mySites.guru

How To Force MFA on Super Users Across Every Joomla Site You Manage

Joomla 6.1 is the first version that lets you require MFA for Super Users. On the 71% of sites still below it, the setting is not reachable at all.

Phil E. Taylor | 15 September 2026

Joomla has had a setting to require Multi-Factor Authentication for a whole user group since 4.2, released in August 2022. Write-ups of it, our own included, told you to add the Super Users group to the list.

You could not. Until Joomla 6.1.0 shipped on 14 April 2026, the Super Users group was filtered out of that field, so the one group with the power to install extensions, edit template files and create more administrators was the one group the setting would not accept. The option looked available, and selecting it was impossible.

That is now fixed, which makes this worth doing on any site you manage that is new enough to allow it. Across the Joomla sites mySites.guru monitors, 3.8% of sites on 6.1 or newer enforce MFA for Super Users, and 71% of monitored Joomla sites are still on a version where the field will not offer the group at all. The check behind those figures is Force Multi-Factor Authentication For Super Users, which reads the setting on every connected site twice a day.

What changed in Joomla 6.1

The setting is `forceMFAUserGroups`, a list of user groups whose members must enrol an MFA method before Joomla will let them use the site. From 4.2.0 through 6.0.4 the field in `com_users` was declared like this:

```
<field name="forceMFAUserGroups" type="usergrouplist"
       label="COM_USERS_CONFIG_FORCEMFAUSERGROUPS_LABEL"
       checksuperusergroup="1" ... >
```

That attribute is read by `UsergrouplistField`, which drops any group holding `core.admin` from the list of options:

```
$checkSuperUser = (int) $this->getAttribute('checksuperusergroup', 0);
...
foreach ($groups as $group) {
```

```
    // Don't list super user groups.
    if ($checkSuperUser && Access::checkGroup($group->id, 'core.admin')) {
        continue;
    }
```

Joomla's shipped permissions give `core.admin` to group 8, Super Users, so the group never appeared in the dropdown for anyone. Pull request #46248, merged on 9 January 2026 for the 6.1.0 milestone, removed the attribute, and its own description is blunt about the state of things beforehand: "Its not possible to force or never force MFA for superusers."

The restriction lived entirely in the configuration form. Enforcement itself is a plain intersection of the stored group list with the groups the user belongs to, with no test for administrator rights anywhere in it, so the feature always worked on Super Users. What did not work was choosing them.

The attribute is still on the field in the Joomla 5 branch. Joomla 5 is in bugfix mode, so it is not coming back to 5.x.

How do I force MFA on the Joomla Super Users group?

There are two answers, and which one you want depends on whether you look after one Joomla site or fifty.

Across your whole portfolio, in mySites.guru

The check is Force Multi-Factor Authentication For Super Users, and it has an all-sites view: one page listing every connected Joomla site eligible for it, each row showing whether that site currently enforces MFA on Super Users. Every row has a toggle. Flip it and mySites.guru adds the Super Users group to `forceMFAUserGroups` on that site for you, so there is no administrator login, no password manager round trip and no tab per client.

Toggling it back off removes only the Super Users group and leaves any other groups you have enforced in place, which matters on sites where somebody has already set up MFA for Administrator or Manager.

The same page is the audit. Sites that already enforce it read as fine, sites that do not are the queue, and the twice-daily snapshot keeps both current, so next month's answer is the same page rather than another sweep. If your sites are not connected yet, a free audit is the quickest way to see which of them are exposed here.

On a single site, by hand

On a Joomla 6.1 or newer site:

1. Log in to `https://yoursite.com/administrator`.
2. Go to Users, then Manage, then Options at the top right.
3. Open the Multi-factor Authentication tab.
4. Add Super Users to the field labelled **Enforce Multi-factor Authentication**.
5. Save.

The requirement attaches to the group, so a Super User account created next year inherits it without anyone going back. The field directly above it, Disable Multi-factor Authentication, is the opposite list, and enforcement wins where a group somehow appears in both.

Either route leaves the same step outstanding, and it is the one most instructions skip: log in as each existing Super User and enrol them there and then, saving the backup codes at that moment. Saving the setting only schedules the work.

> **Super Users, not Super Admins**
>
> Joomla's group is called Super Users. "Super Admin" is the phrase everyone reaches for in conversation, and going by search results it is mostly the phrase people use once a site has already been compromised.

Why did so few Joomla sites force MFA before 6.1?

Because they could not. The usual explanation for low adoption of an optional security setting is apathy, and this one was measuring something else entirely.

3.8%
of monitored Joomla 6.1+ sites enforce MFA for Super Users
the option has existed there since April 2026

0.1%
of Joomla 4.2 to 6.0 sites have it set
not reachable through the admin interface

71%
of monitored Joomla sites are on a version that cannot
mostly Joomla 5

Latest snapshot per site, 90-day window, across the Joomla sites mySites.guru monitors.

The 0.1% is the interesting residue: sites where the Super Users group reached that parameter through a database edit or a migrated configuration, and where Joomla duly enforces it, holding a setting their own administrator screen would never have offered them. It is fragile in a way worth knowing about, too. The next time anyone opens that options tab and saves, the field re-renders without the group and drops it again, with no warning that a security control just came off.

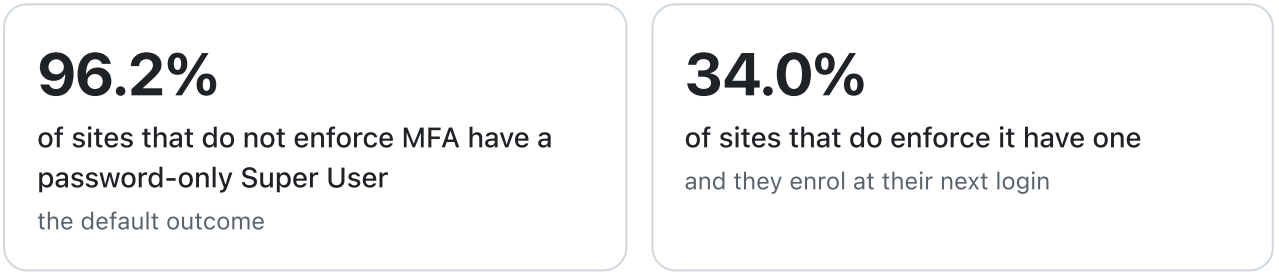
None of that changes what the accounts themselves look like. On 93.4% of monitored Joomla 6.1+ sites there is at least one Super User with no MFA method enrolled, and across all monitored Joomla sites it is 95.8%. Full administrative control, and a password is the only thing in front of it.

Passwords fail in ordinary ways that have nothing to do with how strong they are. One reused on a forum that later gets breached turns up in a credential-stuffing list, and bots work those lists against `/administrator` login forms continuously, without anyone deciding to target you. A user enumeration bug in an extension supplies

the usernames to try. A dormant account no one has used in six months is still a valid login.

Does forcing MFA on Joomla Super Users change anything?

It does, measurably. Split the monitored Joomla sites by whether the setting is on, then count how many still have at least one Super User with no second factor enrolled:



Same window and method. Enforcement is the difference between the two columns.

It does not reach zero, for a mechanical reason rather than a disappointing one. Joomla prompts an account to enrol when it next logs in, so a Super User who has not signed in since you saved the setting still reads as un-enrolled. That remaining third is a queue of accounts waiting for their owners to turn up.

That has a use when auditing a portfolio. A site that enforces MFA and still shows several un-enrolled Super Users is telling you those accounts have not been logged into since, which is usually the moment to ask whether they should exist at all.

What to do on the Joomla 5 sites that cannot enforce it

Seven in ten monitored Joomla sites are on a version where this option does not exist, so “switch it on everywhere” is not a plan on its own. Three things do work today:

- Enforce MFA on the groups Joomla will let you select. Administrator and Manager have been available since 4.2, and on most client sites those accounts can do enough damage to be worth protecting.

- Enrol the Super Users by hand and then watch the state, rather than trusting that it stayed done. mySites.guru counts Super User accounts with no MFA method at each snapshot, which is the part that is still true after a staff change.
- Treat it as one more reason the move off Joomla 5 has a date attached. Joomla 5 leaves bugfix support in October 2026, and this is a security control that is only ever going to exist on the newer branch.

What forced MFA still does not cover

Enforcement is worth having, and there are routes into an administrator account that go around it. These are in Joomla's own source rather than in anyone's threat model.

Silent logins skip it by default. "Multi-factor Authentication after silent login" defaults to off, and the silent response types default to `cookie, passwordless`, so a Remember Me cookie or a passkey login goes straight in without an MFA challenge. If you want the second factor on all of them, that switch needs turning on, and it sits on the same tab you were just in.

API tokens and the CLI never see it. Joomla's MFA handler is used by the site and administrator applications only, and the core documentation for it says an application designed to work non-interactively "MUST NOT use this trait". A Super User's API token is therefore a password-free route into the site that enforcement does not touch. If you use Joomla's Web Services, the tokens deserve the same attention as the logins.

Backup codes alone do not count. Joomla treats an account whose only method is backup codes as having no MFA at all, which is correct and also means an account can look enrolled to a person and un-enrolled to the system.

Rolling it out without a lockout queue

Flipping the setting is the easy half. The half that decides whether your Monday is quiet is people, and no toggle covers that.

Worth doing before you turn it on anywhere:

- Work out who the Super Users are first. Most sites have more of them than the person paying the invoice expects: an old developer, an agency handover account, a vendor's support login. Finding rogue admin accounts across every Joomla site you manage covers the search, and enforcing MFA on an account no one recognises is worse than deleting it.
- Tell people the day before rather than the morning of. The enrolment prompt is not self-explanatory to someone who has never seen it, and the support call it generates is entirely avoidable.
- Make everyone save their backup codes while they are enrolling, because that is the only moment anyone ever will, and on a Super User account it is the difference between a five-minute problem and a database edit.
- Keep the recovery path in mind before you need it. Joomla only lets a Super User's MFA methods be deleted by that same user, so a second Super User cannot rescue the first. Backup codes, or `DELETE` from the user MFA table, are the whole list.

> **Remove the account, do not exempt it**
>
> The temptation on rollout is to leave one account out of the enforced group so there is always a way in. That account then becomes the one an attacker wants, and it will be the one with the oldest password. If an account cannot hold a second factor, it should not hold Super User rights.

MFA enforcement is not a substitute for patching Joomla

Enforcing MFA assumes the implementation underneath it is sound, and three times this year it was not. Joomla fixed CVE-2026-48896 and CVE-2026-48897, both MFA authentication bypasses, in 5.4.6 and 6.1.1, and CVE-2026-73337, another one, in 5.4.8 and 6.1.3. All three were insufficient checks in the same area of the captive-page logic. The patch order for those ten CVEs is worth reading if you are running either branch behind.

The rest of the login path matters on the same terms. Enforced MFA sits alongside not shipping a Super User called admin, keeping the administrator session separate from the front end, and not emailing people their passwords in plain text. Each closes a different part of the same route, and a stolen session cookie does not care how you logged in originally.

Checking it is still enforced next month

Settings drift. A restore from a backup taken before the rollout, a hand-edited configuration, a site rebuilt by someone else: any of those undoes the work with no warning, and Joomla says nothing about it.

That is the argument for reading the setting on a schedule rather than trusting a finished checklist. Because the check runs at each snapshot, a setting that comes back off changes state on the all-sites page the same week, rather than waiting for someone to notice at the next annual review. The full list of checks shows what else is read in the same pass.

The wider pattern is the one the numbers keep making. Across every optional security setting we measure, adoption sits somewhere between rare and almost non-existent, which is the subject of what site audits reveal about Joomla and WordPress security. Forced MFA on Super Users spent three and a half years as a setting that looked optional and was actually unavailable. Now that it is real, it is the cheapest thing on that list to fix.

Frequently Asked Questions

Which Joomla versions can force MFA on Super Users?

Joomla 6.1.0 and newer, released 14 April 2026. The forceMFAUserGroups setting has existed since Joomla 4.2, but until 6.1 the field carried checksuperusergroup=1, which filtered every group holding core.admin out of the dropdown. The Super Users group was therefore not selectable by anyone, including a Super User.

Can I force MFA for Super Users on Joomla 5?

Not through the administrator interface. Joomla 5 is in bugfix mode and the attribute that blocks it is still on the field, so it will not be backported. You can force MFA on other groups such as Administrator and Manager on Joomla 4.2 and newer, and on Joomla 5 the realistic options are to enrol each Super User by hand and check the enrolment state regularly, or to plan the move to 6.1.

What is the setting actually called in Joomla?

Enforce Multi-factor Authentication, under Users, then Manage, then Options, then the Multi-factor Authentication tab. The stored parameter is forceMFAUserGroups. The field directly above it, Disable Multi-factor Authentication, is the opposite list, and enforcement wins where a group appears in both.

Does forcing MFA lock out a Super User who has not set it up yet?

No. Joomla redirects the account to the MFA setup page at its next login and blocks the rest of the site until a method is enrolled. No one is locked out at the moment you save the setting.

What happens if a Super User loses their phone?

They use their backup codes. Another Super User cannot clear it for them: Joomla only allows a Super User's MFA methods to be deleted by that same user, so if the codes are gone too, the records have to be deleted from the user MFA table in the database directly. That constraint is the reason to make backup codes part of the enrolment step rather than an afterthought.

Does a Remember Me or passkey login still ask for MFA?

By default, no. Multi-factor Authentication after silent login defaults to off, and the silent response types default to cookie and passwordless, so a Remember Me cookie or a passkey

login skips the MFA challenge. Switch that setting on if you want the second factor to apply to every route into the administrator.

Is forcing MFA enough on its own?

No. Joomla has fixed three MFA authentication bypasses in 2026, CVE-2026-48896 and CVE-2026-48897 in 5.4.6 and 6.1.1, and CVE-2026-73337 in 5.4.8 and 6.1.3. Enforcement assumes the implementation underneath it is patched, and API tokens and CLI access bypass MFA by design.

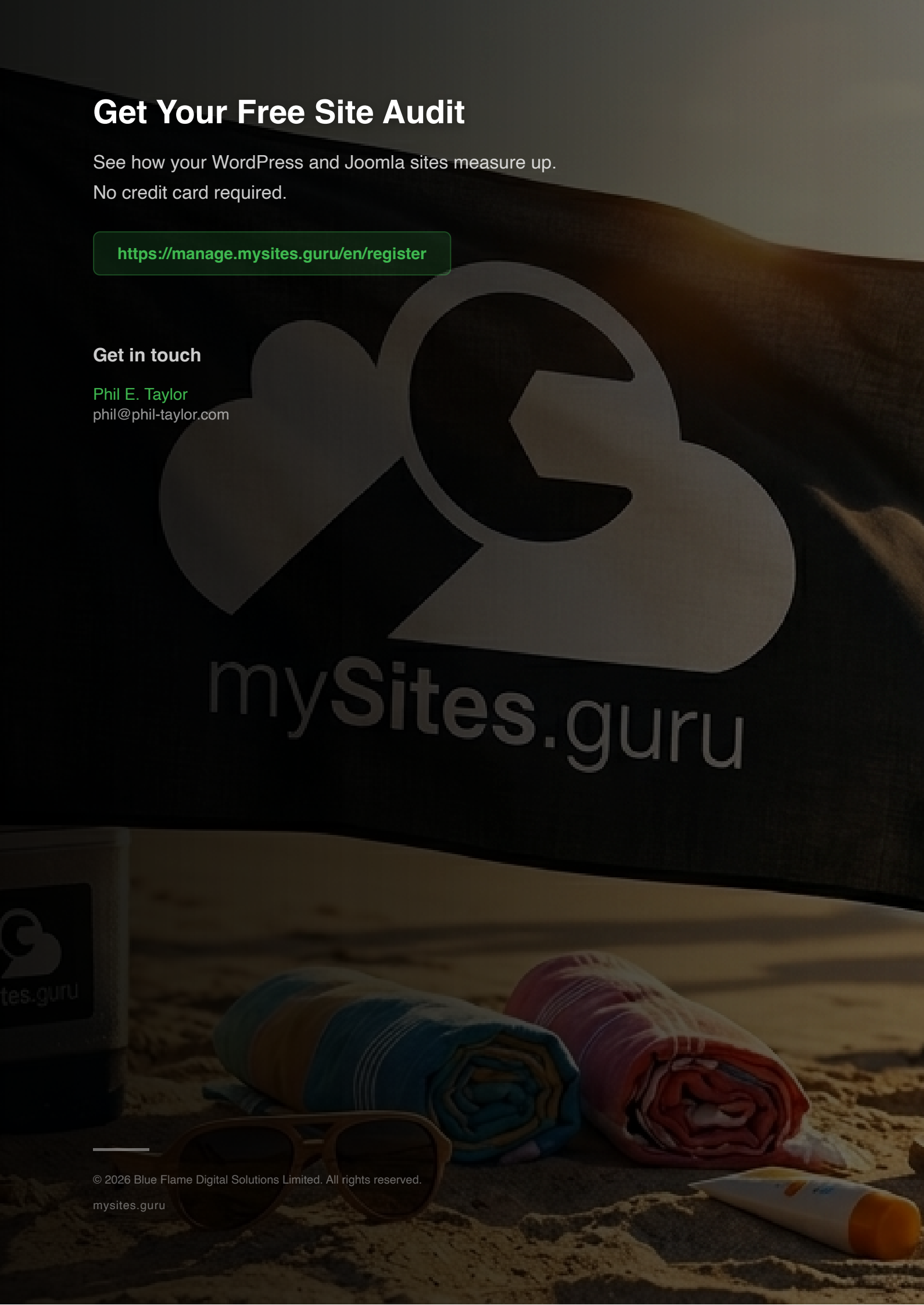
Written and edited by a human, with AI assistance. Our approach to AI

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