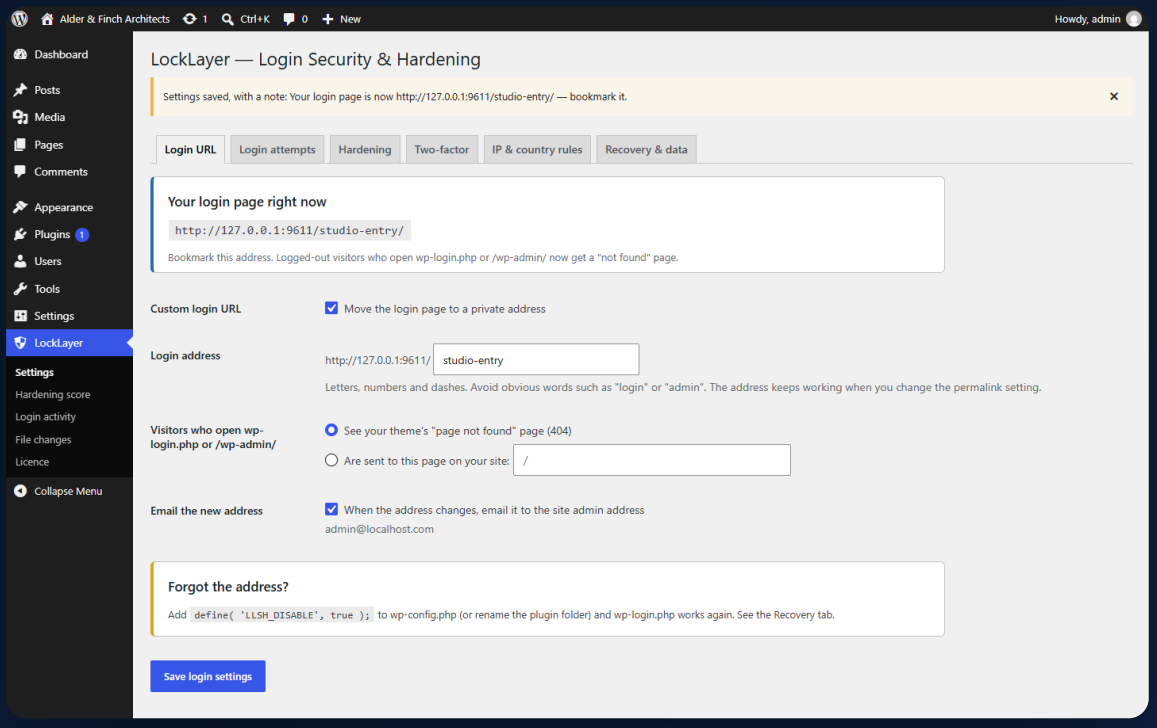
CODE CRAFT
Build. Launch. Grow.

WORDPRESS PLUGIN · USER GUIDE

LockLayer — WordPress Security Plugin for Login Hardening

Version 1.0.0 · Installation, licence activation, every setting explained, FAQ and troubleshooting.



coodecraft.com/market/product/wp-security-hardening · support: coodecraft.com/contact

LockLayer — Login Security & Hardening: user guide

LockLayer is a WordPress security plugin for the login page and the most common weak spots. It runs on your own server: no cloud service, no account, nothing is sent anywhere (the only outside call is the licence check in Pro).

What it is not: it does not make a site impossible to break into, it is not a web application firewall and it is not a malware scanner. Keep WordPress, plugins and themes updated, use strong passwords and keep backups.

---

1. Installation

1. Go to **Plugins** → **Add New** → **Upload Plugin**, choose the zip and click **Install Now**, then **Activate**. (The free version can also be installed from WordPress.org.)
2. A new **LockLayer** menu appears in wp-admin.
3. Right after activation, login attempt limits (5 failures in 15 minutes → 20-minute lockout) and the security headers are on. Nothing else changes until you switch it on.

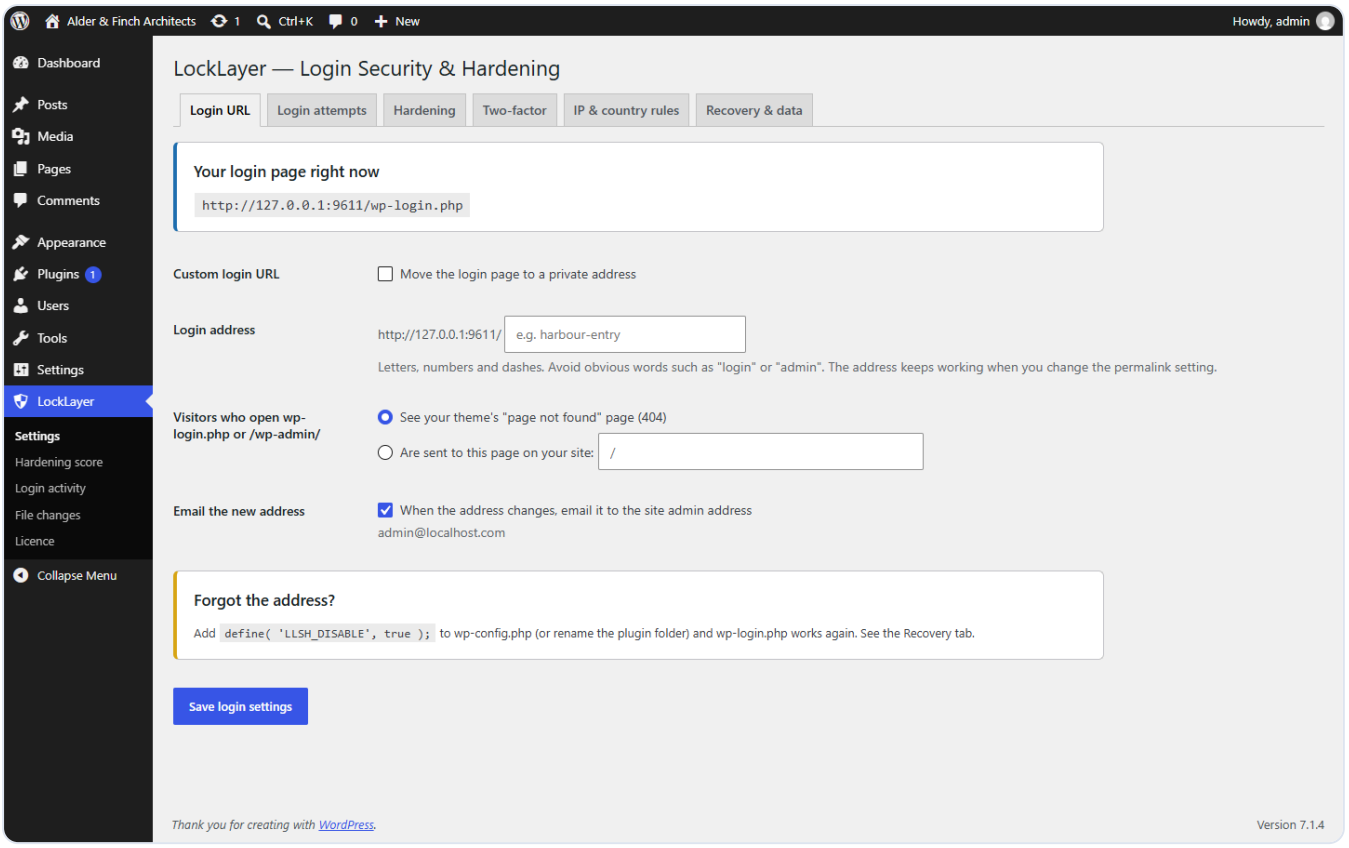
Activating Pro

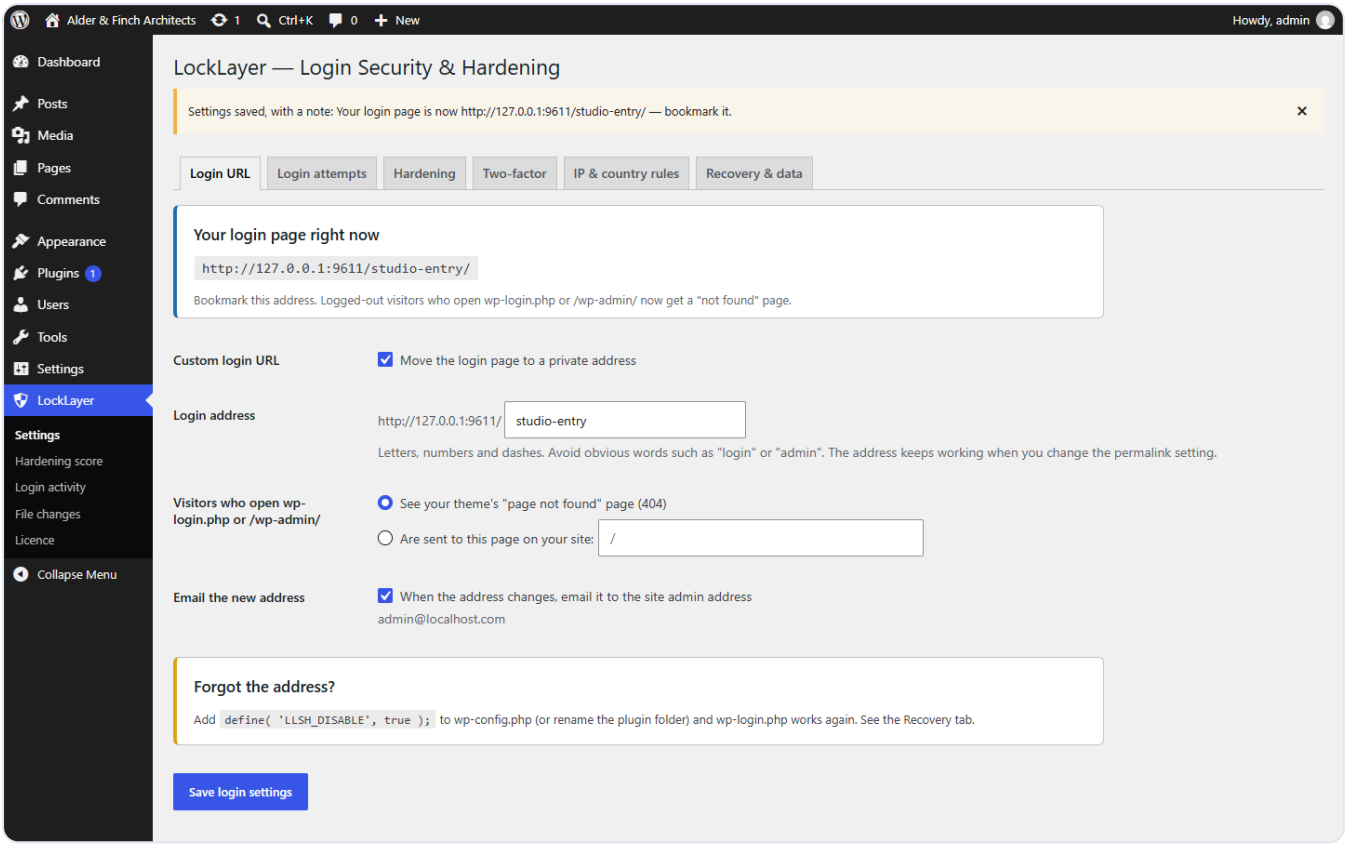
1. Install the Pro zip from your Code Craft account. It replaces the free copy in place; your settings are kept.
2. Go to **LockLayer** → **Licence**, paste your licence key and click **Activate**.
3. Monthly and yearly keys switch Pro off when they end and back on when you renew (the Licence screen has an "I have paid — check again" button). Your settings, logs and two-factor secrets are kept while Pro is off, and the free protections keep working.

---

2. Login URL tab (free)

Screenshot: ,



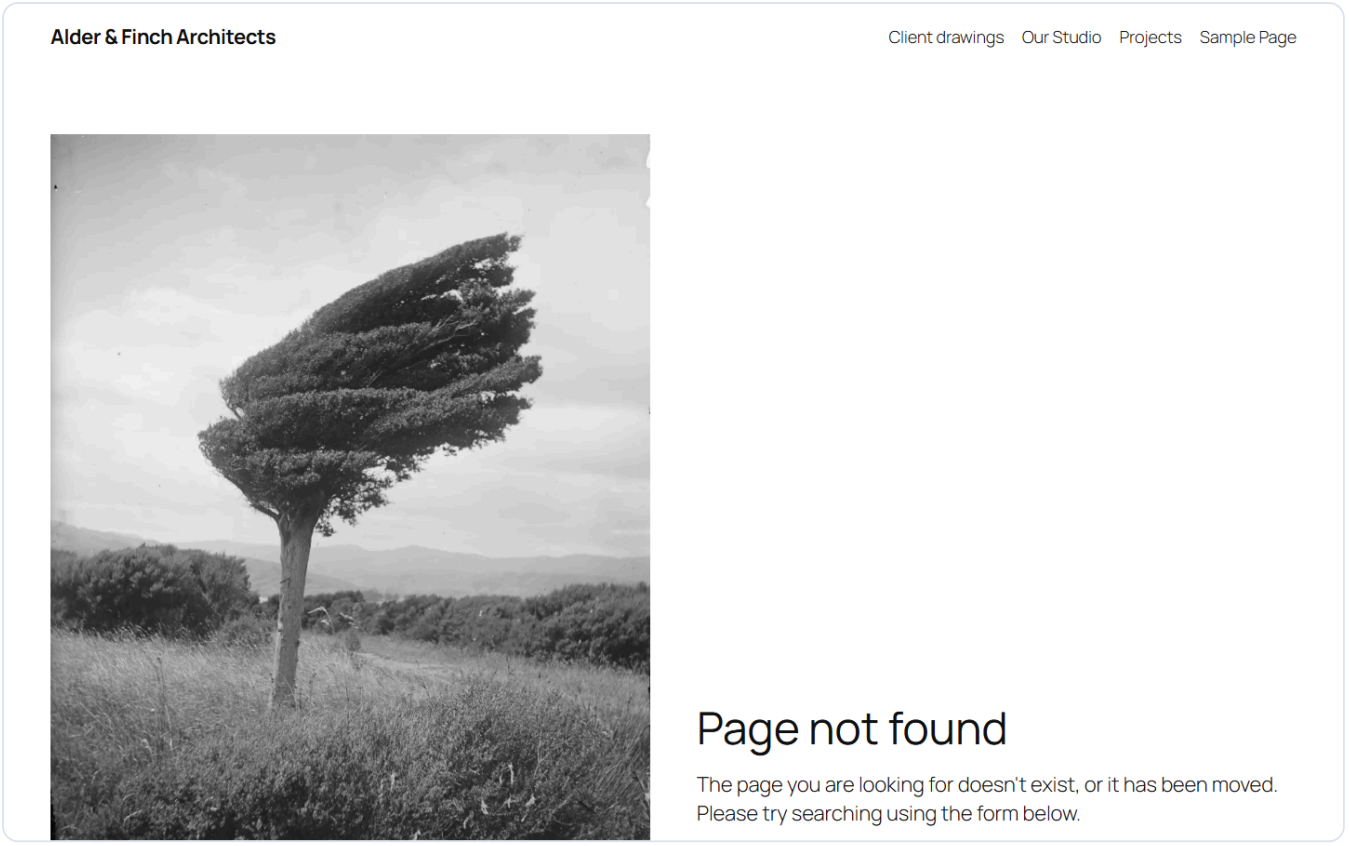


1. Tick **Move the login page to a private address**.
2. Type an address, for example `studio-entry`. Letters, numbers and dashes, 4–60 characters. Obvious words (`login` , `admin` , `dashboard` …) and addresses already used by a post or page are refused.

3. Choose what logged-out visitors see at `wp-login.php` and `/wp-admin/`: your theme's **page not found** page (default) or a redirect to a page you choose.
4. Leave **Email the new address** ticked to get the address in your admin mailbox.
5. Click **Save login settings**. The box at the top shows the new login address — bookmark it.

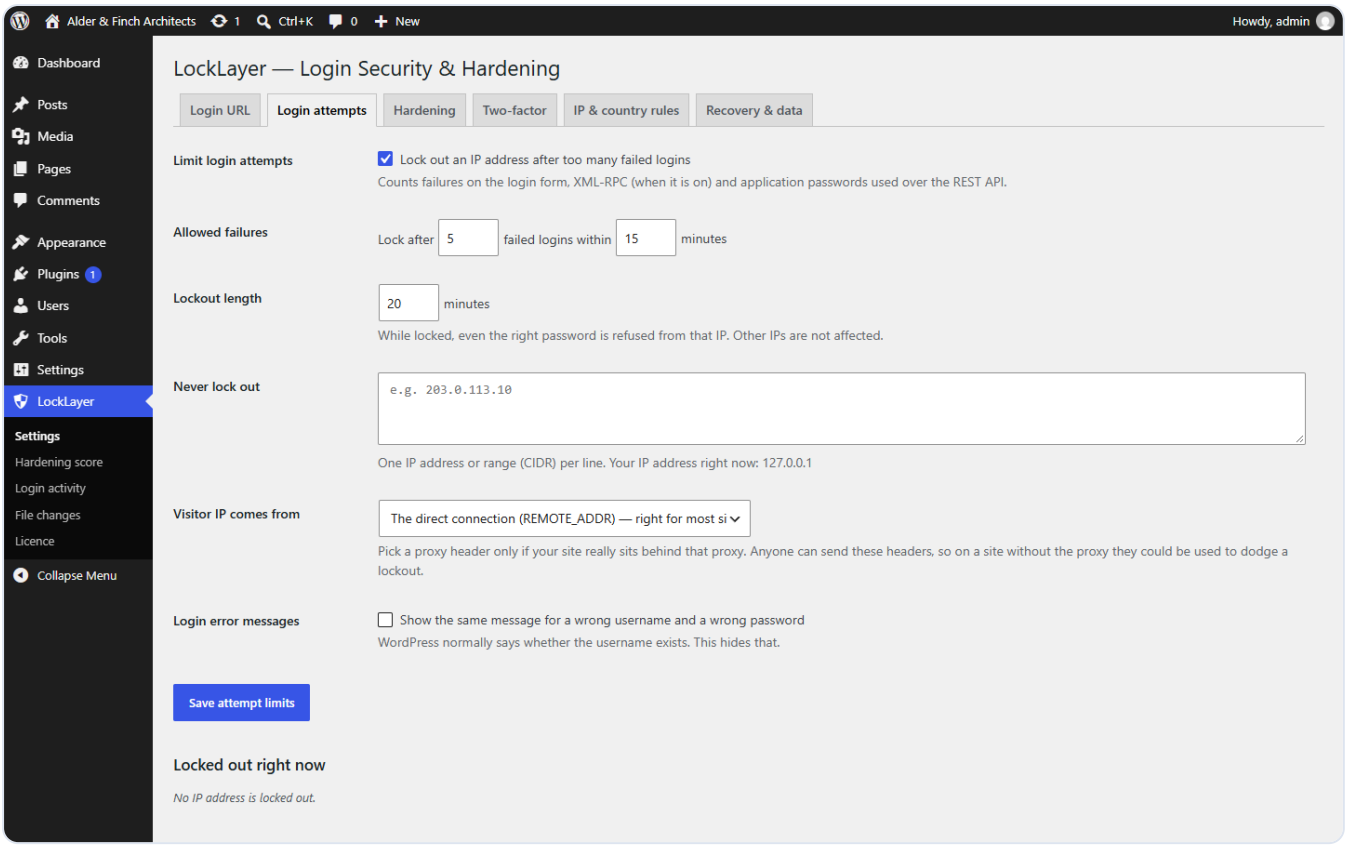
What keeps working: logging in and out, lost password and the reset link in the email, registration (if enabled), the password form on password-protected posts, and every link made with `wp_login_url()`. Logged-in users reach wp-admin as usual. The address does not use rewrite rules, so it keeps working when you change **Settings** → **Permalinks**; with "Plain" permalinks it becomes `yoursite.com/?studio-entry`.

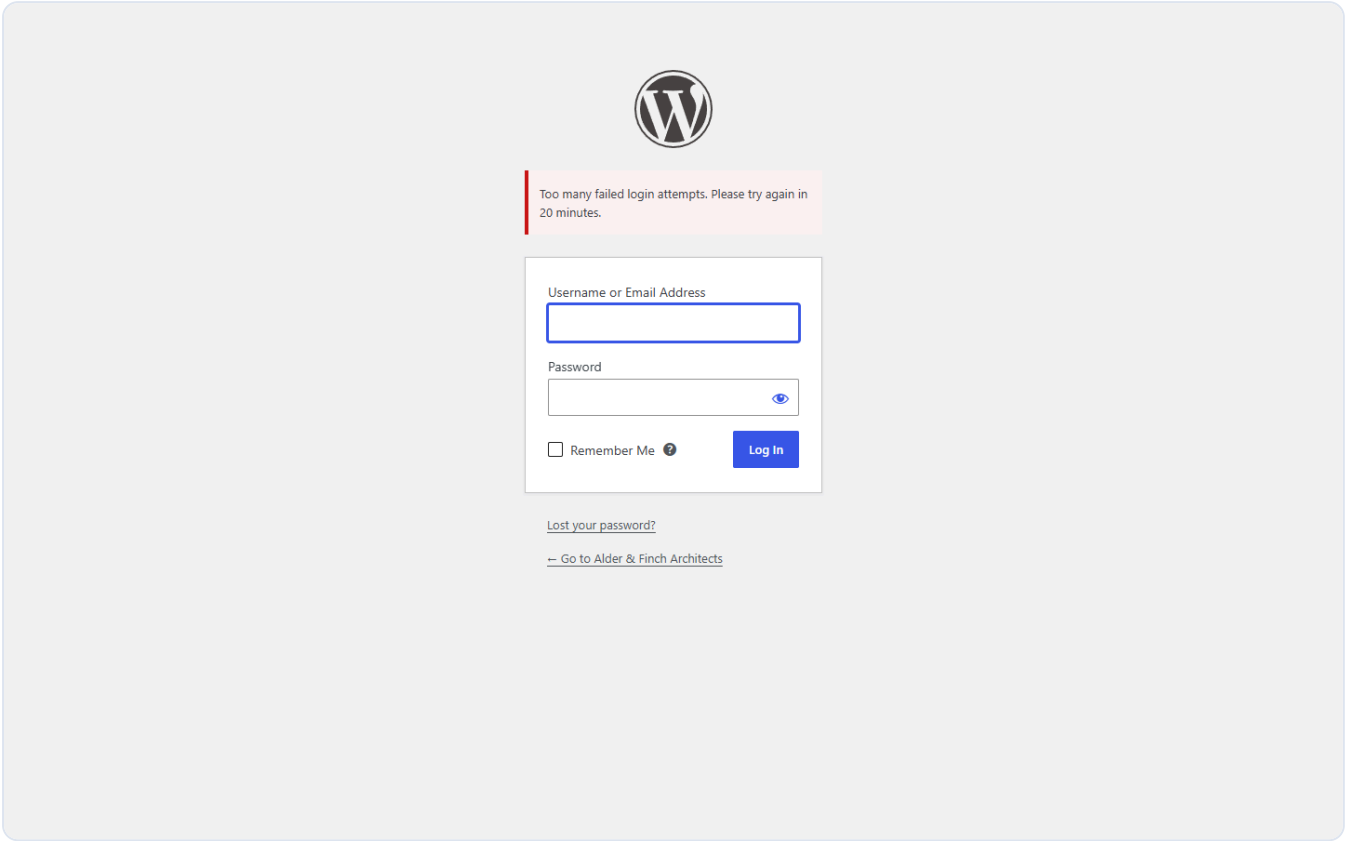
Screenshot of what a visitor sees at wp-login.php: .

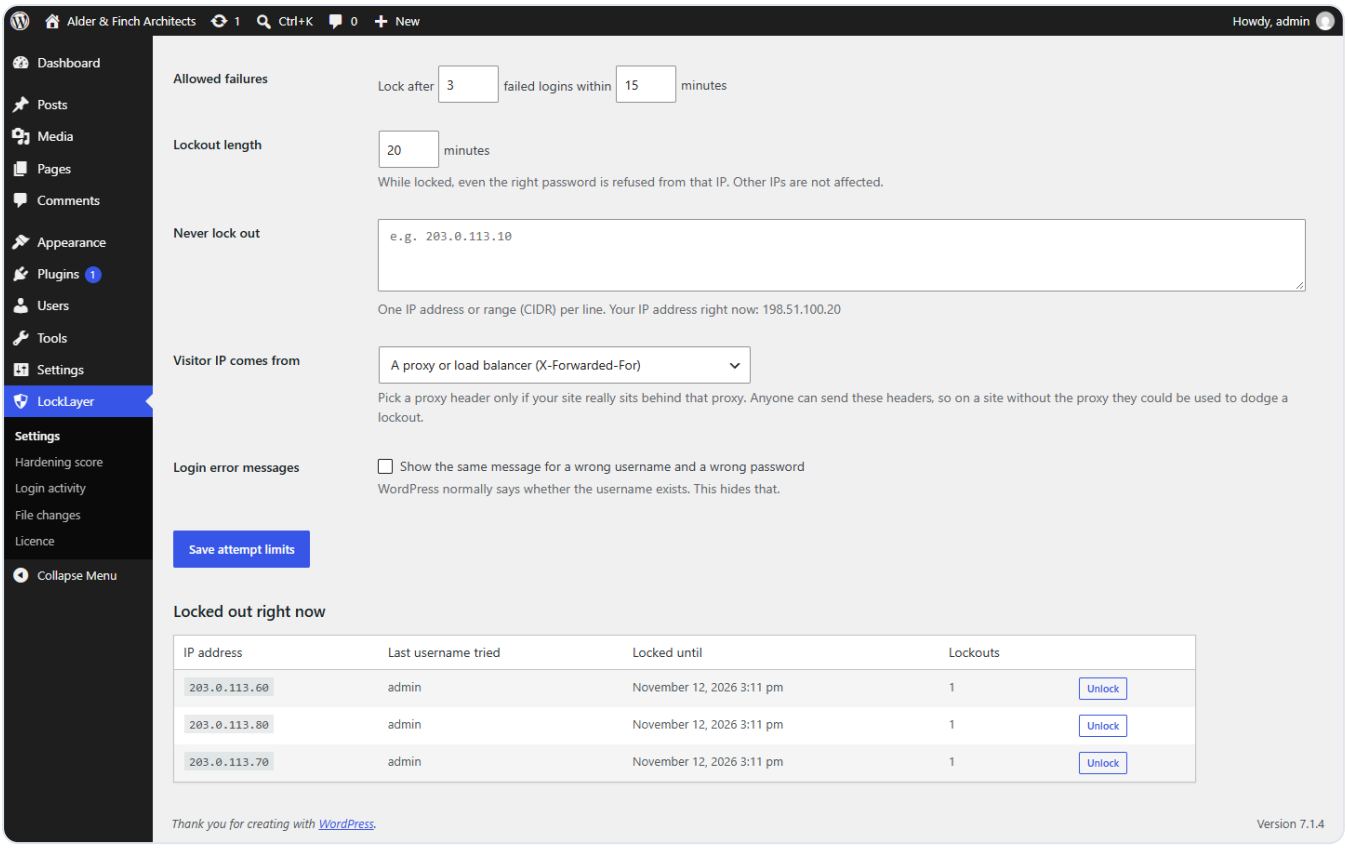


3. Login attempts tab (free)

Screenshots: , ,


Alder & Finch Architects
1
Ctrl+K
0
New
Howdy, admin
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
Users
Tools
Settings
LockLayer
Settings
Hardening score
Login activity
File changes
Licence
Collapse Menu
LockLayer — Login Security & Hardening
Login URL
Login attempts
Hardening
Two-factor
IP & country rules
Recovery & data
Limit login attempts
Lock out an IP address after too many failed logins
Counts failures on the login form, XML-RPC (when it is on) and application passwords used over the REST API.
Allowed failures
Lock after 5 failed logins within 15 minutes
Lockout length
20 minutes
While locked, even the right password is refused from that IP. Other IPs are not affected.
Never lock out
e.g. 203.0.113.10
One IP address or range (CIDR) per line. Your IP address right now: 127.0.0.1
Visitor IP comes from
The direct connection (REMOTE_ADDR) — right for most si
Pick a proxy header only if your site really sits behind that proxy. Anyone can send these headers, so on a site without the proxy they could be used to dodge a lockout.
Login error messages
Show the same message for a wrong username and a wrong password
WordPress normally says whether the username exists. This hides that.
Save attempt limits
Locked out right now
No IP address is locked out.


Too many failed login attempts. Please try again in 20 minutes.
Username or Email Address
Password
Remember Me
Log In
Lost your password?
← Go to Alder & Finch Architects

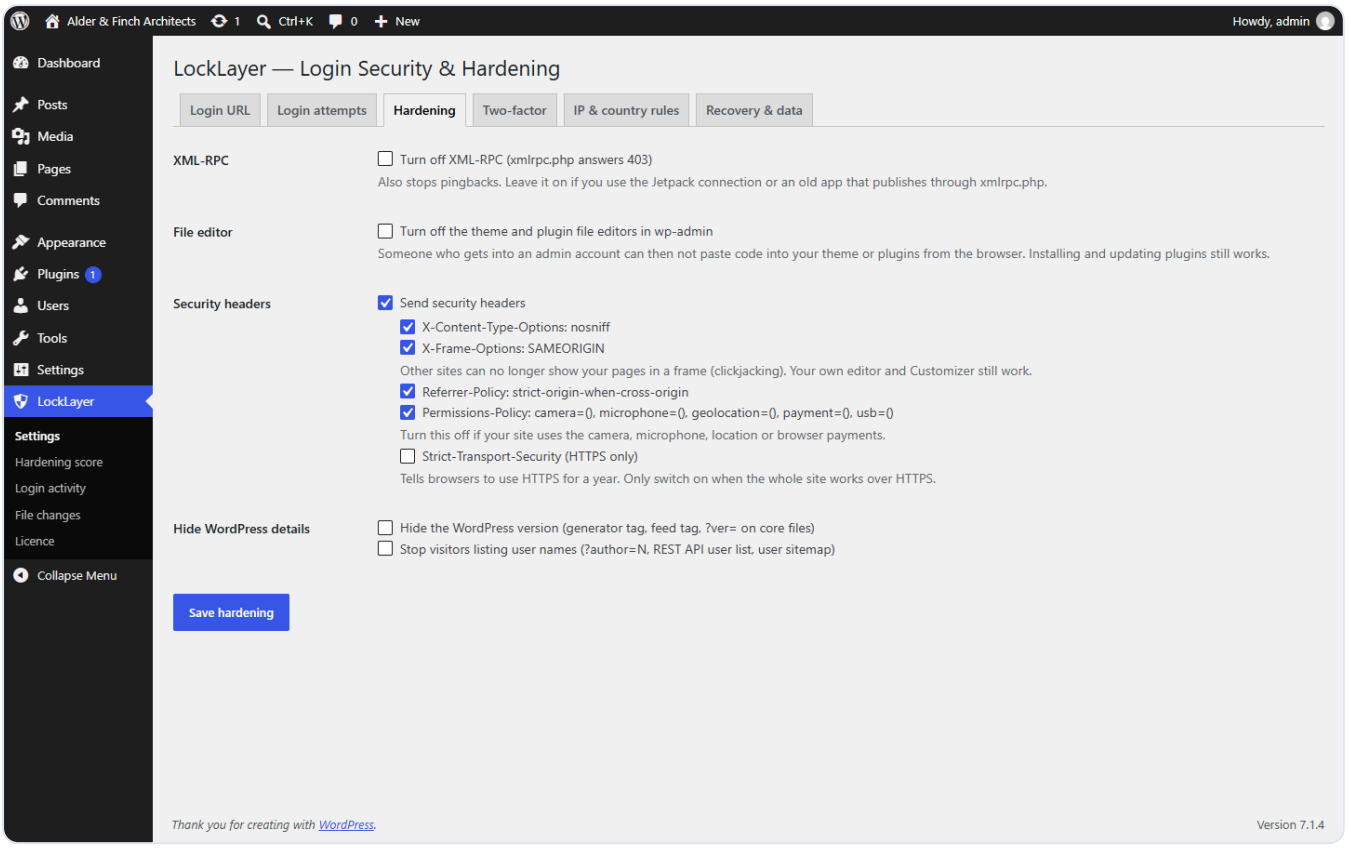


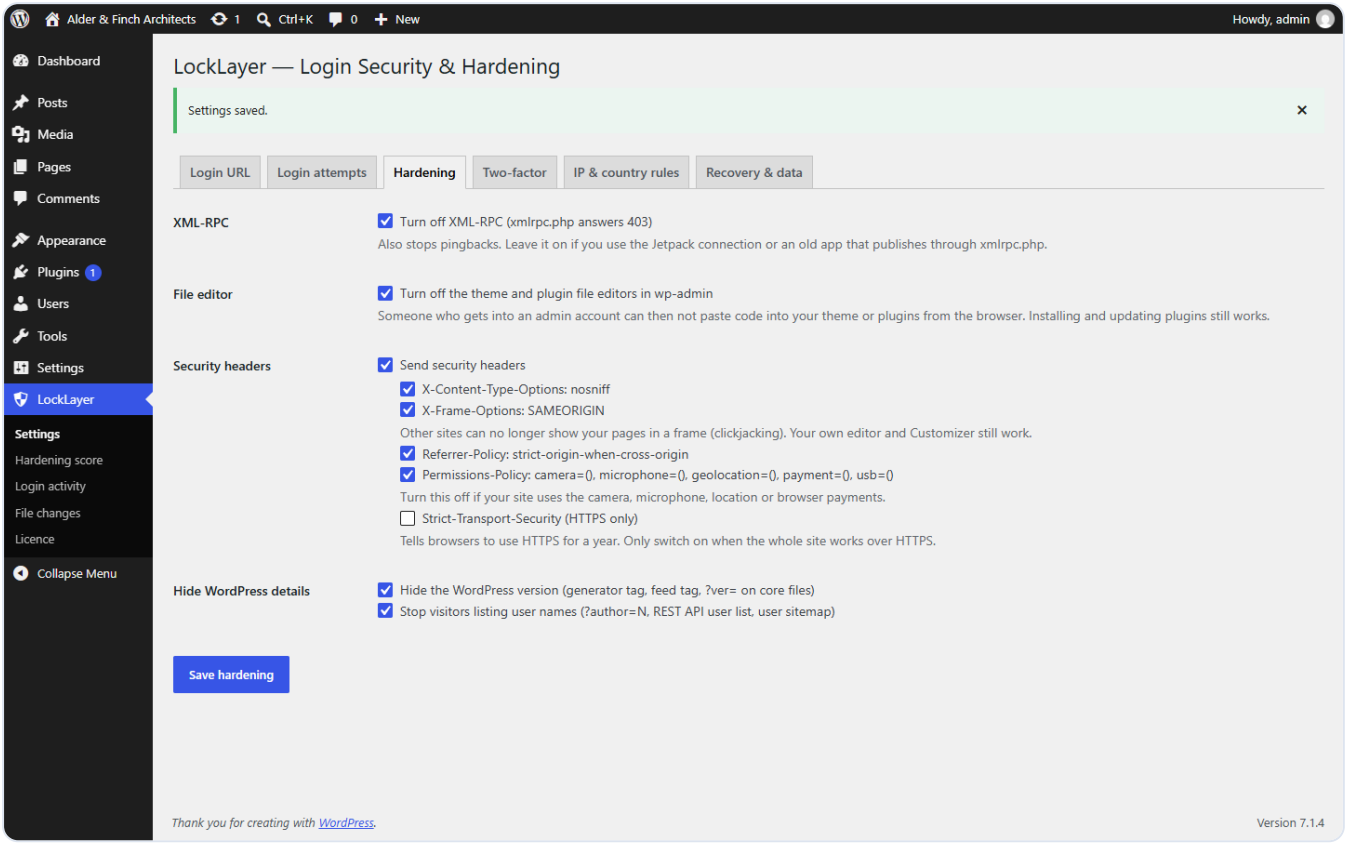
- **Limit login attempts** — on by default.
- **Lock after N failed logins within M minutes** and **Lockout length** — while an IP is locked, even the right password is refused from it; other IPs are not affected. Failures are counted on the login form, on XML-RPC (when it is on) and for application passwords used over the REST API. A wrong two-factor code counts as a failure too.
- **Never lock out** — your office IP or a range such as `198.51.100.0/24`, one per line.
- **Visitor IP comes from** — keep "The direct connection" unless the site sits behind Cloudflare or a proxy. Pick a proxy header only when that proxy really exists, because anyone can send these headers.
- **Login error messages** — show the same message for a wrong user name and a wrong password.
- **Locked out right now** — the list under the form; click **Unlock** to release an IP.

---

4. Hardening tab (free + Pro)

Screenshots: ,





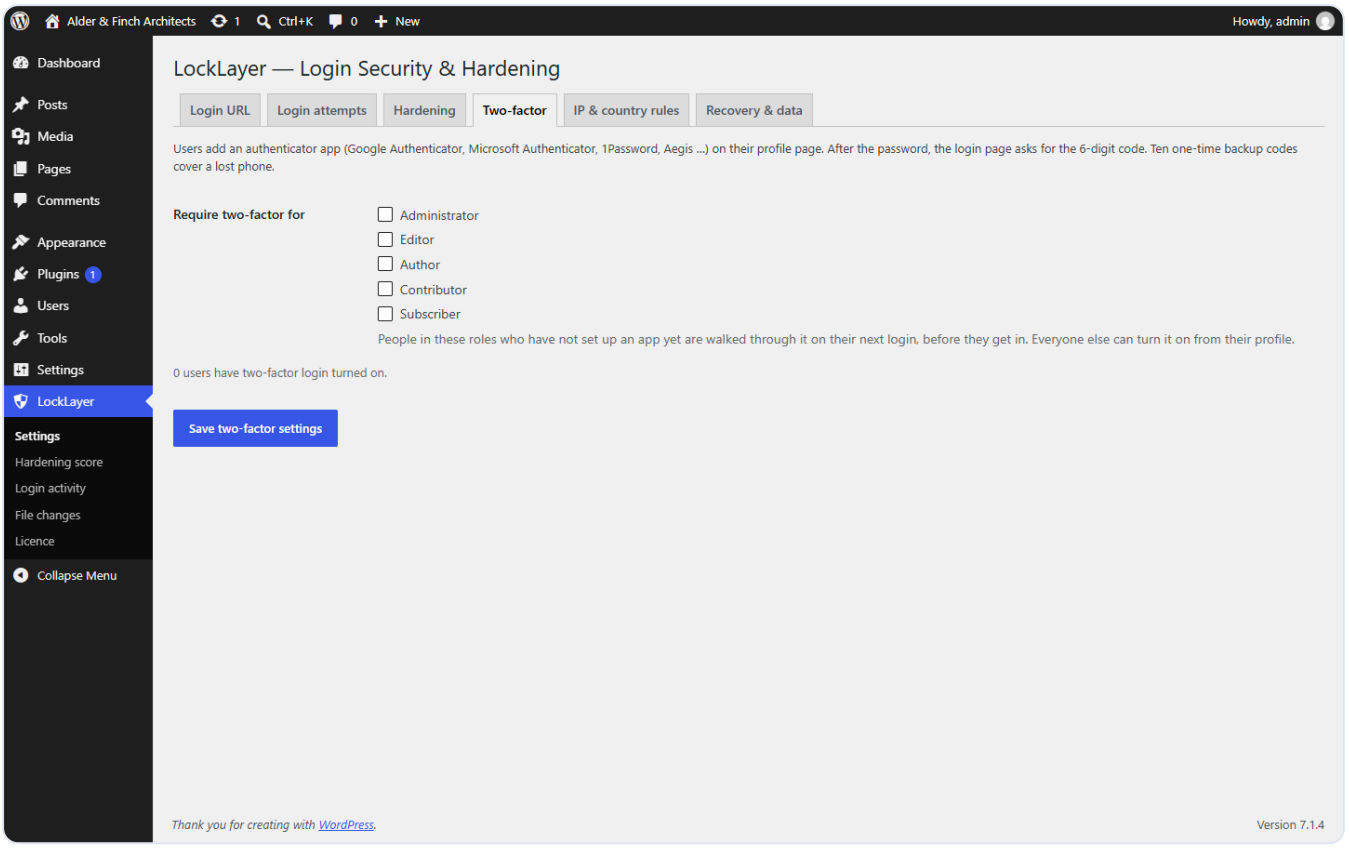
- **Turn off XML-RPC** — `xmlrpc.php` answers 403 before any method runs; pingbacks stop. Keep XML-RPC if you use the Jetpack connection or an old publishing app.
- **Turn off the theme and plugin file editors** — nobody can edit theme or plugin code from wp-admin. Installing and updating plugins still works.

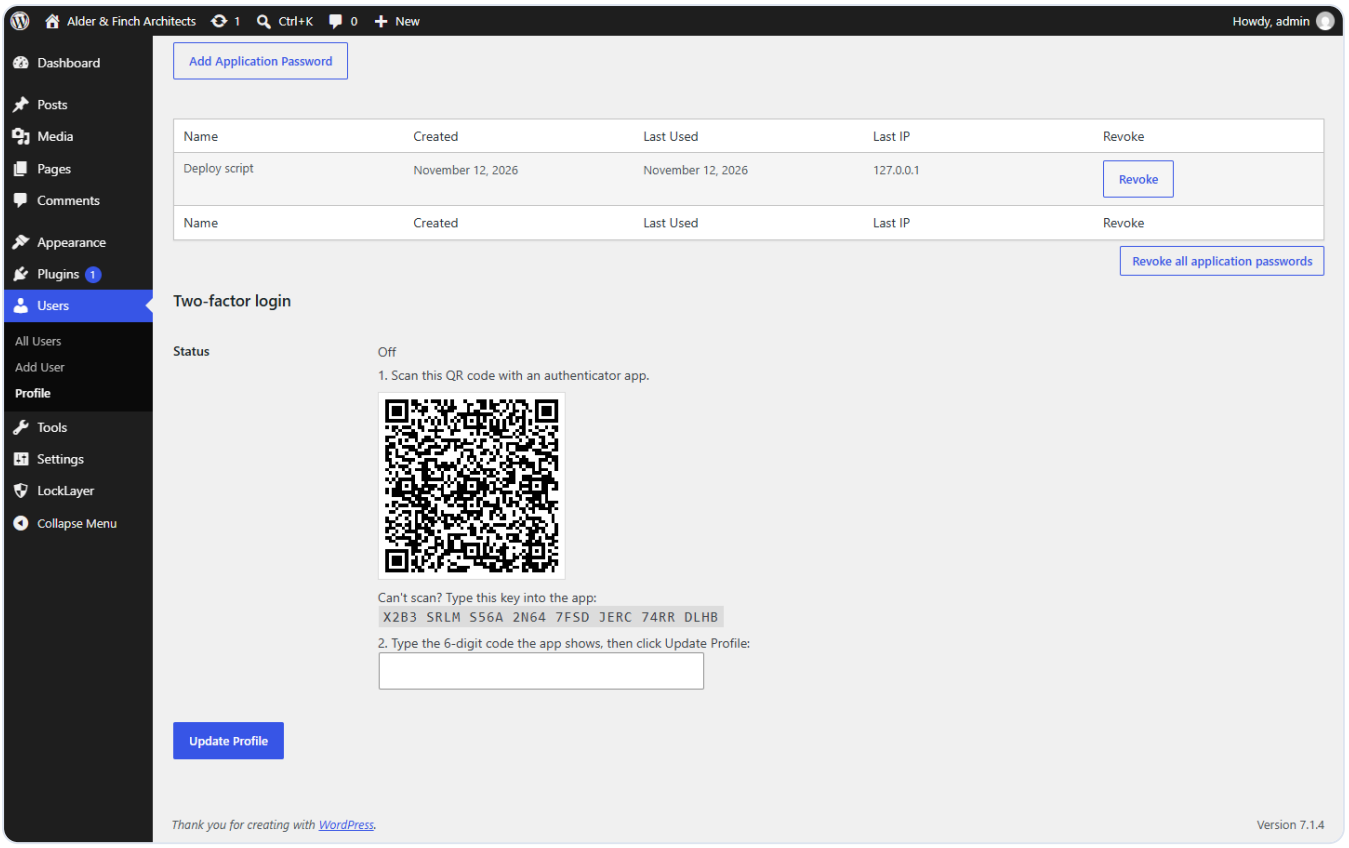
- **Security headers** — X-Content-Type-Options, X-Frame-Options: SAMEORIGIN, Referrer-Policy, Permissions-Policy, and optional Strict-Transport-Security (HTTPS sites only). Untick a header if it gets in the way (for example Permissions-Policy if your site uses the camera or location). The block editor and the Customizer keep working.
- **Pro: Hide the WordPress version** — removes the generator tag (page and feeds) and replaces `?ver=<version>` on core files with a site-specific code.
- **Pro: Stop visitors listing user names** — `?author=1` answers "not found", the REST API user list and the user sitemap are hidden from logged-out visitors. (Author archive pages themselves stay, because many sites use them.)

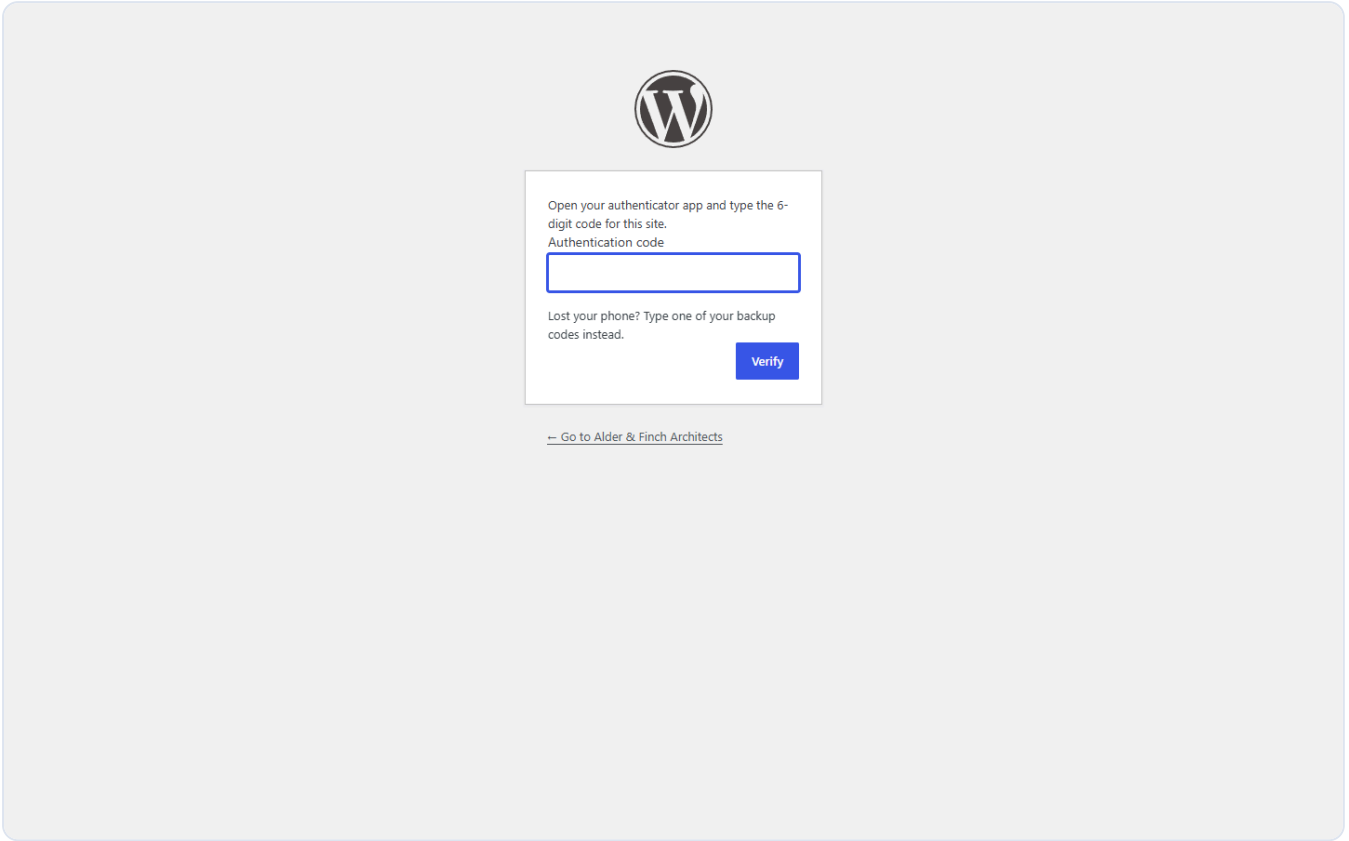
---

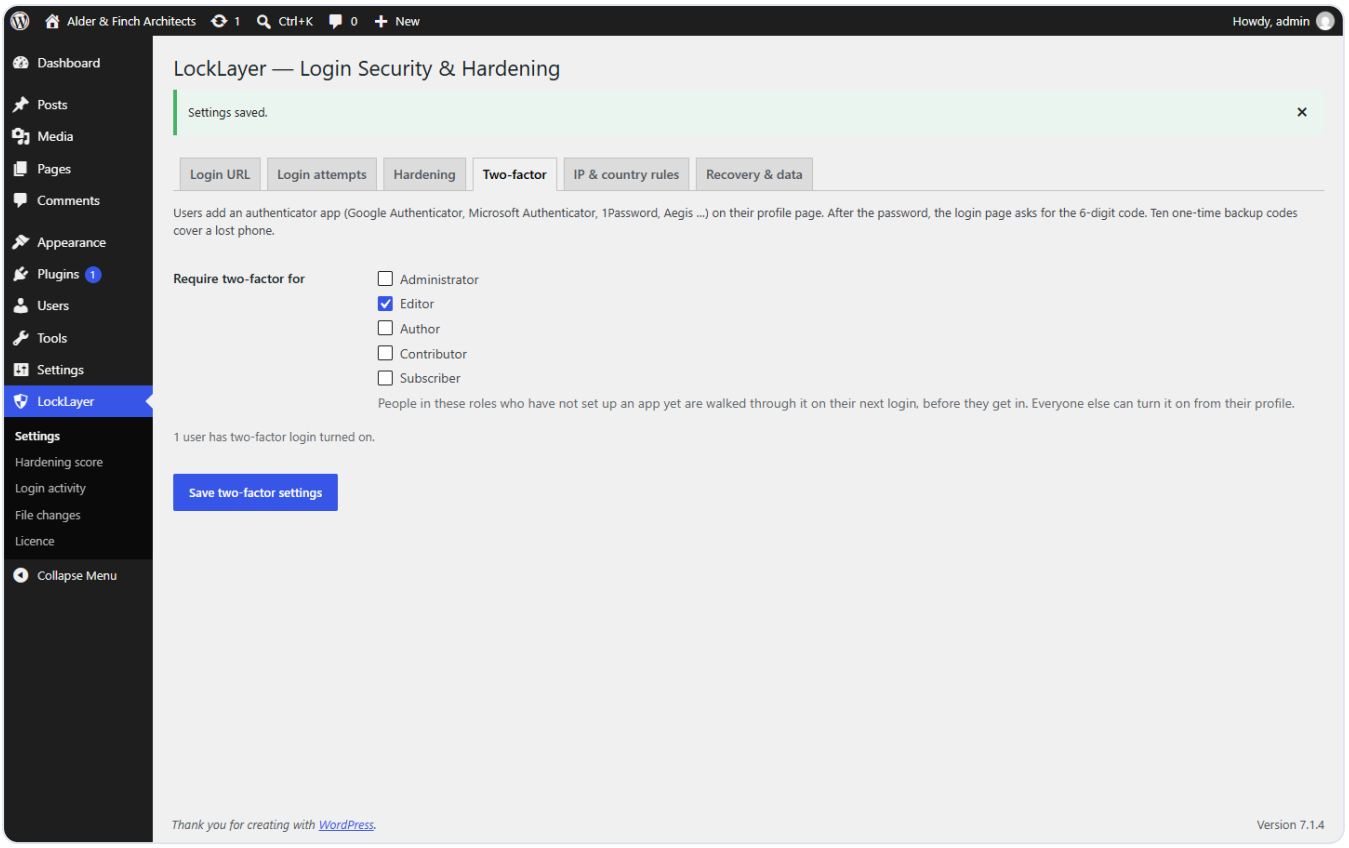
5. Two-factor tab and your profile (Pro)

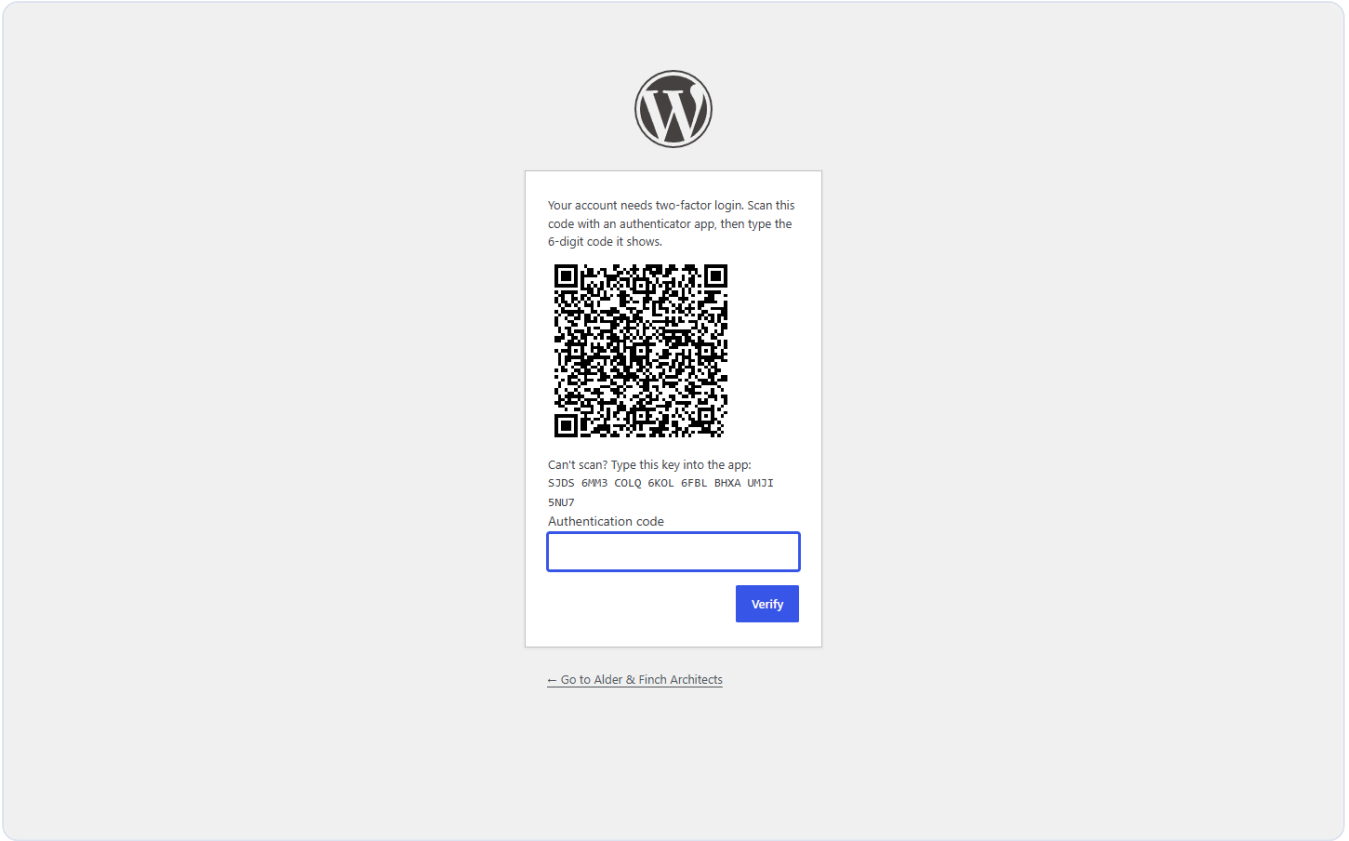
Screenshots: , , , ,




Alder & Finch Architects
1
Ctrl+K
0
New
Howdy, admin
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins 1
Users
All Users
Add User
Profile
Tools
Settings
LockLayer
Collapse Menu
Add Application Password
Name
Created
Last Used
Last IP
Revoke
Deploy script
November 12, 2026
November 12, 2026
127.0.0.1
Revoke
Name
Created
Last Used
Last IP
Revoke
Revoke all application passwords
Two-factor login
Status
Off
1. Scan this QR code with an authenticator app.
Can't scan? Type this key into the app:
X2B3 SRLM S56A 2N64 7FSD JERC 74RR DLHB
2. Type the 6-digit code the app shows, then click Update Profile:
Update Profile
Thank you for creating with WordPress.
Version 7.1.4


Open your authenticator app and type the 6-digit code for this site.
Authentication code
Lost your phone? Type one of your backup codes instead.
Verify
← Go to Alder & Finch Architects





Turning it on for yourself:

1. Go to **Users** → **Profile** and scroll to **Two-factor login**.
2. Scan the QR code with an authenticator app (Google Authenticator, Microsoft Authenticator, 1Password, Aegis ...) or type the key shown under it.

3. Type the 6-digit code from the app and click **Update Profile**.
4. Save the 10 backup codes shown. Each works once if you lose your phone. They are not shown again (you can make new ones from the profile).

Logging in: after the password, the login page asks for the code. A wrong code is refused; after 5 wrong codes the login has to start again, and wrong codes count towards the IP lockout. A code can not be used twice.

Requiring it per role: on **LockLayer → Settings → Two-factor**, tick the roles (for example Administrator, Editor). People in those roles who have no app yet are shown the QR code at their next login and must enter a code before they get in.

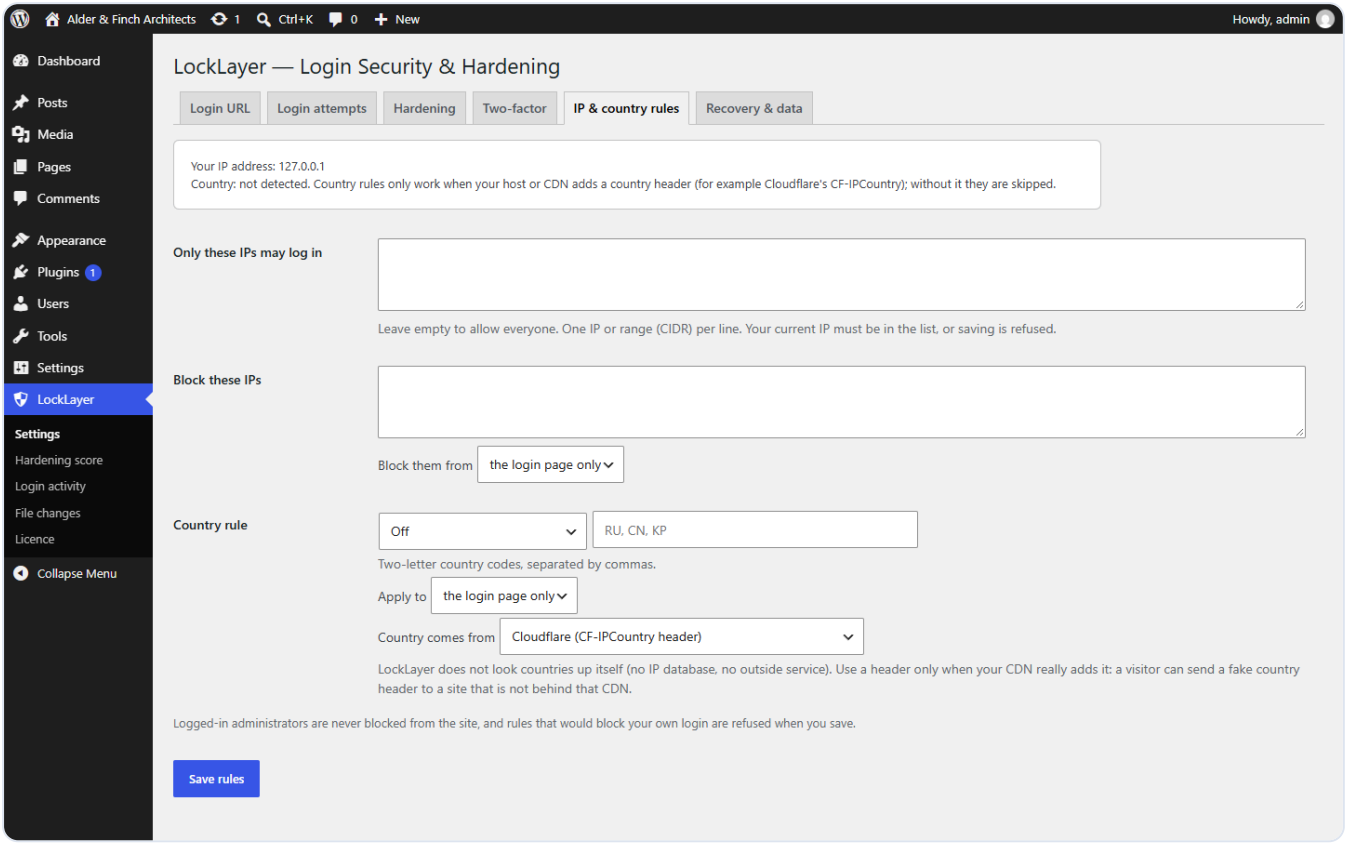
Lost phone: use a backup code, or ask an administrator to tick **Turn off two-factor login for this user** on your profile.

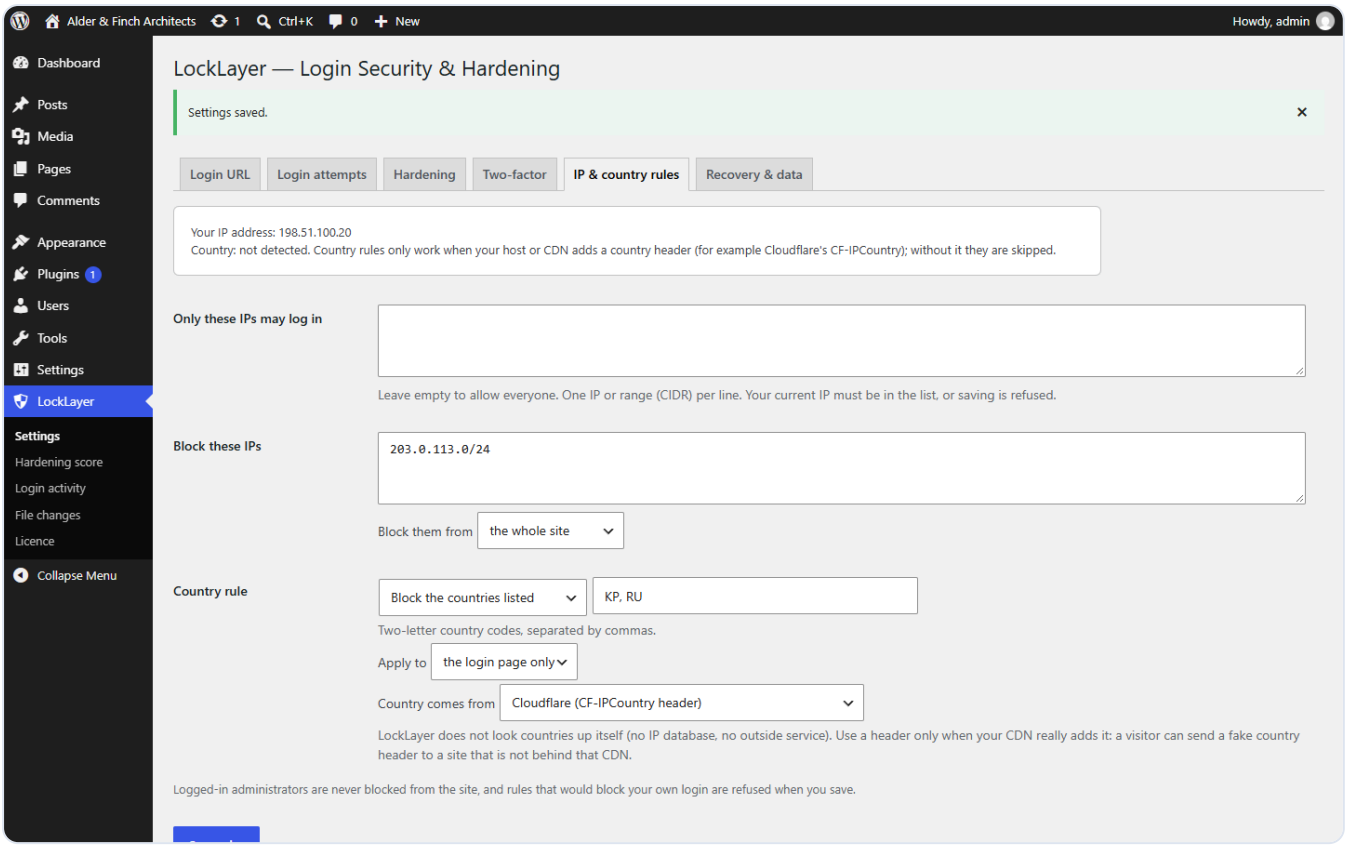
Limits: application passwords (REST API) are not asked for a code, by design. Password logins over XML-RPC are refused for two-factor accounts. The QR code is drawn in your browser by a bundled script; the secret is not sent anywhere.

---

6. IP & country rules tab (Pro)

Screenshots: ,



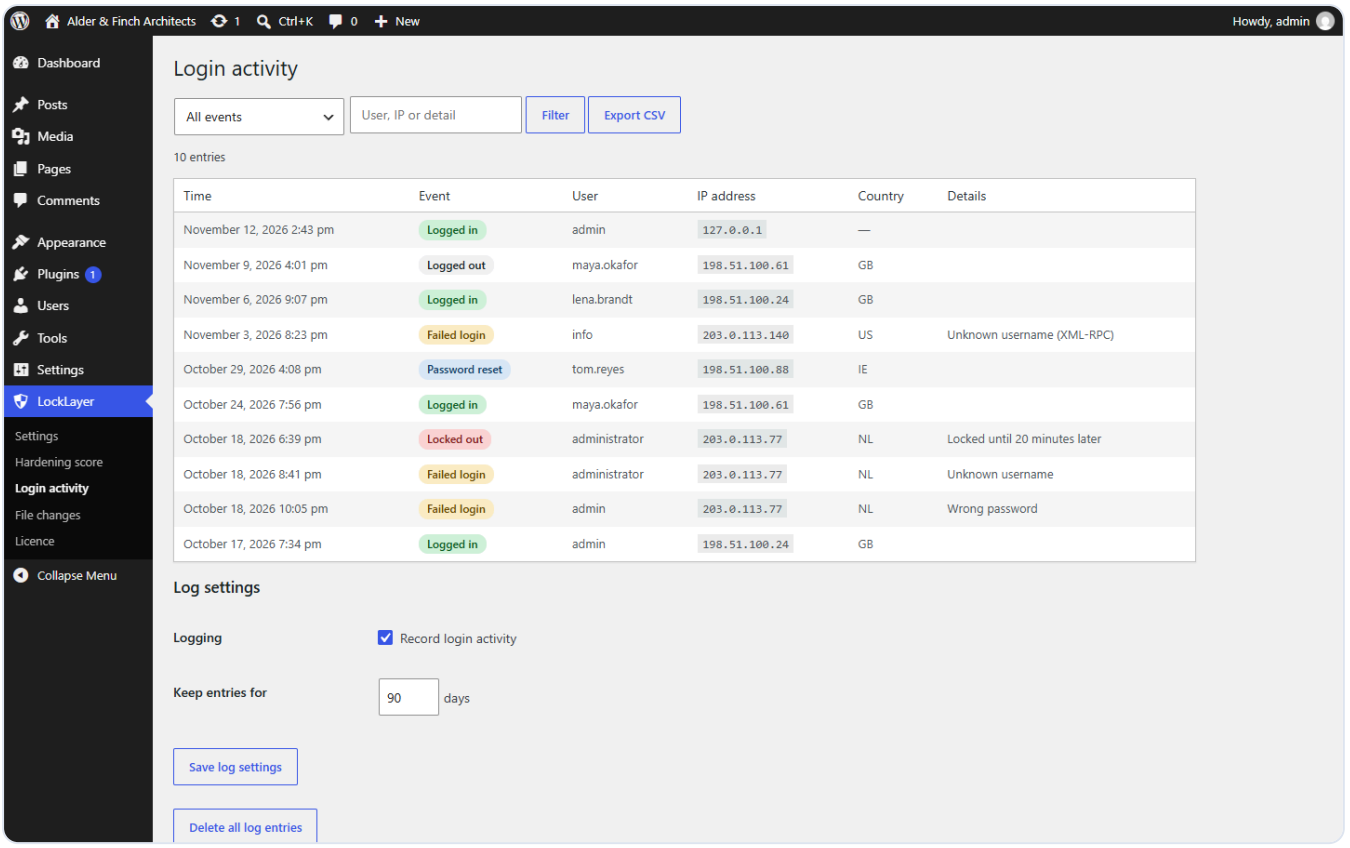


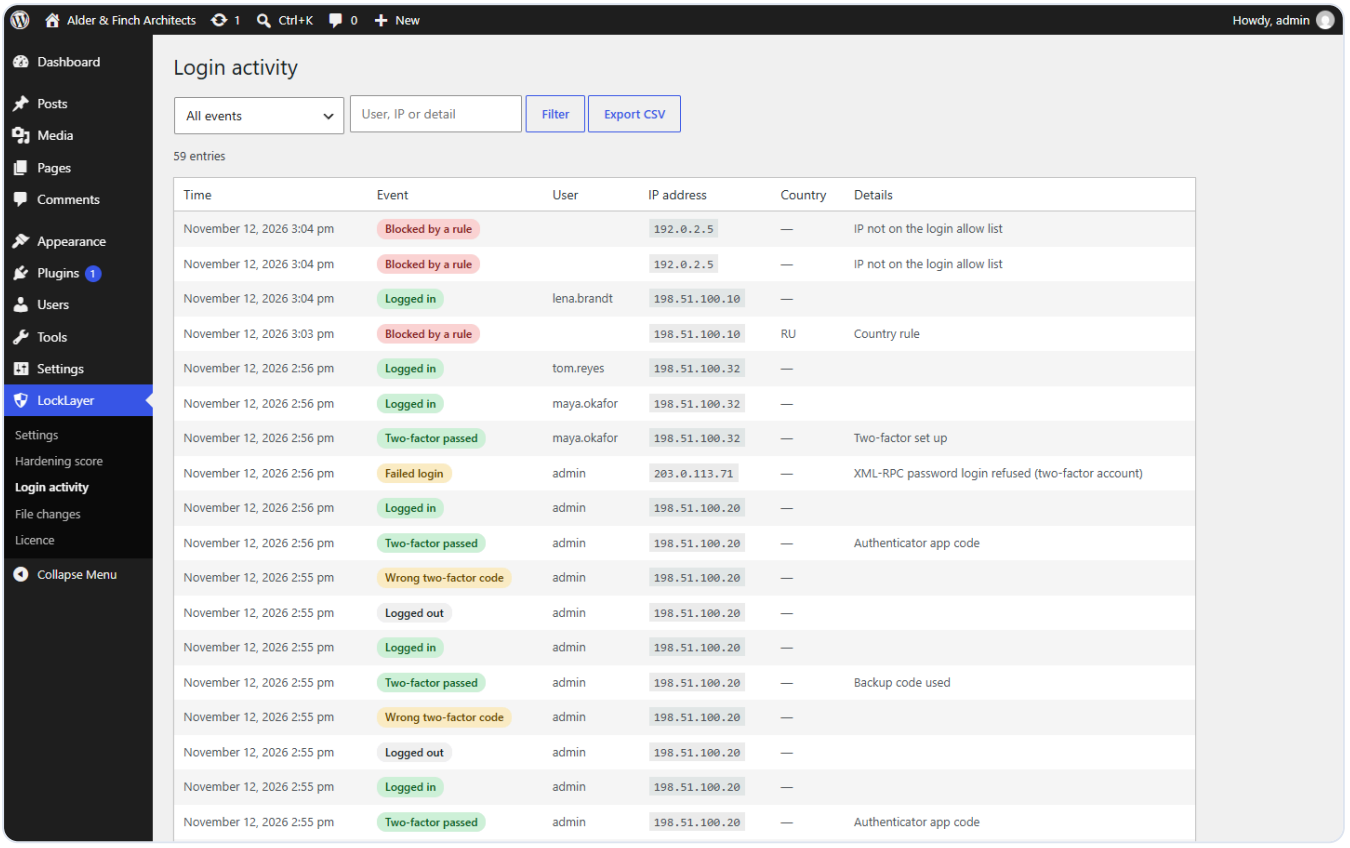
- **Only these IPs may log in** — leave empty for everyone. If you fill it in, your current IP must be in the list or saving is refused.
- **Block these IPs** — on the login page only, or the whole site.
- **Country rule** — block the listed countries, or allow only them, on the login page or the whole site.
- **Country comes from** — LockLayer never looks countries up itself. Choose the header your CDN adds (Cloudflare `CF-IPCountry`, CloudFront `CloudFront-Viewer-Country`), a web-server variable (`GEOIP_COUNTRY_CODE`), or your own code via the `llsh_visitor_country` filter. Without one, country rules are skipped. Only use a header your CDN really sets: a visitor can send a fake one to a site that is not behind it.
- Logged-in administrators are never blocked from the site, and rules that would block your own login are refused when you save.

---

7. Login activity (Pro)

Screenshots: ,

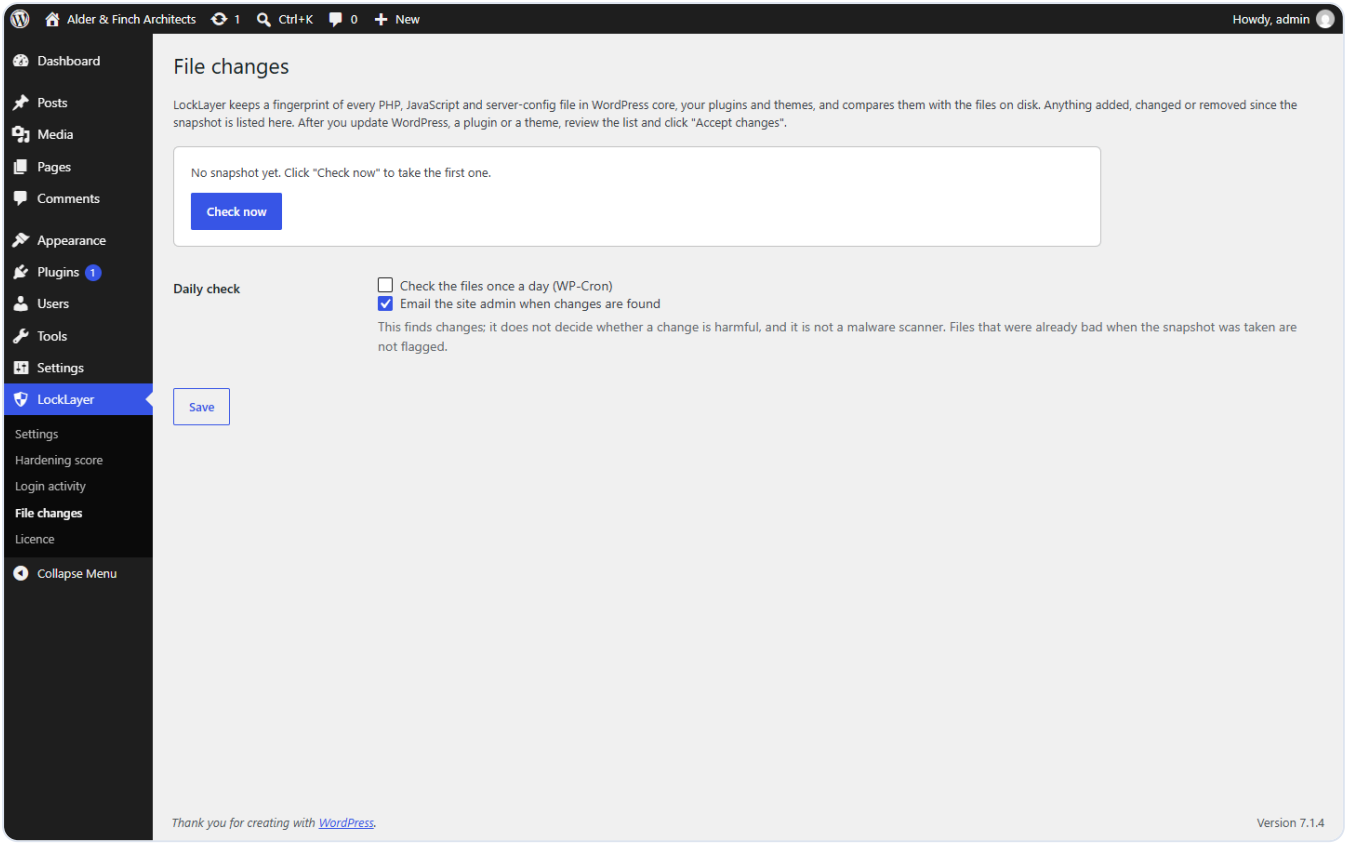


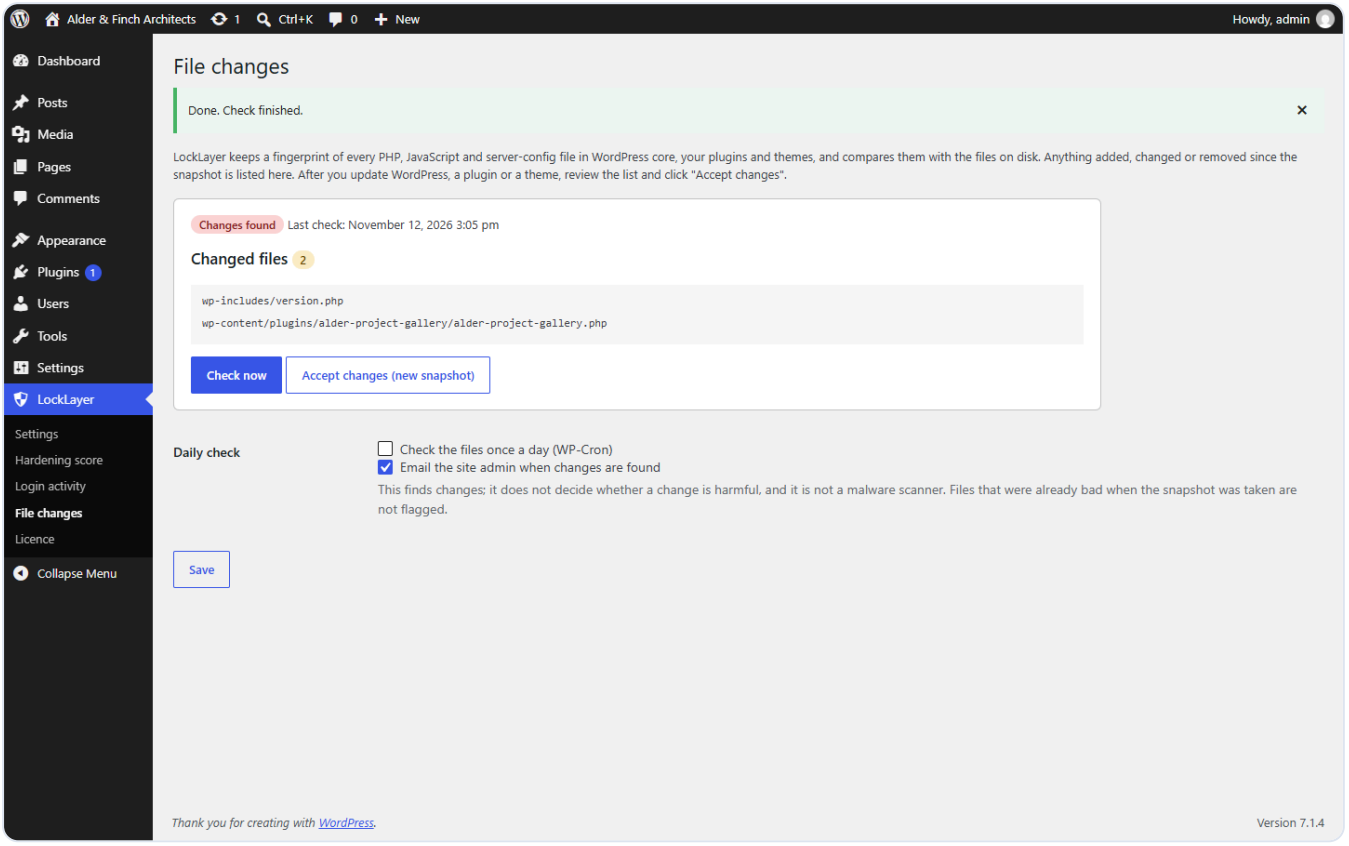


Every login, failed login, lockout, two-factor check, blocked visit, password reset and logout, with user, IP address, country (when known) and time. Filter by event or search by user, IP or detail; **Export CSV** downloads the filtered list. Entries are kept for 90 days by default (change it under **Log settings**).

8. File changes (Pro)

Screenshots: ,





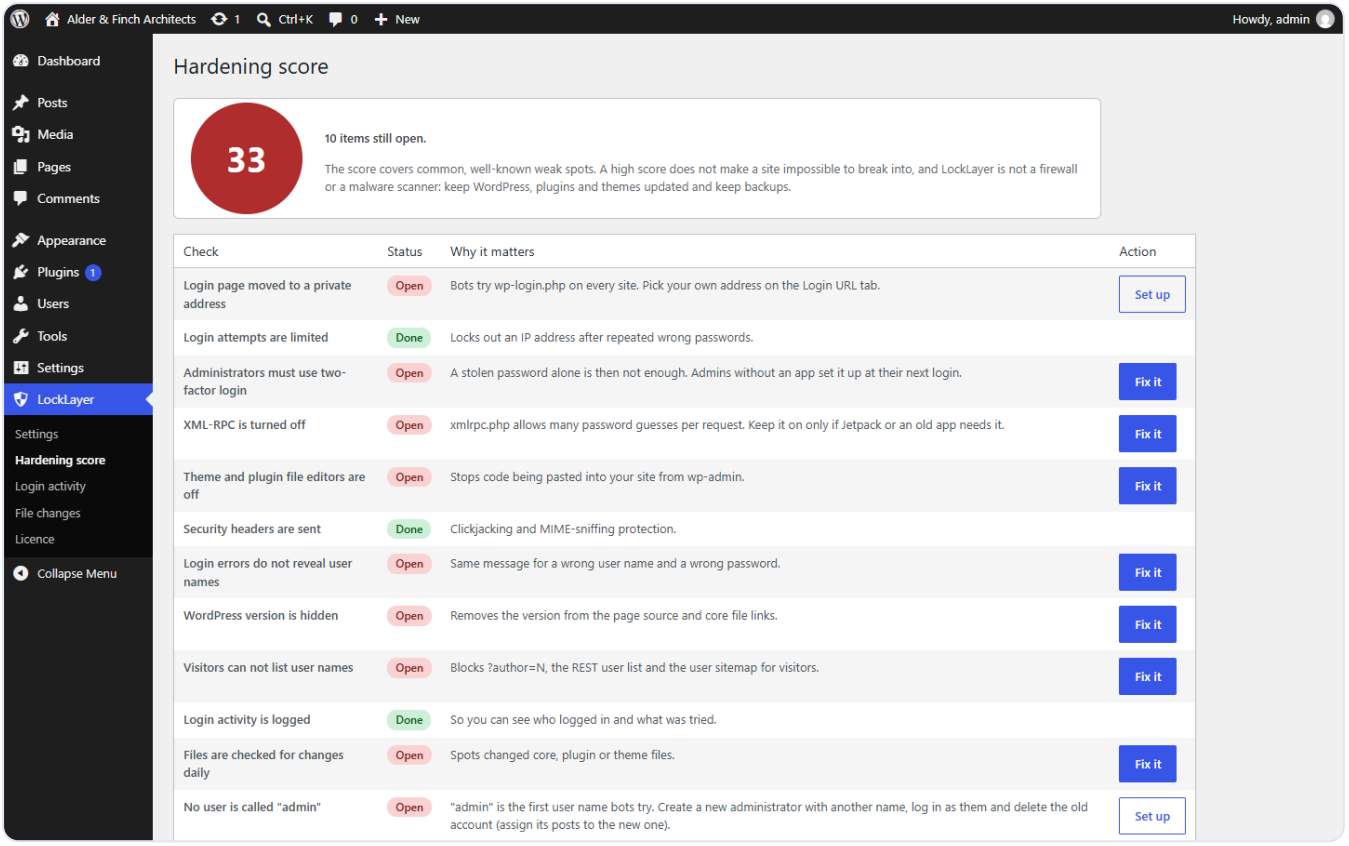
1. Click **Check now** to take the first snapshot (a fingerprint of every PHP, JavaScript, HTML and server-config file in WordPress core, plugins, themes and must-use plugins).
2. Later checks list files that were **changed**, **added** or **removed**, and any PHP file in the uploads folder.
3. After updating WordPress, a plugin or a theme, review the list and click **Accept changes**.
4. Tick **Check the files once a day** to run it with WP-Cron and get an email when something changes.

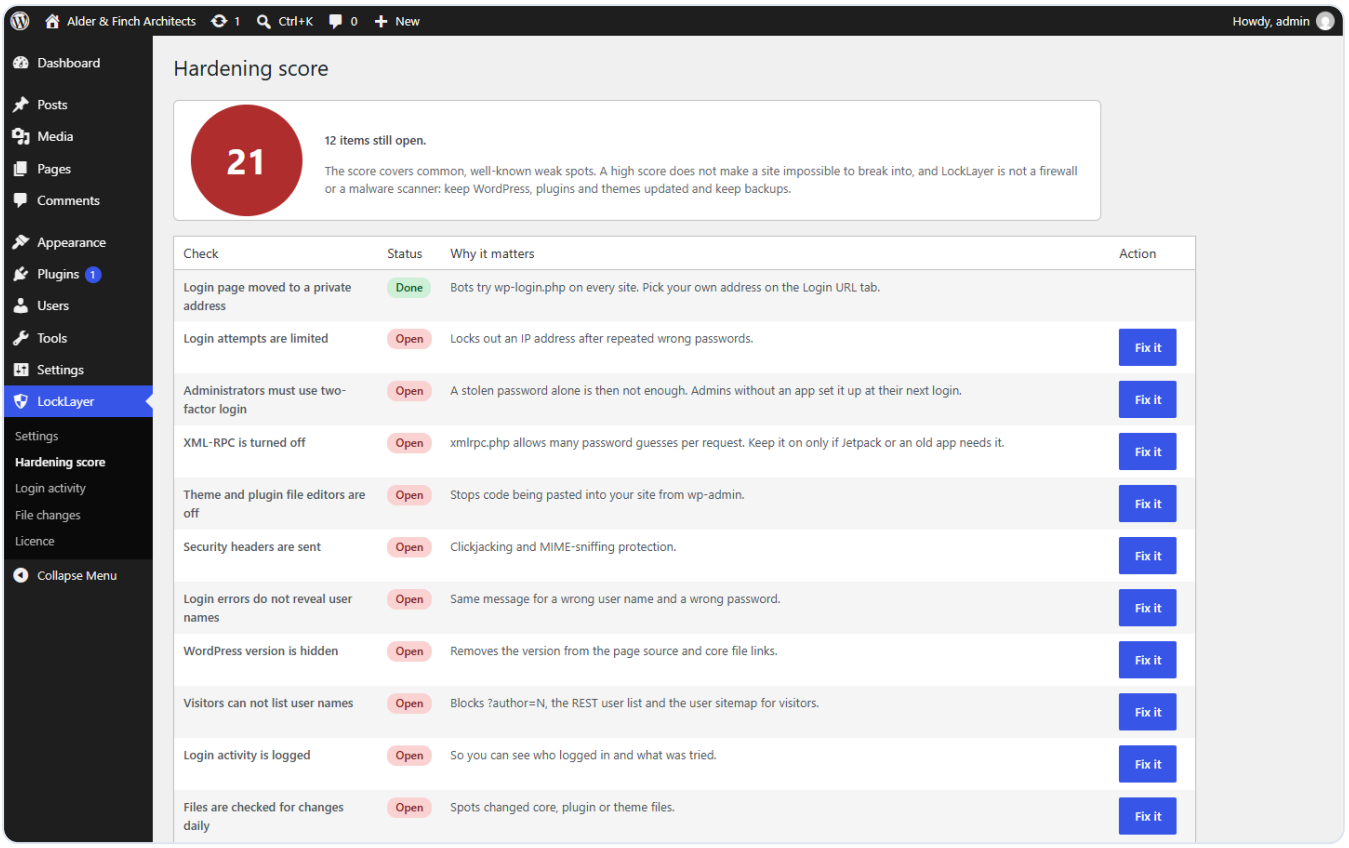
It finds changes since the snapshot. It does not decide whether a change is harmful, and files that were already bad when the snapshot was taken are not flagged.

---

9. Hardening score (Pro)

Screenshots: ,





A checklist with a score out of 100. Items LockLayer controls have a **Fix it** button; every fix only changes LockLayer settings and gets an **Undo** button that restores the previous values. Items it can not change for you (a user called "admin", HTTPS, PHP version, debug display, PHP files in uploads, a custom login address) link to where you fix them.

---

10. Recovery & data tab

If you are locked out:

1. Add `define( 'LLSH_DISABLE', true );` to `wp-config.php` above "That's all, stop editing!". The normal `wp-login.php` works again and no lockout, IP rule or two-factor check applies. Log in, fix the setting, then remove the line.
2. Or rename the plugin folder (`wp-content/plugins/locklayer`). WordPress switches the plugin off.
3. Lockouts end by themselves; another network (your phone on mobile data) is not affected.

Delete all plugin data when the plugin is deleted — off by default so you can swap Free for Pro. Deleting the plugin always brings back the normal login page; LockLayer never writes to `.htaccess` or `wp-config.php`.

FAQ

Does it work with page caching? Yes. Lockouts and the login address are handled on the login request, which caches skip. Security headers are sent by WordPress, so a full-page cache that stores headers keeps them.

Multisite? Not tested on multisite yet.

Hooks for developers: `llsh_client_ip`, `llsh_safe_ips`, `llsh_security_headers`, `llsh_visitor_country`, `llsh_file_roots` (filters); `llsh_lockout`, `llsh_blocked`, `llsh_2fa_passed`, `llsh_2fa_failed` (actions).

Troubleshooting

- *"Too many failed login attempts"* — wait for the lockout, use another network, or add `LLSH_DISABLE`.
- *The login address shows "page not found"* — check the address on the Login URL tab; with "Plain" permalinks use `/?address`.
- *Two-factor codes are refused* — the phone's clock must be right (set it to automatic time). Use a backup code to get in.
- *Country rules do nothing* — the Rules tab shows "Country: not detected": your server or CDN does not add the header you chose.