HTProtect

Joomla Security – always up to date.

JOOMLA SECURITY

Documentation

HTProtect – secure your Joomla website with ease. Overview, back-end protection, protection shield, site scan, backups & updates and help – short and beginner-friendly.

htprotect.org · As of: July 2026

Documentation

HTProtect – Documentation

HTProtect isn't a rigid lock, it's a protection that thinks along for your Joomla site: layered, always up to date – and it never locks you out. This guide shows chapter by chapter **what** exactly happens, **when** it happens, and **why** that keeps you safe.

What is HTProtect?

HTProtect is a "server shield" for Joomla that watches several places at once. Three things set it apart:

- **A mini-firewall that updates itself live.** When a new attack method or a fresh flaw in a popular extension becomes known, HTProtect blocks the attack path automatically – you don't have to wait for the vendor's update first. Experts call this *virtual patching*.
- **It keeps itself up to date.** HTProtect installs its own updates automatically, usually within about three hours – without you doing anything, the protection is always on the latest state.
- **It never locks you out.** Every protection rule is tested on the real server after it's written, and automatically taken back if needed.

On top of that come server hardening, an extra password in front of the back end, a malware scanner and automatic updates with backups. HTProtect refreshes its protection data the way an antivirus refreshes its virus definitions: it regularly *downloads* public, signed data – it does not send out site- or person-related data unasked.

For most people, one click is enough

The normal case is a single click on **"Secure now"** in the overview – everything else happens automatically. And no need to worry: HTProtect does not break anything. Before every change it makes a backup, checks itself, and automatically rolls back if something goes wrong.

Download HTProtect

Overview

The overview is your cockpit. A **security traffic light** shows at a glance where you stand: green means all good, orange is a hint, red means action needed. Orange or red items are clickable – they take you straight to the fix. The big **"Secure now"** button does everything important in a single click.

To keep that light accurate, **the guardian** works in the background. It runs first on *every* page load – with practically no noticeable delay – keeps the mini-firewall current and watches over the integrity of the protection shield. Read-only, it also detects injected code in the core and active template files and reports it.

Anything suspicious about your accounts catches its eye too – a new Super User, a secretly changed password. It notifies you by email, bundled and in the language of your back end, and only when something is really wrong. So no spam.

What happens when

The protection follows a fixed rhythm – most of it without you ever doing a thing:

1. **At installation**
   HTProtect sets itself up but does not arm anything yet. You decide when it starts.
2. **One click on "Secure now"**
   The shield is written, the upload folders are sealed off, everything is tested on the real server, and your safe downloads are released automatically.
3. **On every page load**
   The guardian checks the firewall and integrity – imperceptibly fast.
4. **Regularly in the background (about every 6 hours)**
   HTProtect fetches the signed feed and keeps the mini-firewall and its knowledge of vulnerabilities current. Security-critical entries take effect at once.
5. **About every 3 hours**
   HTProtect checks for its own updates and installs them automatically.
6. **At the scheduled time**
   Optional auto-updates for your extensions – with a backup, a health check and an automatic fallback.

Back-end password protection

In front of the Joomla login, HTProtect places a **second password prompt** – right before the back-end address (the one ending in `/administrator`). Attackers and bots never even reach the login page. It's an extra hurdle, and it protects even against flaws in the login itself that nobody knows about yet.

1. **Choose a username and password**
2. **Turn the protection on – done**

And the fair worry "what if I lock myself out?" – HTProtect takes that off your hands: it tests the lock on the real server and switches back automatically if something isn't right. An existing password protection it simply adopts.

Forgot the password? No problem: delete the file `administrator/.htaccess` via FTP – the extra prompt is gone and you can get back into the back end.

Protection shield

The protection shield is the server layer of your defence: a hardened `.htaccess` following the principle "everything forbidden except what is needed". One click on **"Secure now"** is enough – the recommended settings are already in place. Everything else sits collapsed under **"Advanced settings"** (for pros; when in doubt, just leave it).

Behind it, several layers interlock:

- **Upload folders sealed.** In folders you can upload to (uploads, media, cache, tmp), running PHP is completely disabled. The most common way in – an uploaded web shell – runs into a dead end (403).
- **Sensitive files hidden.** Direct access to `configuration.php`, backups, log files and the like is blocked.
- **Protective headers & HTTPS.** Security headers are set; if your site runs on HTTPS, HTProtect automatically redirects unencrypted requests to the secure connection (switchable).
- **Web Application Firewall.** Known attack patterns are caught *before* Joomla – the attack never even reaches your site.

The mini-firewall: protection that doesn't age

Here's the clever part: those patterns aren't set in stone. HTProtect regularly – about every 6 hours – syncs with a **signed feed**, exactly the way an antivirus refreshes its virus definitions. When a new attack method or a fresh flaw in a popular extension becomes known, the matching block rule is added automatically – the attack path is closed **before** there's even an official update for the vulnerable extension. Security-critical entries take effect at once, not only at the next sync.

So no one can abuse that channel, the feed's signature is verified right on your site – only untampered data is accepted.

HTProtect never locks you out

New protection rules carry a theoretical risk: what if one of them locks *you* out? This is exactly where HTProtect thought ahead. Every rule is **tested on the real server** after it's written (whether Apache, LiteSpeed or nginx, it detects itself). If it would lock you out, HTProtect takes it back automatically. The shield only goes live once it's proven to work.

> **Your own downloads stay intact**
> After securing, HTProtect visits your site itself and **automatically** re-allows legitimate, linked downloads and forms. So securing never breaks your own downloads. Only genuinely risky things – such as a PHP program file in the image folder – are reported to you by name, so you can decide on purpose.

After a server move or domain change? If something then acts up, delete the main `.htaccess` in the Joomla root via FTP and let **"Secure now"** write a fresh one – this removes old rules that no longer fit.

Common problem: your own file gets blocked (403)

The shield only lets known things through and rejects the rest with **403 (forbidden)** – and that is exactly what protects you. But if you add something yourself (your own script, a forum, a shop), the shield doesn't

know it yet → 403. Not a fault: a 403 on a file that **you** added on purpose simply means "please allow me once".

How to find the blocked file – right in the browser, no server access needed (30 seconds, you can't break anything):

1. **Open the page or feature that isn't working.**
2. **Press the `F12` key**
   This opens the developer tools built into every browser. Click the **Network** tab at the top.
3. **Trigger the action again**
   Reload the page or submit the form, then click the **red "403" entry** – it shows the path of the blocked file (e.g. `custom-form.php`). Remember that path.

Name	Status
index.php	200
custom-form.php	403

The "Network" tab: the red **403** is the blocked file.

How to allow it – under **HTProtect › Protection shield › Advanced settings**, then always click `Save + write .htaccess` (only then does it take effect):

- **A single file:** field "Allow individual files directly" – one per line, e.g. `custom-form.php` (in a subfolder: `tools/specialtool.php`).
- **A folder with its own software** (forum, shop …, runs PHP): field "Allow folders completely, including PHP execution" – e.g. `forum`.
- **A folder with download files only** (PDFs, images – no PHP): field "Allow all file types in a folder, without PHP" – e.g. `downloads`. The safer choice when no PHP is needed.
- **A whole, exotic file type:** field "Allowed file extensions (comma-separated)" – for unusual extensions that aren't allowed yet, e.g. 3D/CAD files (`stl, dwg, step`).
- **Last resort, if none of the above is enough:** field "Trusted paths (allow everywhere)" – for these paths it also lifts directory locks and exploit signatures. **Only for paths you have checked yourself and know are harmless**, never broadly.

Rule of thumb: allow as narrowly as possible – the one file rather than the whole folder, "without PHP" rather than with. Once the 403 is gone in the Network tab, it's solved.

A page won't embed as an iframe

Problem: A page can no longer be embedded via `<iframe>` on another domain (e.g. a contact form hosted on site B, embedded on site A). The browser console reports: `Refused to display … X-Frame-Options: SAMEORIGIN`.

Cause: The clickjacking protection "Forbid embedding on other sites (X-Frame-Options)" on the **embedded** site B forbids third-party embedding.

Solution (on site B, not on A!): under `HTProtect › Protection shield › Advanced settings`, turn off the switch "Forbid embedding on other sites" → `Save + write .htaccess`. Harmless for public forms.

Site scan

Should something slip through after all, the site scan tracks it down. It searches your entire website for malicious code, planted files, and hidden back doors (so-called web shells) – and can remove anything it finds right away. It is started **only by you**, never on its own, and puts no lasting load on your server.

Very large sites are scanned in small chunks so nothing is cut off by a time limit; a repeat scan then only checks what has changed. It can also test whether your linked files and downloads are reachable.

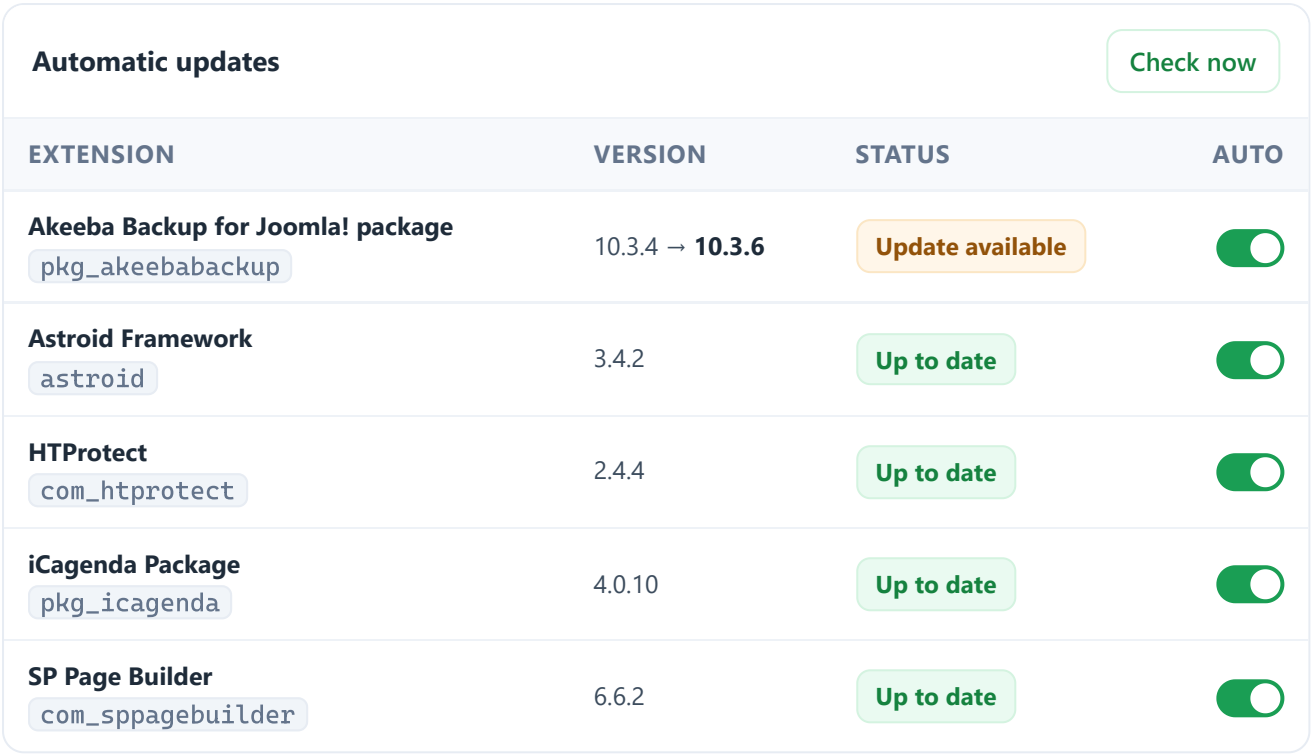
It watches on the small scale too: **newly installed or updated files** are checked for malicious code – web shells or injected JavaScript, for example. If it finds something, it can isolate or remove it, with strict safeguards against accidental wrong deletions. There's special handling for one common pattern: JavaScript injected into **Helix templates** is detected and removed on purpose – reversible, with a backup.

Backups & updates

Before **every** change to the `.htaccess`, HTProtect automatically makes a backup – a single click brings you back to the previous state any time. The same principle applies to updates: never without a net.

Your site maintains itself
Automatic extension updates – on your own schedule.

If you like, HTProtect keeps your Joomla extensions up to date automatically. **Before** each update it backs up files and database, then checks with a health check that the site still runs cleanly – and, if there's a problem, falls back automatically to the previous state. By default, security updates are preferred, daily at the time you set.



Auto-update overview in HTProtect

And HTProtect knows **what** should be updated: it compares your installed extensions against a list of known security flaws and points you to the available updates.

Recommended: run non-security updates once a week, with a 3-day grace period – a good middle ground.

The safety net behind it:

- **Interval & time freely selectable:** weekly, daily or "instant" (every 15 minutes).
- **Security updates run immediately** – with no waiting time.
- **Grace period selectable:** none, 1, 3, 7 or 14 days.
- **Malware scan during the update:** if something is found, it is rolled back at once (usually a false positive – the signatures are maintained centrally, without any site- or person-related data; the update then runs on the next pass).
- **Considerate:** update sources are never switched off; HTProtect queries external servers gently (throttled) to spare them.
- **Emergency brake:** if an update turns out to be highly problematic, it can be blocked centrally for everyone right away.

Help & support

Here you can reach **support** (optionally with helpful diagnostic data), the **live chat**, this documentation, and the tip jar.

HTProtect is built to give way *gently* rather than fail hard. If an over-eager server virus scanner damages an HTProtect file, for example, your site stays reachable: the affected part quietly disables itself, HTProtect

restores itself via its self-update, and a clear notice page explains what's going on. It gets along with existing security tools (hands-off mode) and keeps server load minimal.

And if you want to be rid of HTProtect? During uninstall an assistant offers to cleanly remove the protection files and restore your original `.htaccess` – without a trace. Honest and reversible, like everything here.

Securing the Joomla .htaccess with HTProtect
Background article