



How to add exception for mySites.guru in Admin Tools

Admin Tools' .htaccess Maker gives mySites.guru a 403 on Joomla until plugins/system/bfnetwork is in the right exception list. Which one, and why backups fail.

Phil E. Taylor | 19 October 2026

A Joomla site running Akeeba's Admin Tools Professional can block mySites.guru in two separate places, with two separate symptoms. The .htaccess Maker returns 403 Forbidden to the connector itself, so connecting or reconnecting the site fails. The Web Application Firewall bans our IP after a handful of blocked requests, and the only thing that stops working is backups. This post is the reference for both: which list the exception goes in, what to type, what it writes into .htaccess, and why fixing one does nothing for the other.

mySites.guru already points you at the first fix. When the last connection error for a site contains a 403, the reconnect screen tells you to add the .htaccess Maker exception. For the second, the Backup tab spots the WAF ban during the twice-daily snapshot and clears it in one click. What follows is the long version, for anyone who wants to do it by hand or understand what the buttons change.

The short version

In the Joomla administrator go to Components, Admin Tools, Server Config. File Maker, open the .htaccess Maker and find the Server protection card. In the list labelled "Allow direct access, including .php files, to these directories" add a new row with the path `plugins/system/bfnetwork`, then choose "Save and create .htaccess". If audits run but backups fail with 403, that is the Web Application Firewall instead: click "Unblock our IP" on the site's Backup tab in mySites.guru, or add 178.62.5.35 to "Never block these IPs" in the WAF.

What Is Akeeba Admin Tools?

Admin Tools is a Joomla extension from Akeeba Ltd, whose founder and lead developer Nicholas K. Dionysopoulos has been building it since 2010. Akeeba also makes Akeeba Backup, the extension mySites.guru drives when it takes a backup of your Joomla site. Akeeba describes Admin Tools as "Administration and security improvements for Joomla! sites". It comes in two editions, Core (free) and Professional (paid), and there is a separate Admin Tools for WordPress with its own feature set.

Core covers the housekeeping side: Password-protect Administrator, Emergency Off-Line, Fix Permissions, Database Tools, Clean Temp-Directory, Temporary Super Users, Obsolete Core Files and the Site IP Allow List. Professional adds the parts that actively defend the site: the Web Application Firewall (with Configure WAF, automatic IP blocking of repeat offenders, the Site IP Disallow List and a Blocked Request Log), the .htaccess Maker along with an NginX Configuration Maker and a web.config Maker for other web servers, the PHP File Change Scanner, and a set of Joomla CLI commands. The current release supports Joomla 4.4 to 6.2.

We recommend it. One of mySites.guru's own checks, "Use A Joomla Core Or Akeeba Admin Tools .htaccess File", points you at the Admin Tools .htaccess builder because it produces a tighter file than Joomla's stock htaccess.txt, and in our own AcyMailing disclosure the Professional WAF **blocked a real SQL injection attack in its default settings**. Those two Professional features, the .htaccess Maker and the Web Application Firewall, are also the two that block mySites.guru, each in its own way. The rest of this post covers the two settings that let Admin Tools keep doing its job while mySites.guru does ours.

Which Admin Tools Block Is Your Joomla Site Hitting?

A 403 when you connect or reconnect the site, or on every audit, is the .htaccess Maker. Audits and snapshots running normally while every backup fails with 403 Forbidden is the Web Application Firewall. The two features do not affect each other, so match the symptom before changing anything, or you will fix the wrong one and conclude the fix does not work.

.htaccess Maker

Symptom: 403 Forbidden on connect, reconnect or audit, and nothing from mySites.guru works. Cause: Server Protection rules in .htaccess block any .php file under plugins/ before PHP runs. Fix: add plugins/system/bfnetwork to the list that allows direct access including .php files, then write the new .htaccess.

Web Application Firewall

Symptom: audits, snapshots and tools all work, but backups fail with 403 Forbidden. Cause: the WAF auto-banned the mySites.guru IP after repeated blocked requests, and backups are the one job that goes through index.php. Fix: click Unblock our IP in mySites.guru, or add 178.62.5.35 to Never block these IPs in the WAF.

How Admin Tools' .htaccess Maker Blocks the Joomla Connector

On Joomla, mySites.guru connects through a system plugin installed at `plugins/system/bfnetwork` . Its PHP files live one level down, in `plugins/system/bfnetwork/bfnetwork/` , and the service requests them directly over HTTPS rather than through Joomla's `index.php` . The connection test is `bfPing.php` ; audits, snapshots, tools, auto-login, restores and upgrades each have their own entry points, and there are more than fifty PHP files in that folder. We have written before about hosts misreading the bfnetwork connector plugin, and the .htaccess Maker misreads it in a similar way: as a stray PHP file in a folder where PHP should not run.

Server Protection is designed to stop that. With "Frontend protection" on, which is the default, the .htaccess Maker writes rules that only allow listed file types inside the "Frontend directories where file type exceptions are allowed". The default set is

components, modules, templates, files, images, plugins, media and libraries. PHP is not an allowed type, so any `.php` request under `plugins/` gets 403 Forbidden:

```
RewriteRule ^(components|modules|templates|files|images|plugins|media|lib
RewriteRule ^(components|modules|templates|files|images|plugins|media|lib
```

There is a second, site-wide option that does the same job more broadly: "Disallow access to all other PHP files throughout the site, unless they are explicitly allowed". It writes:

```
RewriteCond %{REQUEST_FILENAME} (\.php)$
RewriteCond %{REQUEST_FILENAME} -f
RewriteRule (.*\.php)$ - [F]
```

Either way Apache blocks the request before a single line of PHP runs. The connector does not see it and Admin Tools' own firewall does not see it either, which is why no WAF setting, allow list or log entry has any bearing on this 403. The fix has to be in the same place as the block: the generated `.htaccess`.

Adding the Exception in the Joomla .htaccess Maker, Step by Step

You need Admin Tools Professional; the free Core edition has no .htaccess Maker, and a Core site returning 403s has a different cause (covered at the end). Labels below are from Admin Tools 7.9.3. Older documentation and forum threads call the page the ".htaccess Maker", Admin Tools 7 lists it under Server Config. File Maker, and both names refer to the same page.

Check the label word by word before you type

Admin Tools puts three exception boxes one after another, and their labels are nearly identical:

"Allow direct access to these files"

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

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

The mySites.guru exception goes in the third box only, the one that says **including .php files** and ends in **directories**. The second box differs by a single word and looks right, but it keeps every PHP file blocked, so the connector still gets a 403. The first box is for single files: do not put `bfPing.php`, or any other connector file, in it by name. Allow the whole `plugins/system/bfnetwork` folder in the third box instead. If the connection still fails after you save, the wrong box is the first thing to check.

1. In the Joomla administrator go to Components, Admin Tools, Server Config. File Maker, and open the .htaccess Maker.
2. The page has no tabs. It is a stack of cards: "Basic security", "Server protection", "Custom .htaccess rules", "Optimisation and utility" and "System configuration". Open "Server protection".
3. Scroll to the sub-heading "Exceptions from Server Protection". These lists are only shown while "Backend protection" or "Frontend protection" is set to Yes, so if you cannot see them, that is why.
4. Find the third box, labelled "Allow direct access, including .php files, to these directories". Read the label to the end before typing: it must say "including .php files" and "directories". This box has one default row, `installation`, which is a good way to confirm you are in the right one. Leave that row alone.
5. Use the Add button to create a new row. Each row shows a fixed `/` in front of the text box, so enter the path with no leading slash, no trailing slash and no domain: `plugins/system/bfnetwork`. A full URL will not match.
6. Choose "Save and create .htaccess". The same dropdown also has "Save without creating .htaccess" and "Preview". If you use the plain save, Admin Tools reports "Changes have been successfully saved. Do not forget to apply them by creating the new .htaccess file" and the file on disk stays as it was, which catches a lot of people out.
7. On success Admin Tools reports "The new .htaccess has been written to disk". Your previous file is kept as `.htaccess.adminintools` in the site root, which is your rollback if anything else on the site objects.

If the site runs on NginX or IIS, the NginX Configuration Maker and the web.config Maker have the same three lists with the same labels and defaults. The same path goes in the same-named list, followed by "Save and create nginx.conf" or "Save and create web.config".

Which of the Three "Allow Direct Access" Lists?

Three lists sit next to each other under Exceptions from Server Protection, with similar names, and picking the wrong one is the commonest reason the fix "does not work". Their labels and defaults in 7.9.3:

Allow direct access to these files

Individual files. Defaults: the restore.php scripts of Akeeba Backup (com_akeeba and com_akeebabackup) and of Joomla Update (com_joomlaupdate), plus Joomla Update's extract.php, all under administrator/components. Wrong for mySites.guru, because the service calls many files in the connector folder and new ones arrive as features ship.

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

Whole directories, but PHP stays blocked. Default: .well-known. Looks right and does not help, because the files we need are the PHP ones.

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

Whole directories, PHP included. Default: installation. This is the one. Add plugins/system/bfnetwork here.

The first list is how Akeeba handles its own direct-access scripts: Akeeba Backup's **restore.php** is in it by default. Never use it for the mySites.guru connector. Listing **bfPing.php** or any other connector file by name lets that one file through while the

rest of the connector keeps getting 403, and every new release adds files the list does not know about. Allow the whole `plugins/system/bfnetwork` folder in the directory list instead.

What the Exception Writes into .htaccess

The third list writes one line into a block marked `##### Advanced server protection rules exceptions -- BEGIN` and `-- END`, which Admin Tools places before the `##### Advanced server protection -- BEGIN` block:

```
RewriteRule ^plugins\/system\/bfnetwork/ - [L]
```

Admin Tools escapes the slashes and dots for the regex. The `[L]` flag stops rewrite processing for anything matching that path, so the `[F]` rules further down do not apply to it. Compare that with what the “except .php files” list writes for the same path:

```
RewriteCond %{REQUEST_FILENAME} !(\.php)$  
RewriteCond %{REQUEST_FILENAME} -f  
RewriteRule ^plugins\/system\/bfnetwork/ - [L]
```

The first condition only matches requests that do not end in `.php`. Connector requests all end in `.php`, so they skip that rule, never stop at `[L]`, and fall through to the Forbidden rule as before. Side by side the mistake is easy to see. In the admin screen the two labels differ by one word.

A few rules are written before the exceptions block, so an exception does not bypass them: “Restrict access by IP” (default None, intended for sites behind a load balancer, reverse proxy or CDN), “Block access from specific user agents” (default Off), the common-exploits rewrite rules and file injection protection. If “Restrict access by IP” is set to a custom list, the mySites.guru IP 178.62.5.35 has to be on it as well, or the exception never gets a chance to apply.

Is a Directory Exception Safe on a Joomla Site?

Akeeba's documentation is blunt about the PHP list: "This option should be used sparingly as possible. Each and every directory placed in this list is no longer protected by Server Protection AT ALL", and it recommends the per-file list wherever that will do. For a random folder, we agree. The connector is a case where the directory list is the right tool.

The service calls many files in that folder directly, and the set changes between releases, so a per-file exception breaks with no warning the first time a release adds an entry point. And every request to the connector is encrypted and must include your site's connector key, so letting Apache pass a request to PHP is not the same as letting anyone use it.

Keep the exception to `plugins/system/bfnetwork`, not `plugins` or `plugins/system`, and leave the rest of the Server protection card as it is. Server Protection should stay on: it is the feature that disables PHP in a list of directories, which is where an upload flaw drops its payload. We also stand by what we said about treating .htaccess as a security layer: it limits damage after a compromise, and an exception for one authenticated folder does not change that.

Checking the Fix Worked on Your Joomla Site

The quickest test is a request for the connection test file from your own machine, before and after writing the new .htaccess. Replace example.com with the site:

```
curl -sI https://example.com/plugins/system/bfnetwork/bfnetwork/bfPing.php
```

Before the fix the first line is `HTTP/2 403` (or `HTTP/1.1 403 Forbidden` on older servers). After the fix, anything other than 403 means the server let PHP run. The file expects an encrypted request, so it will not print anything useful to a browser or to curl, and that is fine; the status code is what you are testing. `bfPing.php` is only the file the test requests; the exception is still the whole folder, never this file on its own. Then in mySites.guru, run the test connection for the site from the reconnect screen, or refresh the site.

You can also open the site's `.htaccess` and search for `bfnetwork`. The line should be inside the exceptions block, above the Advanced server protection block. If it is below it, or missing, the file on disk was not regenerated after the setting changed.

Doing It from the Command Line on Many Joomla Sites

Admin Tools Professional 7.x includes Joomla CLI commands, and for an agency with dozens of sites that is a better route than clicking through each administrator. These are taken from the Admin Tools 7.9.3 command definitions:

```
php cli/joomla.php admintools:htmaker:get --key=fullaccessdirs
php cli/joomla.php admintools:htmaker:set --key=fullaccessdirs --add=plugi
php cli/joomla.php admintools:htmaker:make
php cli/joomla.php admintools:ipallow:add --ip=178.62.5.35 --description='
```

`fullaccessdirs` is the field behind "Allow direct access, including .php files, to these directories". Run `htmaker:get` first so you can see what is already there, and `htmaker:make --preview` before the real `make` so you can check the generated file before it is written. The last command is the WAF side of the job, covered next; it adds our IP to the Site IP Allow List so the firewall never bans it in the first place.

Why Joomla Backups Fail When Everything Else Works

Admin Tools Professional's Web Application Firewall bans an IP after repeated blocked requests. The defaults in 7.9.3 are "IP blocking of repeat offenders" on, "Block IP after this many blocked requests" 3, "Time period" 10, "Unit of time measurement" second, with an optional "Add persistent offenders to the IP Disallow List" that is off by default. Three blocked requests in ten seconds and the IP is banned.

Every mySites.guru request comes from one IP, 178.62.5.35 (the uptime monitor is separate, on 165.227.239.229, and the full list is at [our IP addresses](#)). So a ban applies

to the whole service at once. What makes it hard to spot is that most of the service never notices.

The WAF hooks Joomla's `onAfterInitialise` event. The connector never boots Joomla that far, so audits, snapshots and tool calls go straight past a live ban as if it were not there. A backup is the exception: mySites.guru drives Akeeba Backup through the site's own `index.php`, a full Joomla request, so a banned IP gets 403 Forbidden on every backup while everything else on the site's page looks healthy. Audits fine, backups 403, is the signature.

What the ban does to backups

From our own measurements across connected Joomla sites: of the sites found with our IP banned by Admin Tools, roughly 44% had their last backup rejected. On Admin Tools sites where we are not blocked, the figure is 0.6%.

If a site's last backup failed with 403 and Admin Tools is installed but no ban was found in its tables, mySites.guru says so and does not offer the unblock button, because a 403 has many causes and clearing a ban that does not exist fixes none of them.

Clearing an Admin Tools IP Ban from mySites.guru

During each snapshot, and snapshots run twice a day, mySites.guru looks in the Admin Tools block tables, both the manual block list and the automatic ban list, for the IP the request came from. If it is there, the site is flagged BLOCKED by the check "Unblock mySites.guru IP in Akeeba Admin Tools", and the site's Backup tab shows "Akeeba Admin Tools has blocked our IP" with an "Unblock our IP" button.

"Unblock our IP" removes our IP from the manual block list, the auto ban list and the auto ban history, then adds it to the Admin Tools Site IP Allow List with the description "mySites.guru management IP - auto allow-listed". It works while the ban is live because it travels the connector route the WAF never sees. It acts only on our own IP and changes no other Admin Tools setting.

Unblock mySites.guru IP in Akeeba Admin Tools

mySites.guru checks every connected site for this automatically and flags it the moment it appears. These run twice a day on every connected site.

It can also fix this across every connected site with one click.

[Check your site for free →](#)

If you would rather not click it every time, there is a per-site setting under Config, Advanced: "Automatically whitelist mySites.guru in Admin Tools", with the toggle "Clear the block automatically". With that on, a snapshot that finds us blocked clears the ban and allow-lists us without waiting for you. It only writes when it finds us blocked, never on a routine snapshot, so your scheduled backups keep running without anyone babysitting the WAF. The one-click unblock arrived with a batch of other features, and the auto-clear toggle is the version of it you set once and forget.

The manual alternative inside Admin Tools is Configure WAF, "Exceptions", "Never block these IPs": add 178.62.5.35. Akeeba's WAF Exceptions documentation recommends that list for "known external servers accessing your site (e.g. payment service providers sending callbacks to your site, site scanners, Cloudflare, Sucuri, etc)". The separate "Site IP Allow List" page, which describes itself as being for "known, vetted services and servers", does the same job; in the 7.9.3 code both lists make Admin Tools skip its checks for that IP entirely. Either is fine.

The two fixes in this post are not interchangeable, and this is where most people go wrong. An IP allow-list entry in the WAF does nothing for a .htaccess Maker 403, because Apache blocks the file before PHP, and so Admin Tools, ever runs. A .htaccess Maker exception does nothing for a WAF ban on backups, because backups go through **index.php**, which the exception does not touch. Akeeba staff have said as much: the

WAF and the .htaccess Maker do not affect each other. Most sites with Admin Tools Professional need both.

Admin Tools for WordPress Uses Different Labels

Admin Tools for WordPress Professional has its own .htaccess Maker with an “Exceptions” section, and the wording is different from the Joomla edition. The four lists are “Files which will always be made accessible”, “Directories where all files except .php will be accessible”, “Directories where all files including .php will be accessible” and “Directories where only files with allowed extensions will be accessible”.

On WordPress the connector is at `wp-content/plugins/mywpguru` , with its files in `wp-content/plugins/mywpguru/bfnetwork/` . The labels are just as easy to mix up as on Joomla, with four near-identical boxes this time, so read each one to the end. Add `wp-content/plugins/mywpguru` only to “Directories where all files including .php will be accessible”, which has `wp-content/upgrade` in it by default, then “Save and create .htaccess”. Akeeba’s [Server Protection documentation for WordPress](#) covers the page, and its WAF Exceptions documentation names “a third party site management service” as the kind of thing you do not want the firewall blocking. The one-click unblock in mySites.guru is Joomla only, so on WordPress add our IP to the WAF exceptions by hand.

No Admin Tools but Still a 403 on Joomla?

Then something else wrote the rule. Check `/.htaccess` , `/plugins/.htaccess` and `/plugins/system/.htaccess` for a `<FilesMatch>` block that denies `.php` with `Deny from all` . A root `.htaccess` often pairs that deny with an allow list of known core files, and the connector is not on it. Hand-written rules like these need the same `bfnetwork` exception written in whatever style the file already uses.

If none of that is present, the 403 is coming from a server firewall blocking our IP rather than from the site. Hosts do this in several shapes, including [a bot challenge in front of](#)

the whole site, and the fix is the same each time: send the host our IP addresses and ask for them to be allowed.

Admin Tools hardens the site and mySites.guru watches it, and the two settings in this post let both do their job at once. If you look after more than a couple of Joomla sites, having the ban detected and cleared for you is a small part of what the subscription does twice a day on every site you connect.

Further Reading

- [Admin Tools for Joomla: Server Protection](#) - Akeeba's own documentation for the .htaccess Maker, including the three exception lists and the warning about the PHP one
- [Admin Tools for Joomla: WAF Exceptions](#) - the Never block these IPs list and what Akeeba recommends it for
- [Admin Tools FAQ: IP allow lists](#) - how an allow-listed IP is treated by the Web Application Firewall
- [Admin Tools for WordPress: Server Protection](#) - the WordPress edition's .htaccess Maker and its differently worded exception lists
- [mySites.guru IP addresses](#) - the current list of IPs our service and uptime monitor connect from

Frequently Asked Questions

Which Admin Tools .htaccess Maker list does the mySites.guru exception go in?

The third one, labelled Allow direct access, including .php files, to these directories. Add plugins/system/bfnetwork as a new row and use Save and create .htaccess. The list is inside the Server protection card under Exceptions from Server Protection, and it only appears while Frontend protection or Backend protection is set to Yes.

Can I allow just bfPing.php in Allow direct access to these files?

No. Never add bfPing.php or any other connector file by name. The service calls many files in the connector folder, and each release can add more, so a per-file entry lets the connection test through while audits, snapshots and everything else still get 403. Allow the whole plugins/system/bfnetwork folder in Allow direct access, including .php files, to these directories.

Do I need a leading slash on plugins/system/bfnetwork?

No. Each row shows a fixed slash in front of the text box, so you type the relative path with no leading slash, no trailing slash and no domain. A full URL starting with https:// will never match anything.

Why does the except .php files list not fix the 403?

Because the files the mySites.guru service requests are all PHP. That list writes a rule that only lets non-PHP files through, so every connector request still falls through to the Forbidden rule and you get the same 403 as before.

Does allow-listing the mySites.guru IP in the Admin Tools WAF fix the .htaccess 403?

No. A .htaccess Maker 403 is issued by Apache before any PHP runs, so Admin Tools never sees the request and its IP allow list is never consulted. The WAF allow list fixes the other problem, where a WAF ban stops backups. Most sites with Admin Tools Professional need both.

Is it safe to give a whole directory direct access, including .php files?

For plugins/system/bfnetwork, yes. Every request to it is encrypted and must include your site's connector key, and the service calls many files in that folder directly, which change between releases. Scope it to exactly that path, never plugins or plugins/system, and leave Server Protection on for everything else.

Does the free Admin Tools Core edition have the .htaccess Maker?

No. The .htaccess Maker is in Admin Tools Professional only. If a site running the Core edition returns 403 to mySites.guru, the cause is a hand-written .htaccess or a rule on the host, not Admin Tools.

AI MODIFIED

Written and edited by a human, with AI assistance. [Our approach to AI](#)

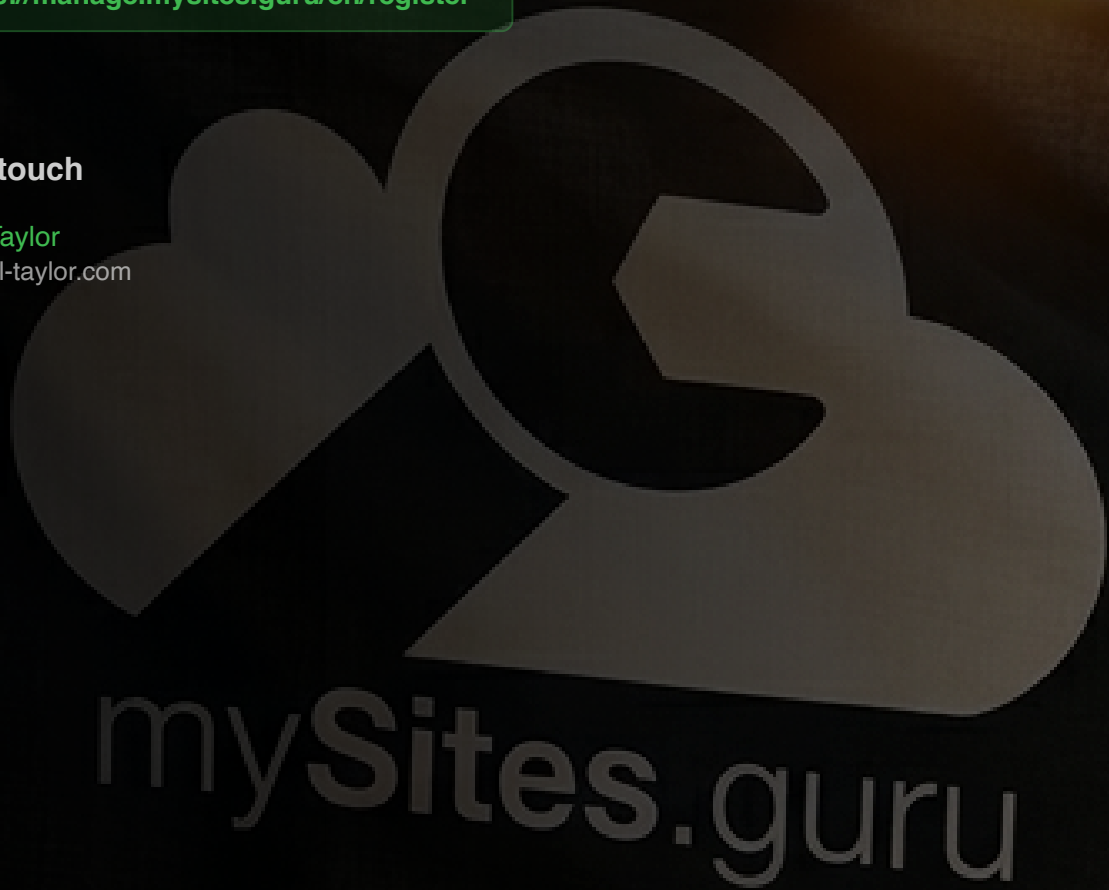
Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.
No credit card required.

<https://manage.mysites.guru/en/register>

Get in touch

Phil E. Taylor
phil@phil-taylor.com



© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

mysites.guru