take immediate actions.

RSFirewall! will list all the malware scripts found and you will also have the possibility to quickly clean these files. However, on some servers this feature will not work. In this case you will have to remove the files manually.

⚠ **Tip:**

- The easiest way of getting a malware uploaded on your server is to allow forums or other file uploaders to load php files. RSFirewall! Active Scanner blocks automatically file extensions that are considered dangerous.

5.1.6 File and Folder Access Check

The File and Folder Access Check checks for the following:

1) Checking if the Joomla! temporary folder is outside of public html

Joomla! has a temporary folder that is mainly used when installing extensions. You can set the temporary folder from ***Administrator >> Site >> Global Configuration >> Server >> Server Settings >> "Path to Temp-folder"***. When this verifications is made you can receive one of the following results:

The Joomla! temporary folder is accessible through the public html

This message comes out if the temporary folder is accessible through your website. The default Joomla! temporary folder is located in *http://yoursite.com/tmp*. Even if it's not a potential threat, it's better to set the temporary folder outside the public html folder.

The Joomla! temporary folder is outside of public html

Setting the temporary folder out of the public access enforces your website, since no one can access the files inside.

⚠ **Tip:**

- Setting a temporary folder outside of the public html is easy. Just use your ftp client, access the folder that is on top of the public_html(or www or htdocs on some servers) and create a new folder there. Then, go to Administrator » Site » Global Configuration » Server » "Path to Temp-folder" and set it to point to that folder.

2) Checking if the log folder is outside of public html

You can configure a log folder inside your Joomla! installation. This is where the Joomla! logging data is stored. The log folder can be configured from Administrator >> Site >> Global Configuration >> System >> “Path to Log folder”. During this check, you can receive one of the following results:

The Joomla! log folder is accessible through the public html

This message comes out if the log folder is accessible through your website. The default Joomla! log folder is located in *http://yoursite.com/logs*. Even if it's not a potential threat, it's better to set the log folder outside the public html folder.

The Joomla! log folder is outside of public html

Setting the log folder out of the public access of your website is a good idea, since no one can access the files inside.

Tip:

- Setting a log folder outside of the public html is easy. Just use your ftp client, access the folder that is on top of the public_html(or www or htdocs on some servers) and create a new folder there. Then, go to Administrator » Site » Global Configuration » System » “Path to Log folder” and set it to point to that folder.

3) Checking if there are any files left in the Joomla! temporary folder

Whether the temporary folder is accessible or not through the public html, it's best to keep the temporary folder empty. The temporary folder is used by Joomla! when installing extensions. Some do not install properly, and files are left there. When running this check the following results can be returned:

There are files in the Joomla! temporary folder

Your Joomla! temporary folder contains files. You can easily delete the files from the temporary folder by clicking on the “Empty temporary folder” button from the File and Folder Access Check. This way RSFirewall! will attempt to delete the files from there. If RSFirewall! points out that the files were not deleted then the component does not have enough permissions to delete the files from there and you will have to empty the folder manually.

There are no files in the Joomla! temporary folder

If this message is returned, then no files were found in your Joomla! temporary folder.

4) Checking the integrity of your configuration.php file

The Joomla! configuration.php file is the most targeted file when comes to attacks. This is where sensitive information such as database connection is stored.

Lots of hacked websites have this file modified. That's because configuration.php is one of the first files included when Joomla! parses a page and because this file is included each and every time Joomla! loads a page.

When performing this check the following results can be returned:

Your configuration.php file is not correct

The most common change of this file is whether to add a line of code with lots of spaces at the beginning(so you cannot see the code when opening it) and then a small code that whether includes another file, or send an e-mail to someone,etc.

Your configuration.php file is correct

In this case the configuration.php file from your Joomla! installation is correct and was not modified.

Tip:

- You should move the configuration.php file outside of the public access folder. You can refer to the section below where it is explained how you can achieve this.

5) Checking if configuration.php is outside of public html

There are several ways to protect such sensible files from public access, but most of them are not as feasible. A good way to protect your configuration.php file is to simply move it to a non-public folder. However, note that this isn't a simple copy and paste operation, certain modifications have to be made. Below we will provide step by step instructions on how to achieve this.

Step 1: Move configuration.php to a safe directory outside of public_html.

Step 2: You will have to modify the */includes/defines.php* and */administrator/includes/defines.php* files, more precisely, this constant:

define('JPATH_CONFIGURATION', JPATH_ROOT);

If, for example you wish to move the file up one level and into a folder named "test" the constant will look like this:

define('JPATH_CONFIGURATION', JPATH_ROOT.DS.'..'.DS.'test');

If you wish to move the file up to levels then you can use the following code line:

define('JPATH_CONFIGURATION', JPATH_ROOT.DS.'..'.DS.'..'.DS.'test');

Step 3: Make sure the configuration.php is not writable at all, so that it can not be overridden by com_config.

Step 4: If you need to change configuration settings, do it manually in the relocated configuration.php.

Tip:

- Using this method, even if the Web server somehow delivers the contents of PHP files, for example due to a misconfiguration, nobody can see the contents of the real configuration file. Having into consideration the downside if not beeing able adjust the global settings it is still a good method of protecting against mallacious attacks.

Note:

- On some servers, the path to the moved configuration.php file will have to be added in the allowed paths list for open_basedir.

5.1.7 PHP Check

The PHP Check verifies your PHP variables and checks if they are correctly set. The PHP variables that are verifies are the following: register_globals, safe_mode, allow_url_fopen, allow_url_include, disable_functions and open_basedir.

If the variables are incorrectly set then RSFirewall! will attempt to fix your PHP settings if the configuration is not secure by **creating a local php.ini file in the root of your hosting account.** If the hosting provider allows this, the php.ini file will be read and the new settings will take effect. If it does not work, then it means that the hosting provider does not allow the reading of local php.ini files. Please contact your hosting provider and/or system administrator in order to get this enabled.

The following variables are verified:

register_globals

A common security problem with PHP is the register_globals setting in PHP's configuration file (php.ini). This setting (which can be either On or Off) tells whether or not to register the contents of the EGPCS (Environment, GET, POST, Cookie, Server) variables as global variables. For example, if register_globals is on, the url *http://www.example.com/test.php?id=3* will declare *$id* as a global variable with no code required. Similarly, *$DOCUMENT_ROOT* would also be defined, since it is part of the *$_SERVER* 'superglobal' array.

This feature is a great security risk, and you should ensure that **register_globals is off** for all scripts (as of PHP 4.2.0 this is the default). It's preferred to go through PHP Predefined Variables instead, such as the superglobal *$_REQUEST*. Even more secure is to further specify by using: *$_ENV, $_GET, $_POST, $_COOKIE,* or *$_SERVER* instead of using the more general superglobal *$_REQUEST.*

Note:

- For more information on *register_globals* you can refer to Wikibooks and PHP.net

safe_mode

In PHP, safe mode is a security feature that was designed to prevent hackers from being able to use PHP scripts to execute commands at the operating system level (such as Linux shell commands). It was intended to be a security method for web applications running on shared hosting accounts, as VPS and dedicated servers running single web hosting accounts did not need it. It never functioned well, however, and PHP developers have removed it from the upcoming version 6 release.

The primary problem is that some basic functions required by web scripts would simply not work with PHP safe mode enabled. Dedicated server owners who sold shared hosting accounts to customers were forced to either upset the customers, by providing them with locked-down accounts, or find other security tools. Joomla, in particular, has never played well with safe mode, and the developers recommend disabling it, in order to get the full benefit of the content management system’s functionality.

⚠ **Note:**

- For more information on *safe_mode* you can refer to Joomla! Docs and ServerSchool

allow_url_fopen

If enabled, *allow_url_fopen* allows PHP's file functions -- such as *file_get_contents()* and the include and require statements -- can retrieve data from remote locations, like an FTP or web site.

Programmers frequently forget this and don't do proper input filtering when passing user-provided data to these functions, opening them up to code injection vulnerabilities. A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling *allow_url_fopen* and bad input filtering.

⚠ **Warning:**

- *allow_url_fopen* is on by default.

allow_url_include

If disabled, *allow_url_include* bars remote file access via the include and require statements, but leaves it available for other file functions like *fopen()* and *file_get_contents*. *include* and *require* are the most common attack points for code injection attempts, so this setting plugs that particular hole without affecting the remote file access capabilities of the standard file functions.

Note that at this point we still recommend disabling *allow_url_fopen* as well, but developers who are confident in their secure coding practices may want to leave *allow_url_fopen* enabled.

By default, **allow_url_include is disabled**. If *allow_url_fopen* is disabled, *allow_url_include* is also disabled.

disable_functions

There are a few functions in PHP which allow access to things that the users do not need to know or use. Disabling these can increase security.

There are many functions which can be disabled in PHP using the disable_functions directive via the php.ini file. This setting currently only functions from php.ini so one must be careful to not disable a function which might be needed (by Joomla! or a third party extension, plugin or module). By default, RSFirewall! disables the following functions from the php.ini file:

show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open

open_basedir

The open_basedir directive in php.ini limits PHP file accesses (such as file opening, writing and deleting) within a designated directory such as /home/www/public_html so that it doesn't endanger the rest of the system in any way.

By default, **open_basedir is turned off.** Controversies are raised about whether to use it or not. If a script / file is not included within the allowed paths fatal errors will occur. In this case a warning message is returned and the path that the component wishes to access is pointed out. You will simply have to add the path to the allowed path list in your php.ini file. You can refer to RSFirewall! documentation for further details on this topic.

By default, the php.ini file created by RSFirewall! has the paths to your Joomla! root folder and to your temporary files folder added to the allowed paths list for open_basedir.

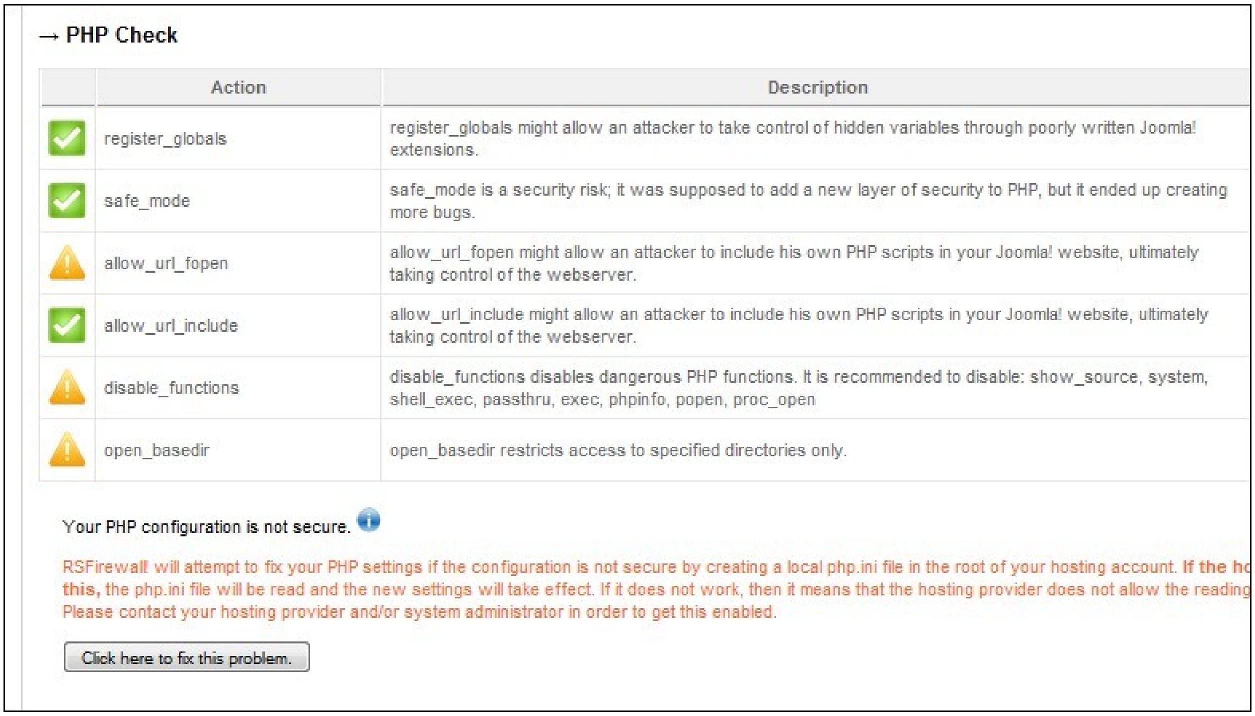
Note:

- On some servers the server's Temporary Files folder will have to be included in the allowed paths list, usually this folder is /tmp.
- If, after you have moved the configuration.php file outside of your Joomla! root folder, an error message similar to the following one is returned:

```
Warning: file_exists() [function.file-exists]: open_basedir restriction in effect.
    File(path_to_file/../../test/configuration.php) is not within the allowed path(s):
    (path/to/Joomla/root:/tmp) in /path/to/Joomla/root/includes/framework.php on line 27
    No configuration file found and no installation code available. Exiting...
```

Then it is best to include the path to the configuration.php file in the allowed paths list for open_basedir.

- Other components may return similar errors that point to an "open_basedir restriction in effect". In this case the paths specified in the error message should be added to the allowed paths list for open_basedir.



→ PHP Check

	Action	Description
✓	register_globals	register_globals might allow an attacker to take control of hidden variables through poorly written Joomla! extensions.
✓	safe_mode	safe_mode is a security risk; it was supposed to add a new layer of security to PHP, but it ended up creating more bugs.
⚠	allow_url_fopen	allow_url_fopen might allow an attacker to include his own PHP scripts in your Joomla! website, ultimately taking control of the webserver.
✓	allow_url_include	allow_url_include might allow an attacker to include his own PHP scripts in your Joomla! website, ultimately taking control of the webserver.
⚠	disable_functions	disable_functions disables dangerous PHP functions. It is recommended to disable: show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open
⚠	open_basedir	open_basedir restricts access to specified directories only.

Your PHP configuration is not secure. ⓘ

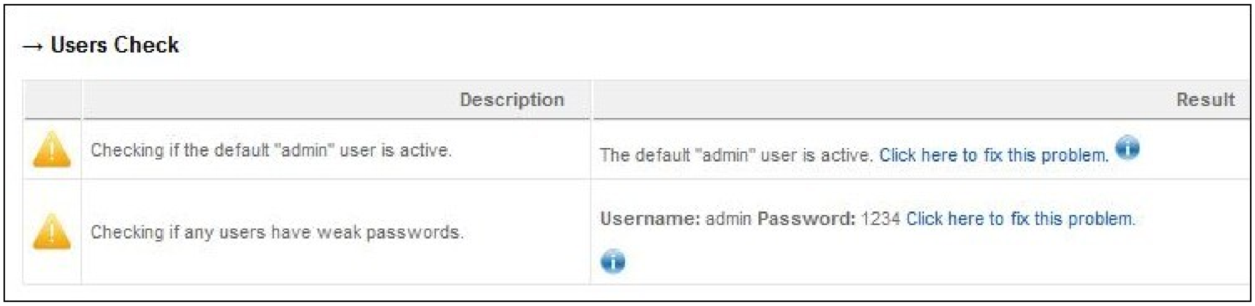
RSFirewall! will attempt to fix your PHP settings if the configuration is not secure by creating a local php.ini file in the root of your hosting account. **If the ho** **this,** the php.ini file will be read and the new settings will take effect. If it does not work, then it means that the hosting provider does not allow the reading Please contact your hosting provider and/or system administrator in order to get this enabled.

5.1.8 Users Check

During the Users Check, RSFirewall! performs two verifications:

1) Checking if the default "admin" user is active

Upon using common usernames your site might be sensitive to brute-force hacking methods. Essentially, these methods try to log in with various combinations of usernames and passwords. Using a username such as **"admin"** for example, will increase the chance of success of such algorithms.



→ Users Check

	Description	Result
⚠	Checking if the default "admin" user is active.	The default "admin" user is active. Click here to fix this problem. ⓘ
⚠	Checking if any users have weak passwords.	**Username:** admin **Password:** 1234 Click here to fix this problem. ⓘ

Among the most the common usernames, **"Root"** was the top username guess by dictionary scripts - attempted 12 times more often than the second-place "admin." Successful root access would open an entire computer or server to a hacker, while admin would grant access to somewhat lesser administrative privileges.

Other top usernames in hacker scripts were *"test," "guest," "info," "adm," "mysql," "user," "administrator" .* All should be avoided as usernames.

⚠ **Note:**

- You can easily rename/disable your usernames, by going to *Site* > *User Manager*.

1) Checking if any users have weak passwords

Generally a normal computer can be attacked up to **2 000** times a day, thus you can imagine that servers are even more susceptible to such attacks. This is why it is best to avoid using simple, intuitive passwords.

The researchers found the most common password-guessing ploy was to reenter or try variations of the username. 43 percent of all password-guessing attempts simply reentered the username. The username followed by *"123"* was the second most-tried choice.

Other common passwords attempted included *"123456", "password", "1234", "12345", "passwd", "123", "test",* and *"1"*. These findings support the warnings of security experts that a password should never be identical or even related to its associated username.

⚠ **Note:**

- You can change a password of a user, by going to *Site* > *User Manager*.

5.1.9 Jumi Check

If you are using Jumi, you might be at risk.

Versions of Jumi, older than 2.0.5 and some versions of 2.0.5 as well include a backdoor. The author has released a clean version on his website. You can download the clean version and install it.

If your site has already been infected, it is recommended that you search for and delete the following files:

1. tmp/.config.php
2. modules/mod_mainmenu/tmpl/.config.php
3. administrator/modules/mod_mainmenu/tmpl/.config.php
4. administrator/components/com_jumi/install.package.php

⚠ **Note:**

- In this case, we strongly recommend that you change all of your website-related passwords: Joomla! Administrator accounts, FTP and MySQL.

5.1.10 Joomla! Configuration

RSFirewall! checks for the following settings in the Global Configuration:

1) Search Engine Friendly URLs

By enabling SEF in your Joomla! Configuration your website will not be vulnerable to targeted Google searches. An attacker could search on Google for a vulnerable extension (by using the syntax "inurl: option=com_dummy") and target all sites that have it installed.

To enable SEF, go to Site > Global Configuration > Site and take a look on the right - you will notice a fieldset called SEO Settings. Here, you must set *Search Engine Friendly URLs* to *Yes.*

2) Session Lifetime

If you setup your session lifetime too high, you will be vulnerable to prying eyes. It's recommended to keep a lower session lifetime so it will expire early in case you leave your computer. We recommend at most 15 minutes.

To change your Session Lifetime, go to *Site* > *Global Configuration* > *System* and take a look on the right - you will notice a fieldset called *Session Settings*. Here, you must set *Session Lifetime* to at most 15 minutes.

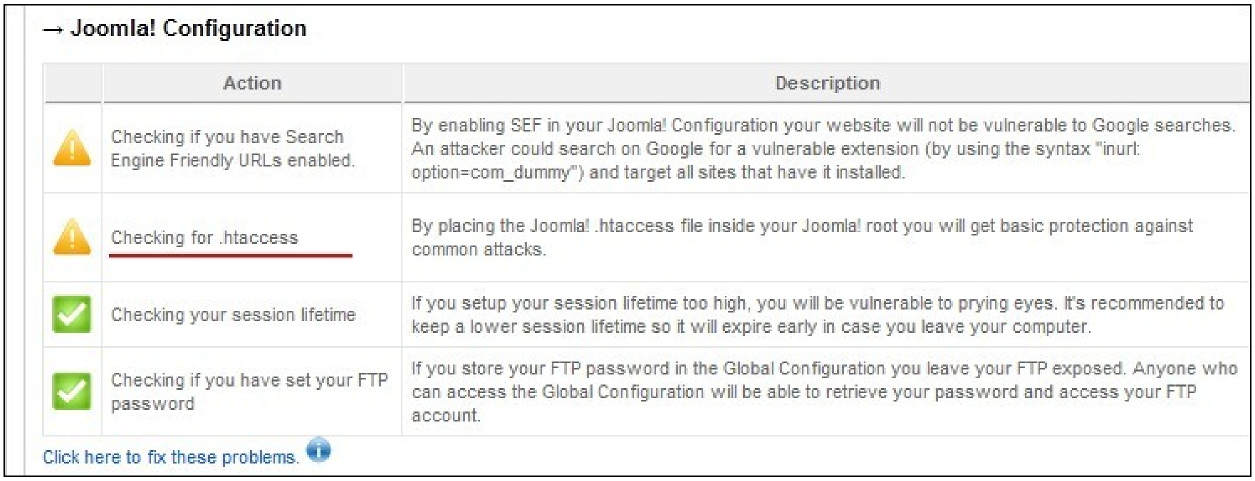
3) FTP Password

If you store your FTP password in the Global Configuration you leave your FTP exposed. Anyone who can access the Global Configuration will be able to retrieve your password and access your FTP account.

To remove your FTP password, go to Site > Global Configuration > Server and take a look on the left - you will notice a fieldset called FTP Settings. Here, you must remove the password from the FTP Password textbox.

4) Checking for .htaccess

An easy way to protect your site against common attacks is by placing the Joomla! .htaccess file in the root of your Joomla! installation folder. This can be easily done by copying the htaccess.txt file and renaming the copy to .htaccess.



→ Joomla! Configuration

	Action	Description
⚠	Checking if you have Search Engine Friendly URLs enabled.	By enabling SEF in your Joomla! Configuration your website will not be vulnerable to Google searches. An attacker could search on Google for a vulnerable extension (by using the syntax "inurl: option=com_dummy") and target all sites that have it installed.
⚠	Checking for .htaccess	By placing the Joomla! .htaccess file inside your Joomla! root you will get basic protection against common attacks.
✓	Checking your session lifetime	If you setup your session lifetime too high, you will be vulnerable to prying eyes. It's recommended to keep a lower session lifetime so it will expire early in case you leave your computer.
✓	Checking if you have set your FTP password	If you store your FTP password in the Global Configuration you leave your FTP exposed. Anyone who can access the Global Configuration will be able to retrieve your password and access your FTP account.

Click here to fix these problems.

Note:

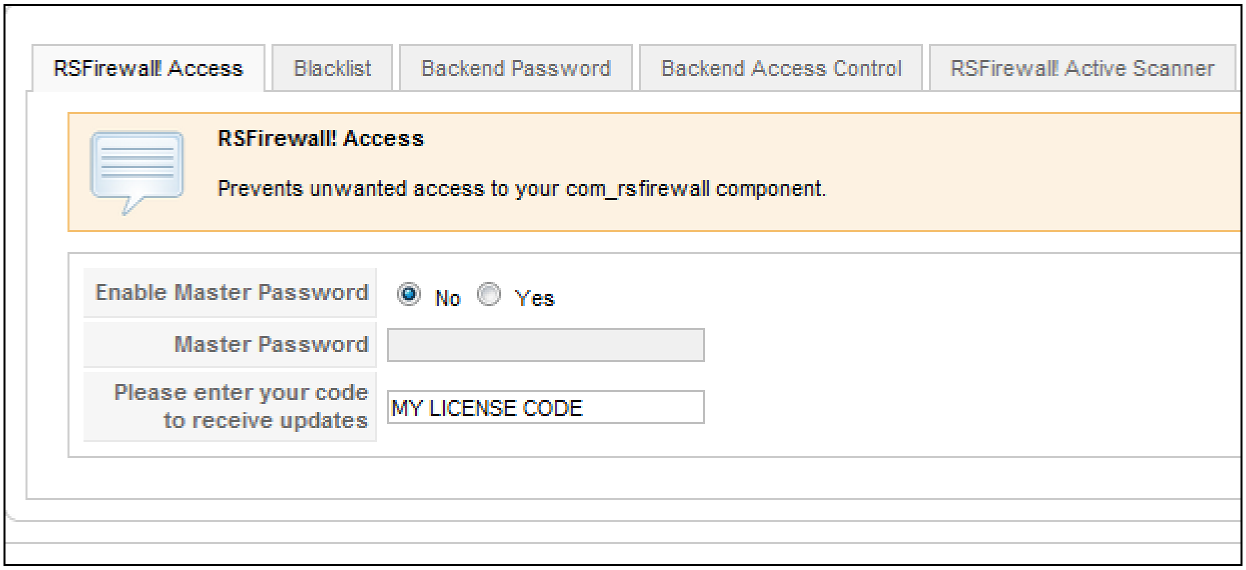
- Some servers may not allow local php.ini files. In this case the PHP Check may not fix the problems pointed out there. You can contact your hosting provider in order to ask if they can enable this option for you.
- On some servers the php.ini file will have to be placed in both your Joomla! root folder and in the /administrator folder from your installation. This way the changes there will be loaded for both the frontend and the backend of your site.

5.2 RSFirewall! Configuration

The **RSFirewall! Configuration** panel is composed of the following security features that can be used in RSFirewall!: RSFirewall! Access, Blacklist, Backend Password, Backend Access Control, RSFirewall! Active Scanner and RSFirewall! Logging Utility.

5.2.1 RSFirewall! Access

In this tab you will be able to set a Master Password for RSFirewall!. When the password is set RSFirewall! will only be accessible on your site if you type the master password.



RSFirewall! Access

Prevents unwanted access to your com_rsfirewall component.

Enable Master Password	● No ○ Yes
Master Password	
Please enter your code to receive updates	MY LICENSE CODE

Note:

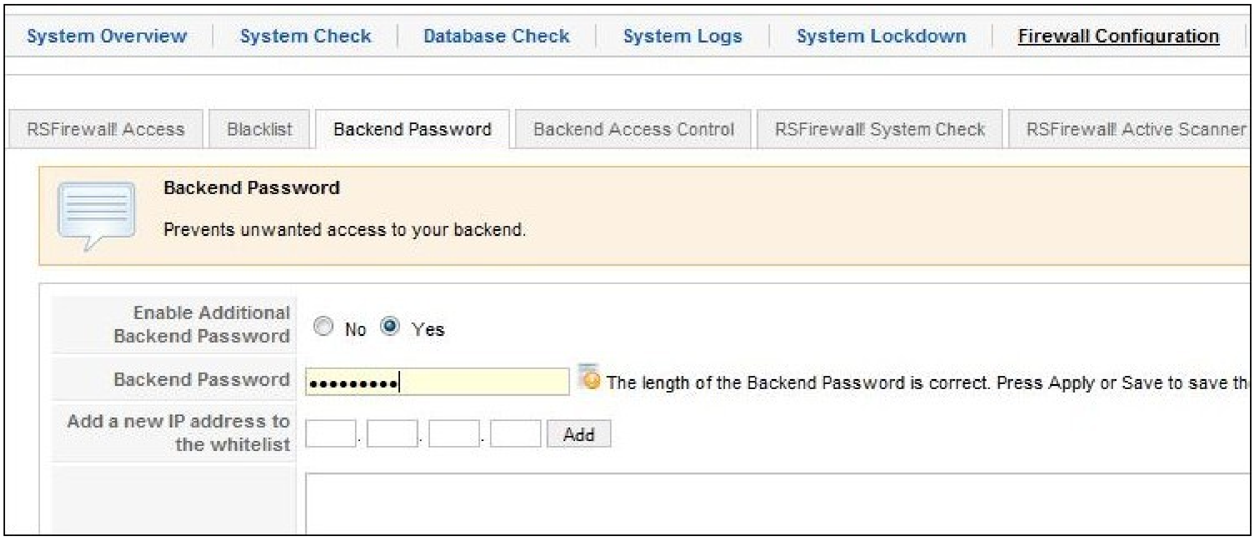
- If you ever lose the master password for RSFirewall! you can reset it from the *_rsfirewall_configuration* table of your Joomla! Database. The table can be edited with PHPMyAdmin(or something similar) and you will have to empty the *master_password* field and set the *master_password_enabled* to 0.

5.2.2 Blacklist

The **Blacklist** option from RSFirewall! prevents unwanted access to your site, blocking configured IP addresses.

5.2.3 Backend Password

Prevents unwanted access to your Joomla administrator panel by adding a password. This tool also offers the possibility to add a so called "white list", meaning that certain users that use one of the pre-configured IPs do not require the extra password.



Backend Password

Prevents unwanted access to your backend.

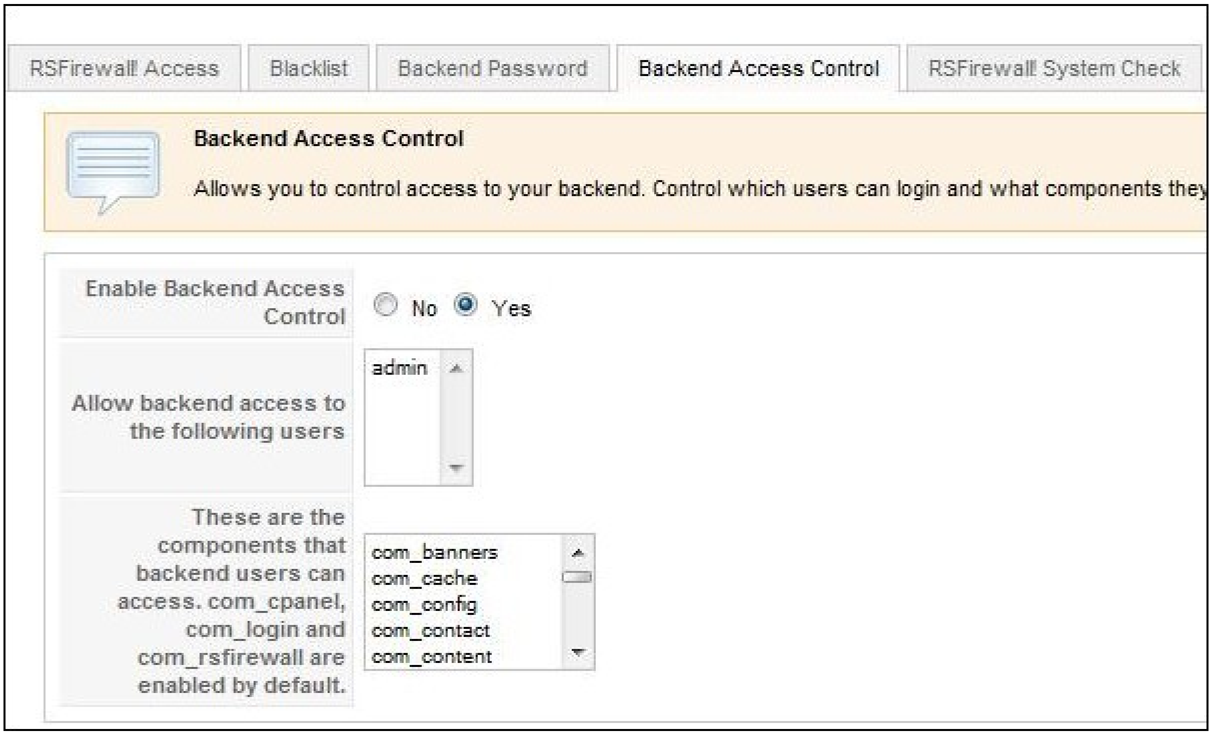
Enable Additional Backend Password: ○ No ● Yes

Backend Password: ••••••••• The length of the Backend Password is correct. Press Apply or Save to save th

Add a new IP address to the whitelist: . . .

5.2.4 Backend Access Control

Allows you to gain more control over what your backend users can edit or manage by restricting which component a user can access.



Backend Access Control

Allows you to control access to your backend. Control which users can login and what components they

Enable Backend Access Control: ○ No ● Yes

Allow backend access to the following users: admin

These are the components that backend users can access. com_cpanel, com_login and com_rsfirewall are enabled by default.: com_banners, com_cache, com_config, com_contact, com_content

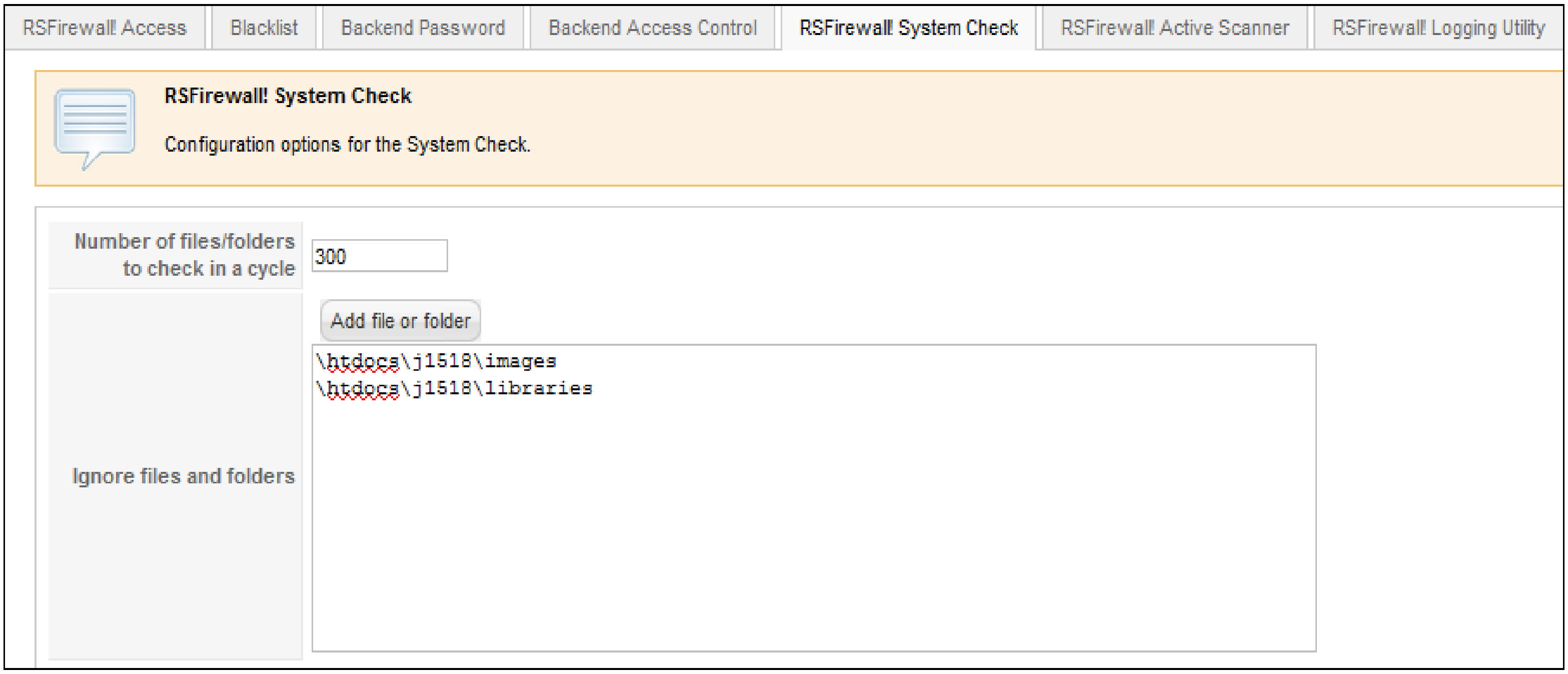
5.2.5 RSFirewall! System Check

Here you can find some some configurable options for the System Check. The following options are configurable:

- Number of files/folders to check in a cycle: If you set a higher value there's a good chance you will run out of memory and the System Check will not finish. Please use a lower value if you are experiencing issues. The default value is 300.
- Ignore files and folders: During the System Check these folders and/or files will be ignored.

Note:

If you select a folder to be ignored, all its files and subfolders will be ignored as well.



RSFirewall! System Check

Configuration options for the System Check.

Number of files/folders to check in a cycle: 300

Ignore files and folders:

```
\htdocs\j1518\images
\htdocs\j1518\libraries
```

5.2.6 RSFirewall! Active Scanner

Provides a configuration tool for the RSFirewall! Active scanner which actively protects your Joomla! website, offering the following configurable options:

- **Enable/Disable Active Scanner**
- **Activate CAPTCHA after this number of failed login attempts**: Activate CAPTCHA after this number of failed login attempts. CAPTCHA will show up in the admnistrator area login form.
- **Protect against DoS attacks**: Protect against bots trying to flood your website by making several requests at a time.
- **Check User-Agents for common malware**: Protect against automated scripts who scan your website looking for vulnerabilities.
- **Convert email addresses from plain text to images**: This setting will convert all email addresses from plain text to images, in the same way as the Email Cloaking plugin will convert them to Javascript.
- **Remove the generator meta tag from your template**: Removing the generator meta tag from your website's template will protect you from spambots or attackers that target Joomla! Websites.
- **Verify system variables for SQL injections**: GET and POST variables will be checked if they contain SQL commands.
- **Skip the following components when verifying for SQL injections (CAUTION!):** If you are using a database management component that allows you to type in SQL commands (eg. SELECT * FROM jos_users), please select it from this list so that RSFirewall! will not consider it an SQL injection attack.
- **Verify system variables for PHP injections**: GET and POST variables will be checked if they contain directory traversal (../../) attacks or links to other websites (http:// or https://).
- **Skip the following components when verifying for PHP injections (CAUTION!)**: If you are using a banner management component that keeps the website's address in the URL (eg. com_something?goto=http://www.google.com), please select it from this list so that RSFirewall! will not consider it an PHP injection attack.
- **Verify system variables for Javascript injections**: GET and POST variables will be checked if they contain <and > tags.

- **Skip the following components when verifying for Javascript injections (CAUTION!)**: If you use a component that allows users to type in text in a WYSIWYG editor, please select it from this list so that RSFirewall! will not consider it an JS injection attack.

- **Verify if uploaded files have multiple extensions**: Uploading files with multiple extensions might trick your or any other user that the file has a safe extension.

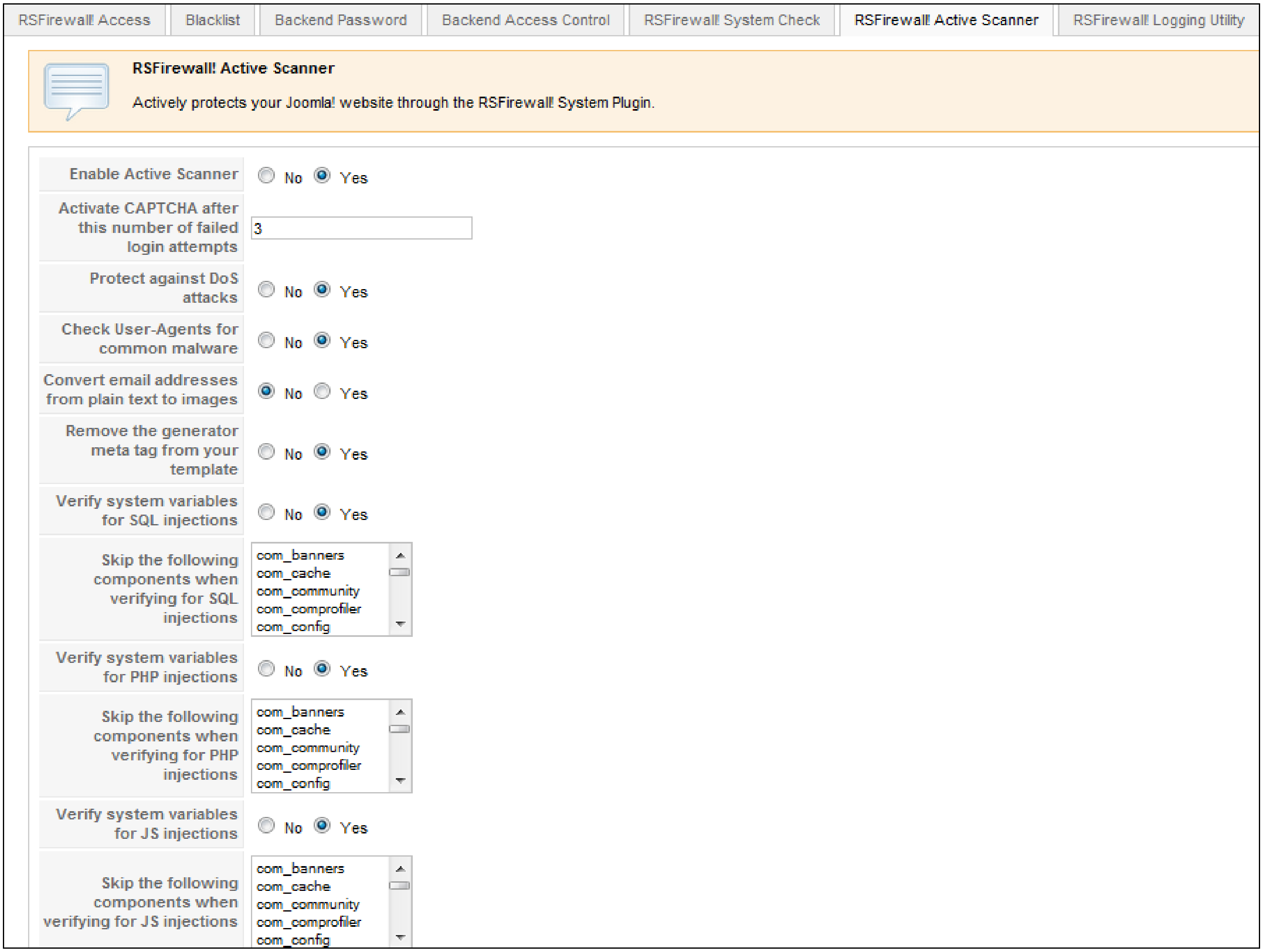
- **Verify uploaded files for known malware patterns**: Verify uploaded files for known malware patterns, such as PHP shell scripts.

- **Don't upload files with the following extensions**: Files with the following extensions will be deleted as soon as they've been uploaded to the temporary directory on your server. If you enable the &quot;Multiple extensions check&quot;, this will check all the files extensions, as opposed to the last one.

- **Check core Joomla! files integrity**: Checks a few core Joomla! files for integrity, like the Joomla! login and index.php.

- **Monitor the following files for changes**: If any of the following files will be changed, you will be alerted by email and an entry will be posted in the System Log. This is useful when you want to monitor important files, such as downloadable documents (if they get infected with a virus, the infection will spread throughout your users).

- **Protect the following users from any changes**: This will create a snapshot of the selected users. If any changes will happen to any of them, it will get reverted back immediately. If you want to update your snapshot, you will have to deselect all the users, press Apply and then select the users again and finally Save the configuration.



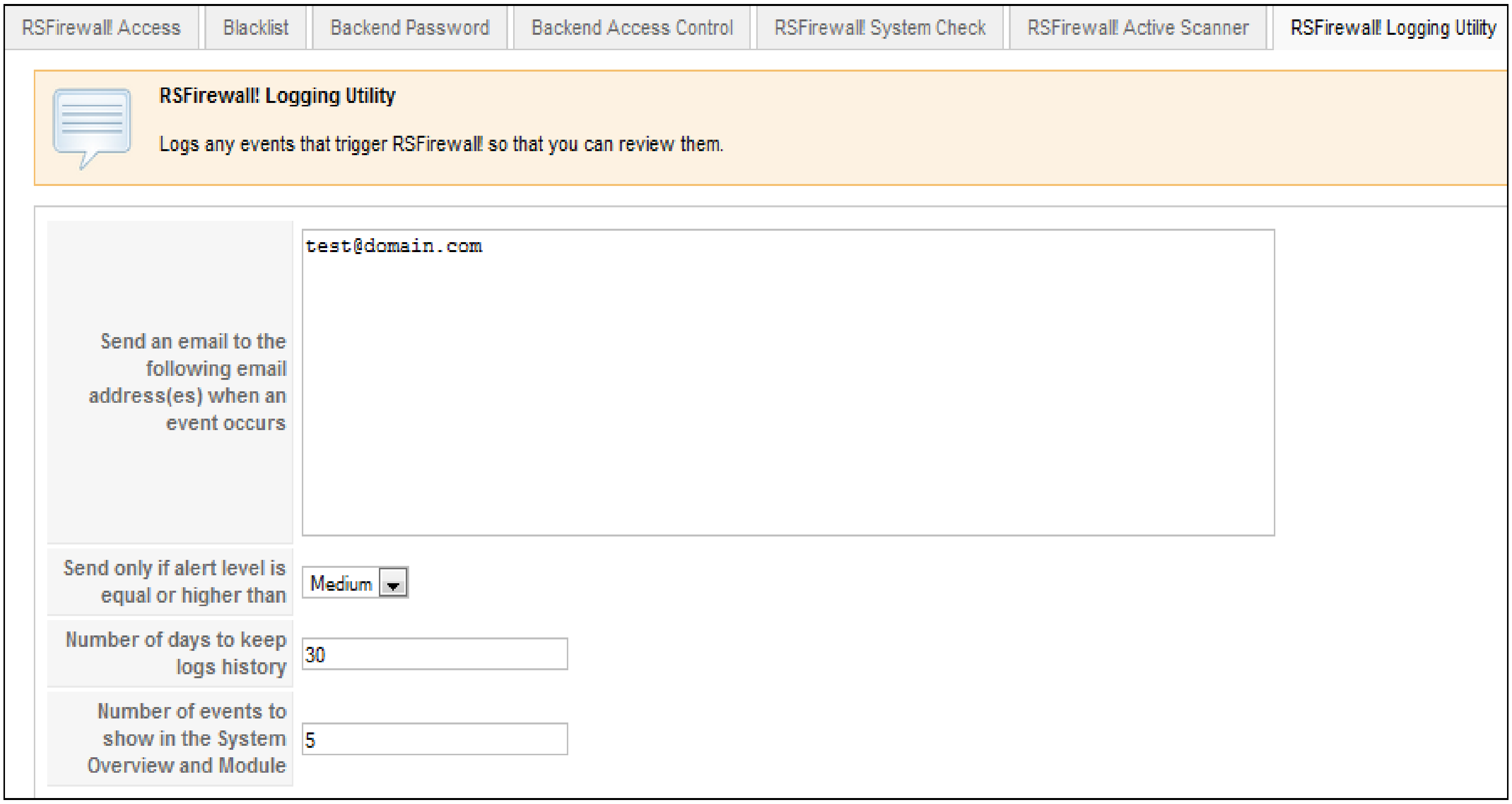
RSFirewall! Active Scanner

Actively protects your Joomla! website through the RSFirewall! System Plugin.

Enable Active Scanner	○ No ● Yes
Activate CAPTCHA after this number of failed login attempts	3
Protect against DoS attacks	○ No ● Yes
Check User-Agents for common malware	○ No ● Yes
Convert email addresses from plain text to images	● No ○ Yes
Remove the generator meta tag from your template	○ No ● Yes
Verify system variables for SQL injections	○ No ● Yes
Skip the following components when verifying for SQL injections	com_banners com_cache com_community com_comprofiler com_config
Verify system variables for PHP injections	○ No ● Yes
Skip the following components when verifying for PHP injections	com_banners com_cache com_community com_comprofiler com_config
Verify system variables for JS injections	○ No ● Yes
Skip the following components when verifying for JS injections	com_banners com_cache com_community com_comprofiler com_config

5.2.7 RSFirewall! Logging Utility

Logs any events that trigger RSFirewall! so that you can review them. The logging utility also offers the possibility to send out an email if a security event is recorded that has a security level higher then a preconfigured value (low, medium, high, critical).



RSFirewall! Logging Utility

Logs any events that trigger RSFirewall! so that you can review them.

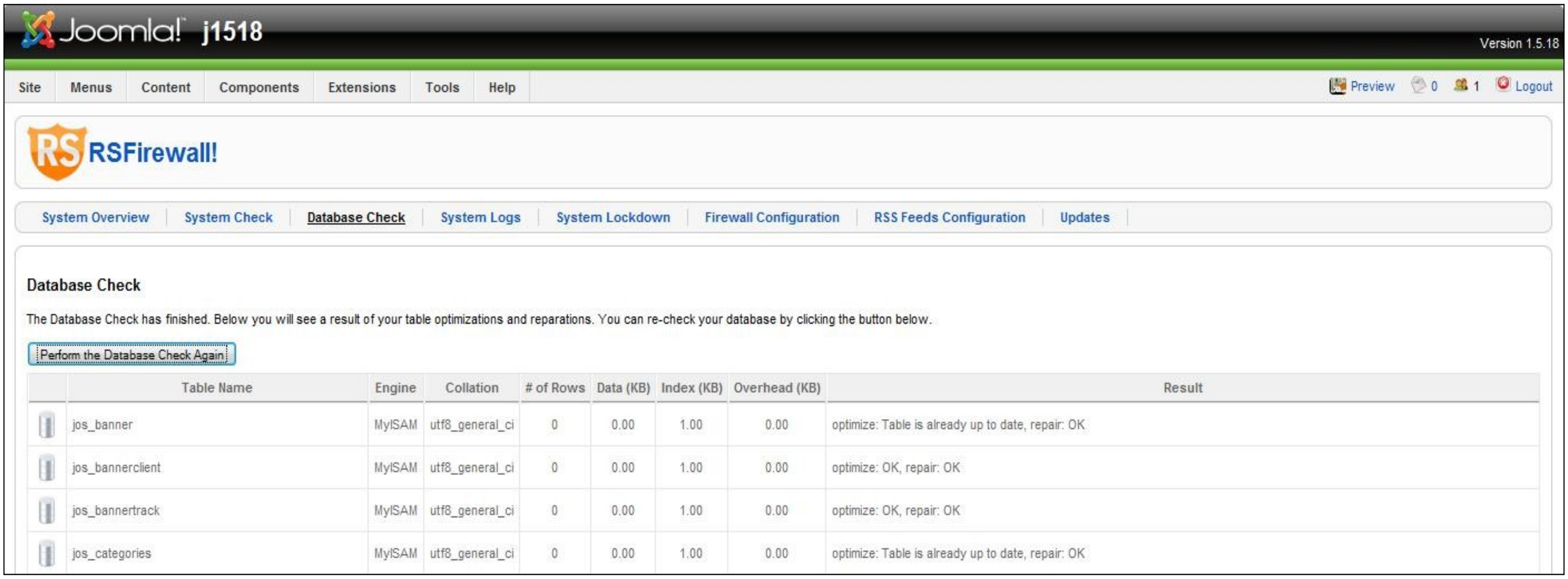
Send an email to the following email address(es) when an event occurs	test@domain.com
Send only if alert level is equal or higher than	Medium
Number of days to keep logs history	30
Number of events to show in the System Overview and Module	5

5.3 Database Check

The **Database Check** from RSFirewall! **verifies all the tables from your Joomla! database**. During the check you will be able to see the following information of each of your Joomla! tables:

- **Table Name**: the name for each table.
- **Engine**: the engine used for each table(by default MyISAM).
- **Collation**: the collation for each table(usually utf8_general_ci).
- **Number of Rows**: the number of rows occupied in each table.
- **Data(kb)**: the size of the Data stored in each table.

- **Index(kb)**: the indexes of the respective table.
- **Overhead(kb)**: the Overhead of each table.
- **Result(kb)**: the Result of the check.



Database Check

The Database Check has finished. Below you will see a result of your table optimizations and reparations. You can re-check your database by clicking the button below.

	Table Name	Engine	Collation	# of Rows	Data (KB)	Index (KB)	Overhead (KB)	Result
	jos_banner	MyISAM	utf8_general_ci	0	0.00	1.00	0.00	optimize: Table is already up to date, repair: OK
	jos_bannerclient	MyISAM	utf8_general_ci	0	0.00	1.00	0.00	optimize: OK, repair: OK
	jos_bannertrack	MyISAM	utf8_general_ci	0	0.00	1.00	0.00	optimize: OK, repair: OK
	jos_categories	MyISAM	utf8_general_ci	0	0.00	1.00	0.00	optimize: Table is already up to date, repair: OK

The Database Check **verifies, analyzes and optimizes your Joomla! tables.** If any table is found corrupted it will attempt to repair the respective table without losing the data from it.

On some tables, on which many operations are done, an optimization will be made, although in some cases this will not be needed.

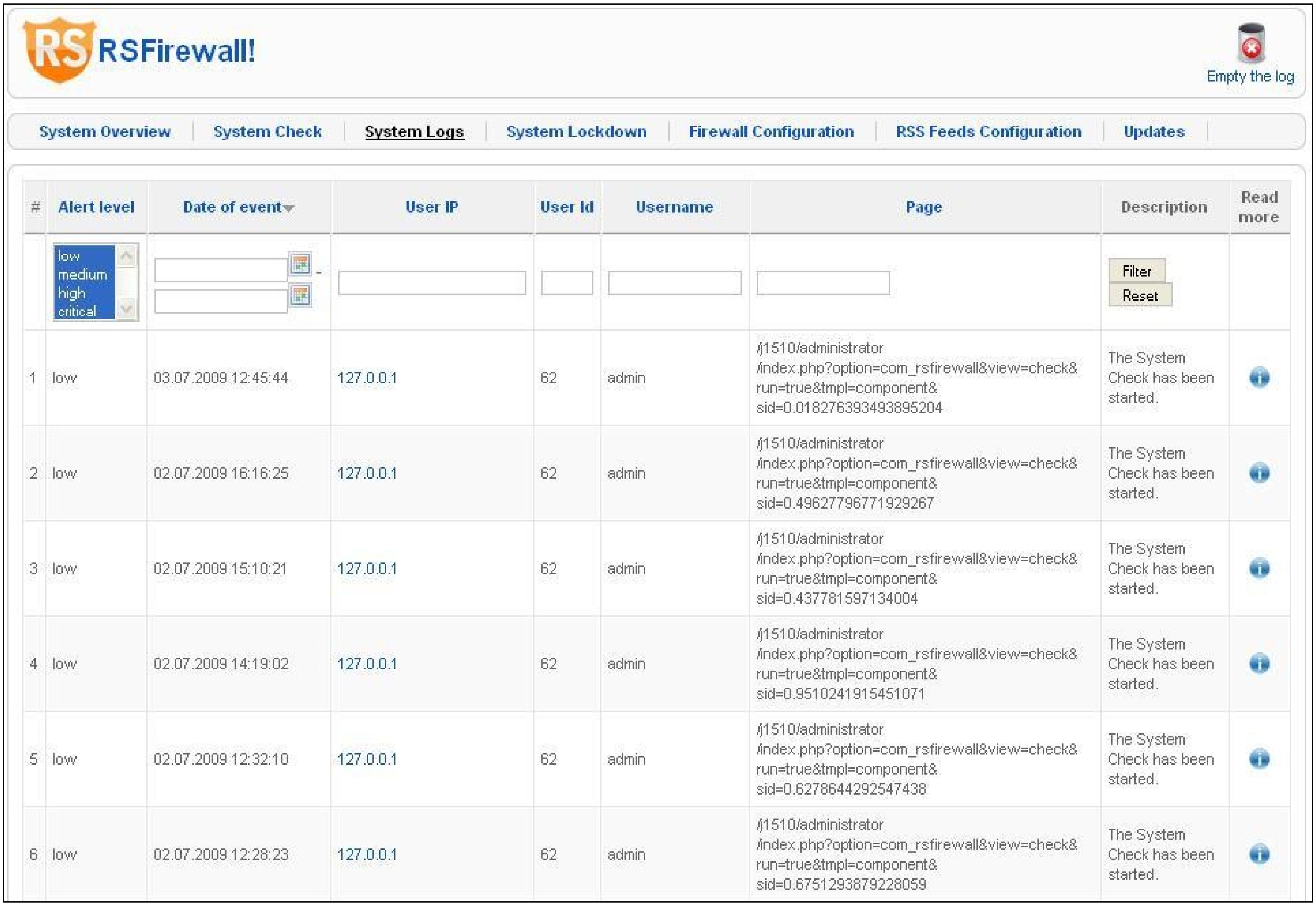
Table optimization verifies for the following: if the table has deleted or split rows or if the index pages are not sorted. Depending on the cases the check will: repair the table or sort indexes.

5.4 System Logs

The **System Logs feature offers a logging utility** to the RSFirewall! component, thus empowering the user to keep track of the site security issues.

Essentially it logs all security important events that take place on your Joomla installation. The System Logs tool enables the owner to add various filters like: alert level, date, IP, userID, username and page. Upon pressing on the IP a "**Who is**" service checks the specified IP address, thus displaying further information.

When clicking on a log event, you will be taken to a page with additional information: several other $_SERVER variables and debugging info (if it's *$_GET, $_POST*, show the contents).



#	Alert level	Date of event	User IP	User Id	Username	Page	Description	Read more
	low medium high critical						Filter Reset	
1	low	03.07.2009 12:45:44	127.0.0.1	62	admin	/j1510/administrator /index.php?option=com_rsfirewall&view=check& run=true&tmpl=component& sid=0.018276393493895204	The System Check has been started.	●
2	low	02.07.2009 16:16:25	127.0.0.1	62	admin	/j1510/administrator /index.php?option=com_rsfirewall&view=check& run=true&tmpl=component& sid=0.49627796771929267	The System Check has been started.	●
3	low	02.07.2009 15:10:21	127.0.0.1	62	admin	/j1510/administrator /index.php?option=com_rsfirewall&view=check& run=true&tmpl=component& sid=0.437781597134004	The System Check has been started.	●
4	low	02.07.2009 14:19:02	127.0.0.1	62	admin	/j1510/administrator /index.php?option=com_rsfirewall&view=check& run=true&tmpl=component& sid=0.9510241915451071	The System Check has been started.	●
5	low	02.07.2009 12:32:10	127.0.0.1	62	admin	/j1510/administrator /index.php?option=com_rsfirewall&view=check& run=true&tmpl=component& sid=0.6278644292547438	The System Check has been started.	●
6	low	02.07.2009 12:28:23	127.0.0.1	62	admin	/j1510/administrator /index.php?option=com_rsfirewall&view=check& run=true&tmpl=component& sid=0.6751293879228059	The System Check has been started.	●

5.5 System Lockdown

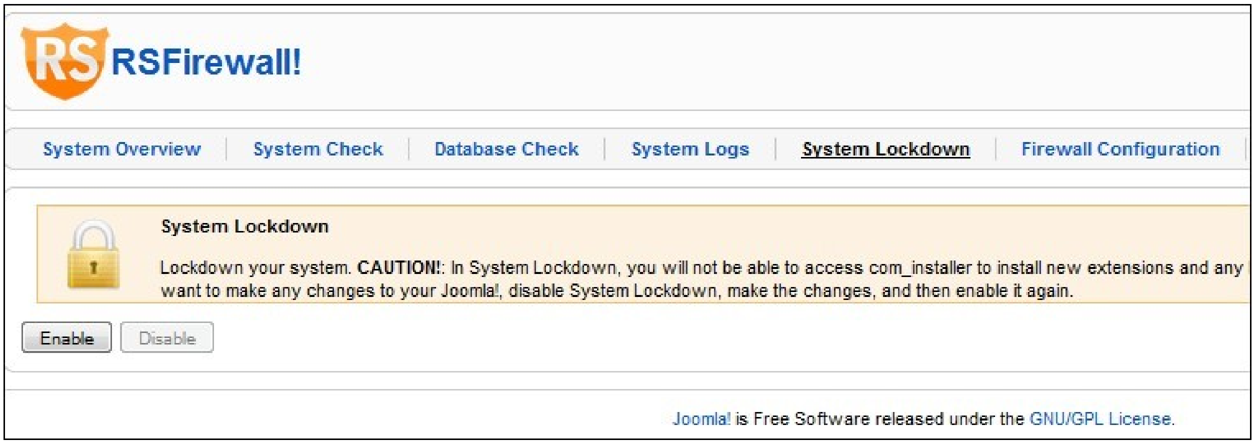
The **RSFirewall! System Lockdown** utility blocks new information from being added to your site. This feature is enabled by the *RSFirewall! System plugin*, performing the following tasks:

- Denies access to com_installer, thus new components can't be installed while the Lockdown is effective;

- Blocks user registration and the alteration in any way of all account information data.

⚠ **Note:**

- By enabling or disabling the System Lockdown an event log is created.



System Lockdown

Lockdown your system. **CAUTION!**: In System Lockdown, you will not be able to access com_installer to install new extensions and any
want to make any changes to your Joomla!, disable System Lockdown, make the changes, and then enable it again.

Joomla! is Free Software released under the GNU/GPL License.

Step 6: Security Tips

In this section we will provide some useful **Joomla! Security tips** which you can take in consideration for your own sites.

Tip 1: DO NOT USE the "admin" user

When you install Joomla!, it comes with the predefined "admin" user. Joomla! had a bug allowing hackers to take over Joomla! websites exploited this "admin" user, but it has been fixed now. **Leaving the admin user as the Super Administrator in combination with a weak password can make your website vulnerable.**

Note:

- To protect the administrator page from being accessed by anyone set up an additional backend password for your Joomla! website.

Tip 2: DO NOT USE weak passwords for admin users

Choose carefully passwords for admin users; don't use common words. It is best to advice your users, when registering to your website, **to choose a good password**, alpha-numeric, because hackers might take advantage and steal valuable information from them.

Do not use the same password to access the Joomla! backend and the hosting account. Try not to include in your password personal information like your name, username, date of birth, common words and easy to guess like "admin","password", "username", "password123" or English words.

You could apply an algorithm, easy to remember to choose a password. For example, create a sentence like : "I have one brother Alan and a sister Kate". If we take the first letter from every word the result will be IhobAaasK . To complicate it replace numbers with digits and if it's possible introduce special characters.

Here is the result: Ih1bA&1sK.

Tip 3: ALWAYS KEEP an updated antivirus

If you have applied all the fixes suggested by RSFirewall! do not think that your site is 100% secure. You will still have to use an antivirus application to protect your computer. New viruses nowadays look for ftp connections and inject malicious scripts directly into your Joomla! files because your computer is has been compromised. It's best to keep your computer protected by getting the latest updates for your antivirus.

⚠ **Note:**

- If your site was hacked, it is best to also scan your computer and all the files from your site for any viruses. Some viruses tend to store your site's FTP details, so it is best to change your FTP password also.

Tip 4: DO NOT ALLOW uncontrolled file uploads(in forums, comments, forms and so on)

Hackers can and will use these applications to upload malware scripts and enter into your Joomla! Website. You must allow as few file extensions as possible, and **NEVER** let executable script files (.php, .php3, .php4, .php5, .phtml) to be uploaded. To avoid this you can use RSFirewall! that automatically blocks unwanted file uploads. Also it can scan your system, look for malware patterns and hacker scripts.

Tip 5: Perform REGULAR backups and updates for your Joomla! installation and database

Always have a backup of your Joomla! site available, in case someone manages to hack your site. This way you will be able to restore your site and have it back online and functional in no time. Also it is best to keep an updated Joomla! installation and have your components updated to the last version. Both Joomla! and your components are frequently updated and many updates include security improvements to their functionality.

Note:

- We recommend performing a backup of your site every 1 or 2 weeks. This way you will constantly have a backup of your data and do not risk losing all the information from your site or possible important updates.
- You should constantly verify if there are any updates available for Joomla! or for other components that you are using. When an updated is available it is recommended to check the changelog of the product first and then apply the update.

Tip 5: Perform REGULAR scans of your Joomla! installation files and folders

It is recommended that a regular scan of your Joomla! files and folders should be made. This way you will constantly verify if your files are infected or if an infected file is placed in your installation folder. You can scan your Joomla! core files for modifications and malware patterns with the help of RSFirewall!. The rest of your files can either by downloaded on your computer and scanned with the help of a computer anti-virus.

Note:

- We recommend performing a scan of your site's files and folders once every 2 weeks.

Tip 6: Keep a LOG FILE that stores the recent activity of your server

Log files are a key part in determining if a someone hacked into your site or is trying to gain access. These files should be put in a safe place and checked periodically for any suspicious traces. Usually, if a hacker tries to perform malicious actions on your site he will try to erase the traces from the log file to protect their location and identity.

The IP address of the person that performs actions on your site is logged. If you detect a pattern for this address that has performed suspicious actions, like trying to log in to the site backend, you can simply block it. Please note that hackers often use multiple IP and various methods to hide their real IP identity via Proxy servers.

Tip 7: Keep a TEST SITE

It is best that you can keep an exact copy of your site on your localhost or on the same server. This way you can test an update or a component before you install and use on your real, live site, thus there will be no surprise site crashing and such.

The purpose of this guide

This guide is designed to assist you, step by step, in configuring the security tool for Joomla!, RSFirewall!.

We've also created a RSFirewall!! Quick Guide, that includes all important steps that you must follow to quickly secure the website.

Additionally, we've launched the RSJoomla! TV Channel to support our components with a series of video tutorials and presentations.

The RSFirewall! Documentation can be found here.

For any other questions, please submit a ticket to the RSJoomla! support department.