ModSecurity in cPanel: Your Site Firewall, and When to Turn It Off for One Domain

cPanel Guides · https://www.hyyat.com/en/knowledgebase/modsecurity-cpanel/

In short ModSecurity is a firewall that checks every request to your site and blocks those that look like attacks. If you get a **403** or **406** error when saving a page or sending a form, ModSecurity may have stopped a harmless request. Do not turn it off for the whole site; send support the time and URL so we exclude only the rule responsible.

Embedded media: https://www.hyyat.com/wp-content/uploads/2026/11/hyyat-cpanel-modsecurity-en.mp4?_=1

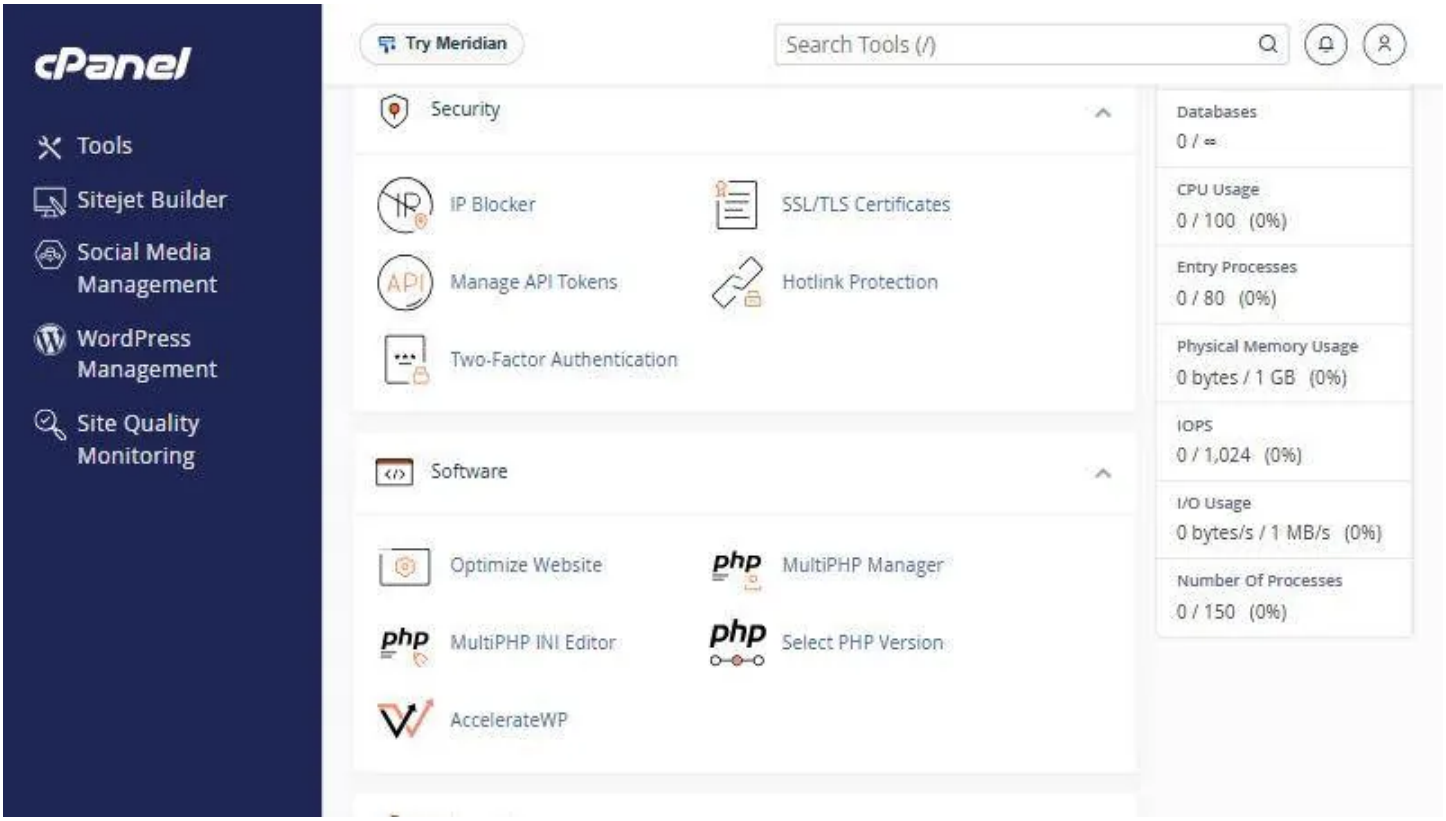
A question we often get: "I try to save a WordPress post and get Forbidden. When I remove part of the text, it saves."
That is a classic ModSecurity case. The text contains something that looks like code, such as a script tag or an SQL statement in a tutorial, and the firewall takes it for an attack. The firewall was over-cautious; the fix is not to switch it off but to exclude the rule that misfired.

What ModSecurity does

It sits between visitors and your site and compares every request with rules describing known attacks: SQL injection, code injection, attempts to read system files and abusive bots. A matching request is refused before it reaches WordPress or any other software. To understand one of the best known attacks, read what SQL injection is.

Signs ModSecurity blocked a harmless request

- A 403 Forbidden or 406 Not Acceptable error when saving or submitting, not when opening the page.
- The problem only happens with certain text or a certain file.
- A line in the Errors tool containing ModSecurity and a rule number (id).



The ModSecurity tool in cPanel

On some servers a ModSecurity tool appears in the Security section, with an on and off switch per domain. If you do not see it in your panel, the firewall is managed on the server side and our support team adjusts it.

Never switch the firewall off for the whole site to fix one form. That opens the site to every attack it was quietly stopping each day.

The right way to fix it

1. **Reproduce the error once** and note the time to the minute and the page URL.
2. **Open the Errors tool** and copy the line mentioning ModSecurity if there is one.
3. **Send a support ticket** with the time, the URL and the line.
4. **We exclude the rule** for that path or domain only, and the firewall keeps protecting the rest of the site.

Common errors that are not the firewall

Error	Likely cause
403 on the whole site	Wrong file permissions, a rule in .htaccess, or an IP block
500 when saving	A WordPress plugin error; check the Errors tool
413 when uploading	The file is larger than the PHP limit

From our support desk

- **A tech blog** that publishes code in its posts failed to save every post containing an SQL statement. Excluding one rule for the save path in the WordPress dashboard fixed it without weakening the rest of the site.
- **A contact form** rejected messages containing many links. A spam-prevention rule was the cause, and the fix was adjusting the form, not switching the firewall off.
- **A product import plugin** sent large files that the firewall refused. Uploading the file with File Manager and importing from the server got round it.

Frequently asked questions

Is ModSecurity active on my hosting?

The firewall runs at server level. If its tool appears in Security, it lets you control it per domain.

Does ModSecurity slow my site?

Its effect on speed is tiny compared with the protection it gives.

How do I know the error comes from it?

Look for the word ModSecurity in the Errors tool in Metrics.

Can I exclude a rule myself?

On shared hosting it is done through support so server security is not affected.

Does ModSecurity protect me from every attack?

It stops many known attacks, but it does not replace updates and strong passwords.

Does the error look the same on every site?

No, it may be 403, 406 or a generic error page, but the line in the Errors tool names the cause.

Related guides

- Block an IP Address or a Whole Range from Your Website in cPanel
- Track Website Errors and Logs in cPanel: the Errors and Raw Access Tools
- What Is SQL Injection and How to Protect Your Website Database
- Turn On Two-Factor Authentication in cPanel: Protection Even If Your Password Is Stolen
- The Security Section in cPanel: IP Blocker, SSL Certificates, Two-Factor Authentication and Hotlink Protection

All cPanel guides →

Need this service from Hyyat Host?Our team handles it for you, with support replying to tickets within 24 hours at most.

Saudi domain reservationDomain Availability Check