JCheck – Security Monitor for Websites

http://www.ravenswoodit.co.uk

Last Updated: June 07

JCheck Owners Manual

Feature Guide

JCheck is a multiplatform security tool which allows automated file integrity checking / host-based intrusion detection on Joomla, Mambo or any other system which supports PHP.

It creates an encoded database which is used to verify the integrity of files on your website. Any change to the files will be flagged for attention by the administrator.

This enables easy detection of hacking attempts and allows prompt action to be taken to prevent further damage.

JCheck can be configured in many ways to eliminate false positives and minimise the effort required my site owners.

Alerts can be sent by Email or logged to a logfile for monitoring by other tools.

JCheck is delivered as a zip file, it can be installed and configured to run at periods as specified by the Administrator.

It can be used as standalone application running thru cron for the most effective protection, better security and flexibility.

It can also be installed and used as a Joomla or Mambo module, whereby the module acts as a bridge to the JCheck application.

It is important to note that JCheck does not prevent any unauthorised activity on your site, but it will help to alert you of this quickly(hopefully before your users do) so that manual remedial action can be taken.

Supported Platforms	☑ Any PHP 4.3+ or 5 web site ☑ Joomla 1.0n ☑ Mambo 4.5.3 and above
File/directory change checks	☑ MD5 Checksums ☑ Size ☑ Mode/permission ☑ Owner ☑ Group ☑ Creation/modification time ☑ Adds/deletes/changes
Additional options	☑ Exclusion of individual subdirectories and/or files is possible. ☑ Exclusion using regular expressions ☑ File checks can be performed at admin-defined intervals. ☑ Integrity database can be manually or automatically updated ☑ Email frequency can be configured i.e. only where changes are found or on every run ☑ Logfiles are generated showing details of runs and can be used by monitoring tools
Security Features	☑ All JCheck package files can be renamed and installed in any directory to help evade detection by hackers. This includes database, logfile and library ☑ Joomla/Mambo Module can be invisible on website ☑ Optional "Monitored by JCheck" graphic can be displayed

JCheck is available in two editions:

Free	☑ Limited to running every 24 hours ☑ Logo/Text displayed on Joomla/Mambo sites
Plus	☑ Enabled by Licence key, no re-installation required ☑ licenced on a per website basis ☑ add on sites at reduced cost

N.B. JCheck is copyrighted commercial software. Some code is encrypted.

Installation of JCheck

Standard install

JCheck comes packaged in a single zip file which should be installed manually.

The steps to follow are:

1. Upload the zip file to your website.
2. Unzip the file, to your preferred location.

Note

The user which will be running JCheck needs to be able to read/write from this directory. It is more secure if this location is **outside** the web server DocumentRoot i.e. it is not accessible from the web.

Before adding a cron entry you need to configure some parameters. In the standalone version, parameters are changed by modifying the **jcdriver.php** file. See Appendix A for details.

Some of the parameters will only have an effect if you have purchased a licence for JCheck, this is explained in Appendix A.

Once the parameters have been configured you will need to add a cron entry for JCheck, how you do this depends on your server configuration. You need to set the cron to run at an appropriate interval, we would recommend 1 – 4 hours as a suitable value.

The entry for the script should look like:

php –q /path_to_jcheck/jcdriver.php

If you are having a problem running JCheck due to our encoded library, there is also an Ioncube version of the library supplied, just rename the ioncube.jcheck.php to jcheck.php.

Joomla/Mambo install

JCheck comes packaged in a single zip file which should be installed via the Joomla/Mambo module installer.

The steps to follow are:

1. Log in into Backend to access the administrative interface.

You need to have the privileges of an Administrator / Superadministrator to install packages.

2. Click 'Installers' => 'Modules' (or 'Modules' => 'Install/Uninstall' when using an older version) in the Top Menu.

In the part 'Upload new module' select the JCheck zip file.

Now click on 'Upload File & Install'. Depending on the network speed, you may have to wait a moment while the file is being uploaded to your server and unpacked.

Note

Package Files are mostly a ZIP or tar.gz compressed file directory, which includes all information for the installation. The main file is an XML document which describes the installation process. In order to use this function for your installation, your web server must support the zlib extension. You can check this in the Admin Section Menu item, System > System Info > System Information.

The JCheck module should be installed now, but it's state will be Unpublished.

Before publishing you should set the Show Title option to no, and configure some parameters. See Appendix A for details.

Some of the parameters will only have an effect if you have purchased a licence for JCheck, this is explained in Appendix A.

If you are having a problem running JCheck due to our encoded library, there is also an Ioncube version of the library supplied, just rename the ioncube.jcheck.php to jcheck.php.

Running JCheck

The first time JCheck runs it will create a new integrity database based on the files it finds and the exclusion settings in force at the time.

Note

If running the Joomla/Mambo version, you will experience a noticeable delay on the pageload when JCheck runs. This delay will only occur once per run and should not affect the normal operation of your site. If you have a particularly large site, we would recommend implementing the cron job which will prevent this delay.

Future runs will be compared against this database and any differences will be reported.

Changes to the following items for each file/directory will generate an alert:

- ☑ MD5 Checksum
- ☑ Size
- ☑ Mode/permission
- ☑ Owner/Group
- ☑ Creation/modification time
- ☑ Adds/deletes/changes

Note

Changing the patterns to exclude from checking after the initial run may generate alerts as this will be flagged as a difference.

It is recommended that JCheck is set to update its database after each run, this ensures that only differences between runs are flagged and involves no intervention or maintenance by the site administrator.

If manual update of the database is set, then it will be necessary for the admin to delete the database file to force re-initialisation.

JCheck can take some time to run, depending on how many files your website contains. If running the cron version then this is not a major problem, running the Joomla/Mambo version may mean that you need to increase the PHP ***max_execution_time*** parameter.

It will be necessary to tune the frequency of JCheck runs to prevent the load on your server, we recommend some time between 1-4 hours between runs.

Monitoring Options

JCheck has two monitoring options:

- ☑ alerts can be sent to the admin by email
- ☑ alerts can be logged to a logfile

Either option can be switched on or off, but is recommended that both are used to ensure full coverage of events.

The JCheck logfile will also provide some information about the actual runs which are carried out, an extract from a sample log is shown below

```
[2007-06-11 Mon 20:05:55] [notice] JCheck: Starting run for: w:\www\joomla
[2007-06-11 Mon 20:05:55] [notice] JCheck: Site: http://localhost/joomla
[2007-06-11 Mon 20:05:55] [notice] JCheck: Licence: 123acbf
[2007-06-11 Mon 20:05:55] [notice] JCheck: Exclude: gif$, jpg$, png$, jcheck.db, jcheck.log
[2007-06-11 Mon 20:06:00] [notice] JCheck: Unable to load database
file(w:/www/joomla/modules/jcheck/jcheck.db) - assuming 1st run
[2007-06-11 Mon 20:06:01] [notice] JCheck: Initializing:
w:/www/joomla/modules/jcheck/jcheck.db
[2007-06-11 Mon 20:06:02] [notice] JCheck: Unable to send alert email to (fred@bloggs.com)
[2007-06-11 Mon 20:06:02] [notice] JCheck: Found (1703) differences since last run
[2007-06-11 Mon 20:06:02] [notice] JCheck:
JCheck Version :  0.5
Server         :  http://localhost/joomla
Last save      :  Jun 11 2007 20:06:00
This Run       :  Jun 11 2007 20:05:55
Directory      :  w:\www\joomla
Exclude        :  gif$,jpg$,png$,xml$,cache_,jcheck.db,jcheck.log
Additions since the last run

Added:w:\www\joomla/index.php
Type          : file
Permissions   : -rw-rw-rw-
Date Modified : May 26 2007 13:29:46
Date Changed  : Dec 24 2006 21:21:24
Owner         : 0
Group         : 0
Size          : 8794
MD5 key       : 1602fd9987bc5236a027e663c65b3e59
```

Appendix A JCheck Configuration

The following options are available to configure JCheck

Joomla/Mambo Module	Standalone	Description
Licence Key	$jc['licence']	Licence key for paid version. This enables some of the configuration options to be changed
N/A	$jc['livesite']	The site URL for the website (this is the value which is used when a licence is purchased.) This is supplied automatically by Joomla/Mambo and is generated by the php_uname function under cron
Run Frequency(Hours) [£]	$jc['run_freq'] [£]	How often (in hours) to run JCheck. In the free version this is fixed at 24.
Update Database	$jc['initialize']	Determines whether database should be automatically updated after each run. Default YES
Alert Email address	$jc['email']	Email address for alerts to be sent to
Email subject	$jc['email_subject']	Text to be sent in the subject line of email alerts, the Site URL as specified above will also be appended.
Alert Frequency	$jc['email_freq']	Determines when alerts are sent, this can be: Never(0), On every run(1), or only when a change is detected(2). Default CHANGE
Starting Directory	$jc['dir']	Top level directory for JCheck to start checking. All subdirectories will be recursively checked unless included in the exclude list. For Joomla/Mambo this is set to the Home directory by default.
File/dir patterns to exclude	$jc['exclude']	Comma separated list of file or directory patterns to exclude from checking. This can be used to prevent alerts where files are legitimately updated, e.g. log files, cache, or temporary files. Standard PHP regular expressions can be used.
Include Directory Check	$jc['incdirs']	This can be used to check if a directory has been changed, normally this would be picked up by file monitoring, but can be useful if only a

[£] Paid Version Only

		specific directory is being monitored. Default NO
Location of JCheck Database	$jc['database']	Path/Filename for JCheck database. This could be changed to make the database less visible, e.g. it could be moved to an images directory and called blank.png. Default jcheck/jcheck.db
Logging	$jc['logging']	Determines whether logging is on or off. Default ON
Location of JCheck Logfile	$jc['logfile']	Path/Filename for JCheck logfile. See notes for database above. Default jcheck/jcheck.log
Path to JCheck library	$jc['library']	Path/Filename for main JCheck library. See notes for database above. Default jcheck/jcheck.php
Show Logo [£]	$jc['logo']	On Joomla/Mambo modules this determines if the JCheck logo is shown or not, on the Free version the logo is always shown. For cron, this option has no effect.
N/A	$jc['cron']	Must be set when running as a cron job.

[£] Paid Version Only