# Quick 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**

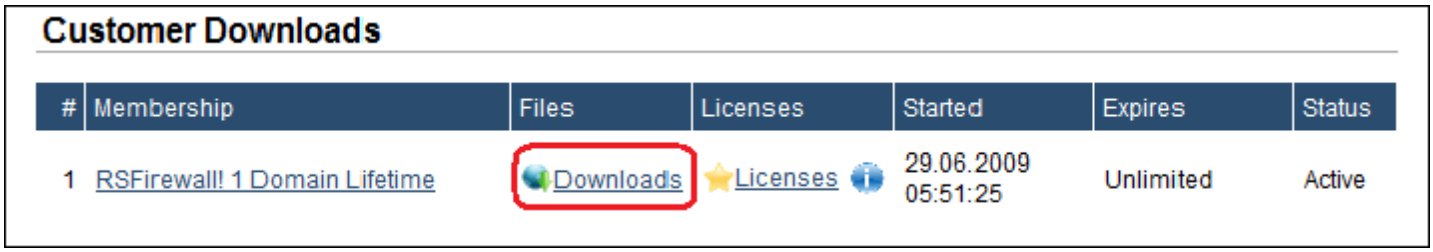

# Step 2: Download RSFirewall!

To download RSFirewall! you need to:

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

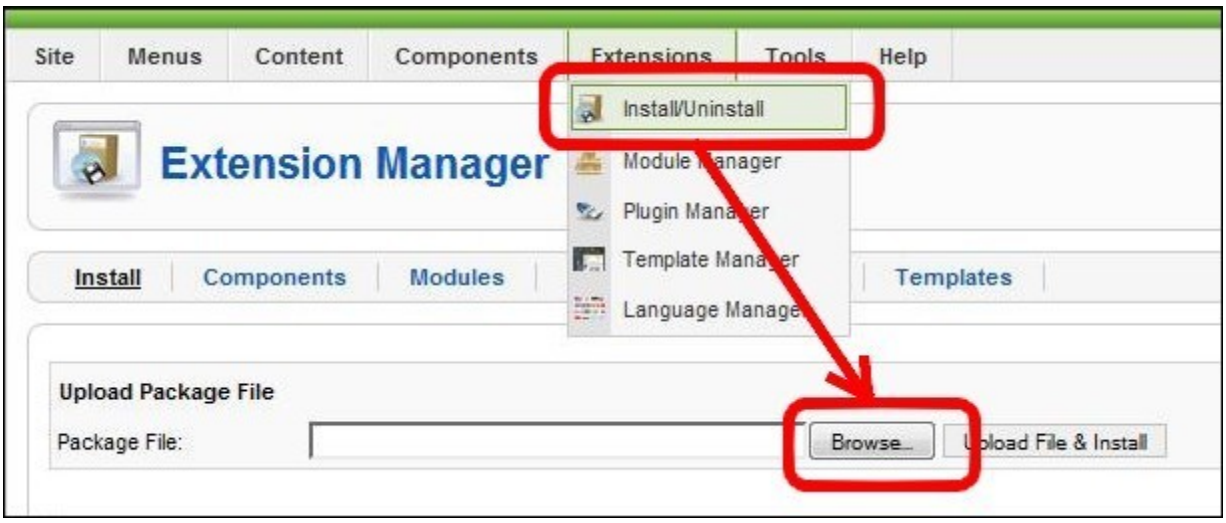
**Step 2:** in the right side, you will find a section dedicated to RSJoomla! customers: **Customer Login.** Click on **View my downloads**


**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***




# Step 3: Installing RSFirewall!

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.***



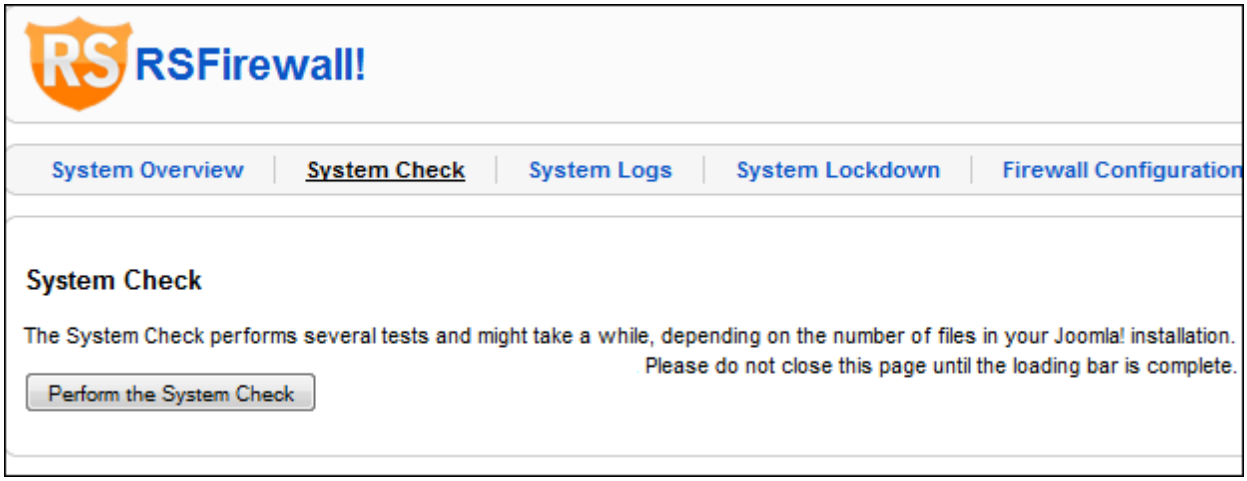

# Step 4: Scan the Joomla! installation

## 4.1 Run the System Check

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

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.

Start the System Check, by clicking on the “Perform System Check” button on the page.



## 4.2 Fix the security vulnerabilities

After running the System Check, RSFirewall! will display a list with the founded security vulnerabilities.

### 4.2.1 Joomla! And RSFirewall! versions

#### 4.2.1.1 Check the RSFirewall! version

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 are using the latest version of RSFirewall!" -** 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!" - i**t'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.

#### 4.2.1.2 Check the Joomla! version

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 are using the latest version of Joomla!" -** 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.

### 4.2.2 File Integrity Check

The File Integrity Check verifies if the core Joomla! files from your installation are either modified or missing. It is recommended to keep track of the core modifications in order to know which changes to accept and which to not.

- **The file has been modified** - download the original file from the Joomla! installation package and replace the modified files if you are unaware of the changes

- **The file is missing -** download a copy of the missing/modified file from our server directly. You will have to upload it manually on your Joomla! Installation.

### 4.2.3 File and Folder Permissions Check

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

#### 4.2.3.1 Folder Permissions Check - identify the folders that you need to fix.

- **You have folders with permissions higher than 755 - f**olders 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.

**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.

#### 4.2.3.2 File Permissions Check - identify the files that you need to fix.

- **You have files with permissions higher than 644 - l**eaving 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.

### 4.2.4 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.

- **There are no malware patterns in your php files -** no dangerous scripts have been found on your server.
- **You have malware patterns in your files -** your server is probably been hacked and you need to take immediate actions.

**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.

## 4.2.5 File and Folder Access Check

The File and Folder Access Check checks for the following:

### 4.2.5.1 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.

### 4.2.5.2 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 Joomla! log folder is accessible through the public html -** 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 - s**etting the log folder out of the public access of your website is a good idea, since no one can access the files inside.

#### 4.2.5.3 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. When running this check the following results can be returned:

- **There are files in the Joomla! temporary folder - y**our 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.

- **There are no files in the Joomla! temporary folder -** no files were found in your Joomla! temporary folder.

#### 4.2.5.4 Checking the integrity of your configuration.php file

When performing this check the following results can be returned:

- **Your configuration.php file is not correct - t**he 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.

#### 4.2.5.5 Checking if configuration.php is outside of public html

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.

### 4.2.6 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.

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.

- **safe_mode - i**n 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). 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.

- **allow_url_fopen - i**f 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.

- **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.

- **disable_functions - t**here 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. 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 - t**he 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, 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.

### 4.2.7 Users Check

During the Users Check, RSFirewall! performs two verifications:

- **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.

**Note:**

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

- **Checking if any users have weak passwords - g**enerally 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.

**Note:**

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

### 4.2.8 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. 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.

### 4.2.9 Joomla! Configuration

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

- **Search Engine Friendly URLs - b**y enabling SEF in your Joomla! Configuration your website will not be vulnerable to targeted Google searches.
- **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.
- **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.

- **Checking for .htaccess - a**n 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.

# Step 5: Configure RSFirewall!

Path: ***Joomla! Backend panel >> Components >> RSFirewall! >> Firewall! Configuration***

**In the RSFirewall! Access tab:**

- set the Master Password
- add the license code to receive updates

**In the "Blacklist" tab -** add IP addresses to the blacklist

**In the "Backend Password" tab –** configure the Joomla! Additional backend password

**In the "Backend Access Control" tab** – rmanage the components that a user can access.

**In the "RSFirewall! Active Scanner" tab:**

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 "Multiple extensions check", 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.

# Step 6: Database Check

Path: ***Joomla! Backend panel >> Components >> RSFirewall! >> Database Check***

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.

# Step 7: System Logs

Path: ***Joomla! Backend panel >> Components >> RSFirewall! >> 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.

# Step 8: Enable the System Lockdown

Path: ***Joomla! Backend panel >> Components >> RSFirewall! >> System Lockdown***

After scanning the Joomla! Installation and fixing the security vulnerabilities it is recommended to enable the System Lockdown.

The **RSFirewall! System Lockdown** blocks the admin take-over attempts and deny access to Joomla! installer preventing hacker attacks.

- 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.

# Security Tips

**Tip 1: DO NOT USE the "admin" user**

**Tip 2: DO NOT USE weak passwords for admin users**

**Tip 3: ALWAYS KEEP an updated antivirus**

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

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

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

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

**Tip 7: Keep a TEST SITE**

# The purpose of this guide

This guide is designed to help you quickly secure a Joomla! Website with the security tool RSFirewall!.

We've also created a detailed RSFirewall! guide, that includes all required steps to configure the component and 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.