

Step-by-Step Security Hardening for WordPress on a Public VPS

☐ Overview

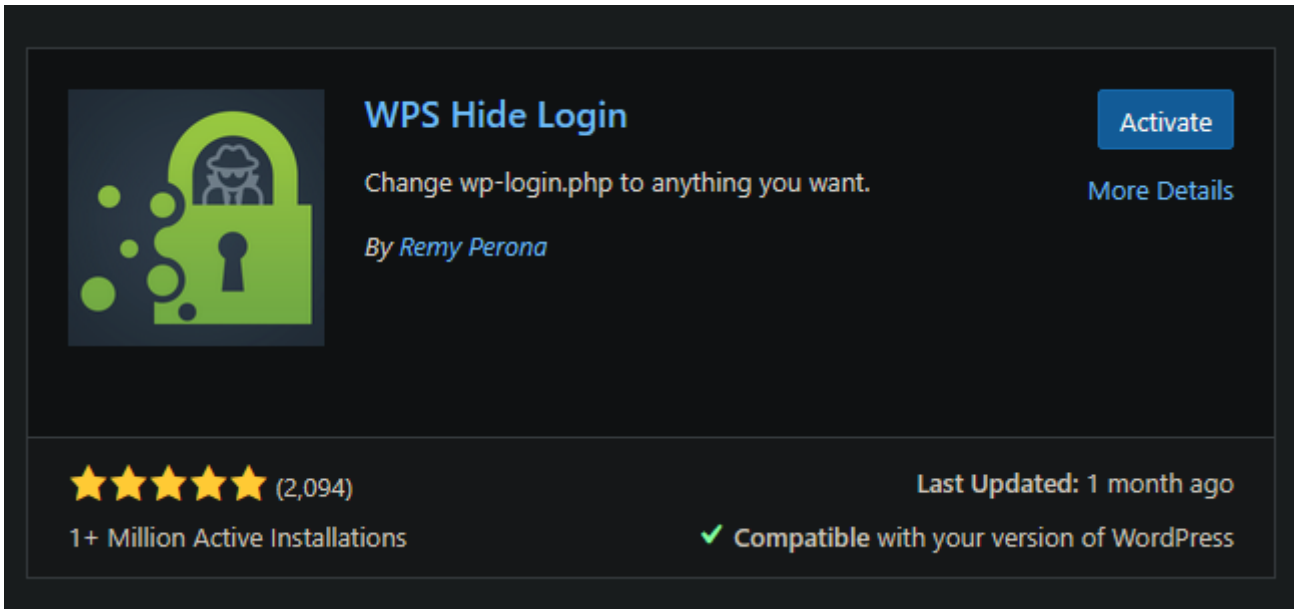
This guide explains how to harden your public WordPress site using free plugins and smart configuration. It includes login obfuscation, brute-force protection, 2FA, and XML-RPC lockdown.

☐ Step 1: Hide the Default Login Page

Change the default `/wp-admin` or `/wp-login.php` to prevent brute-force login scans.

➤ Install the Plugin

Go to **Plugins > Add New**, and search for **WPS Hide Login**.

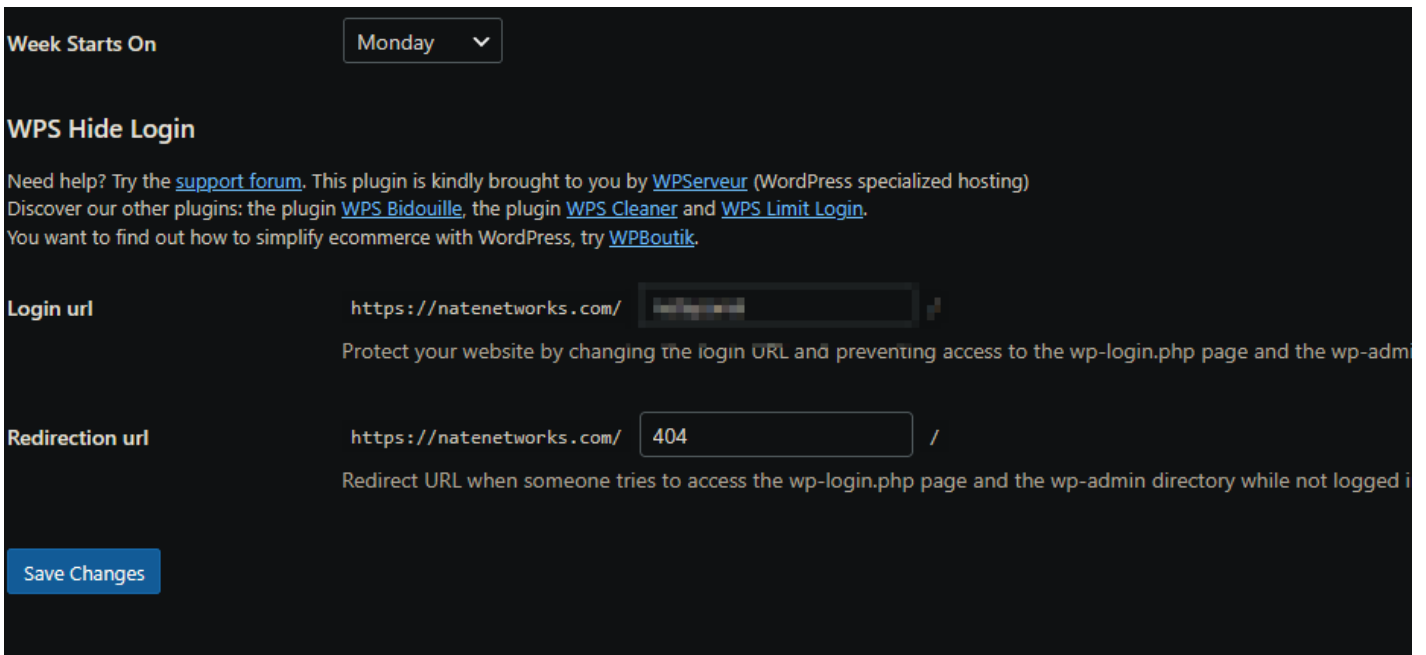


The screenshot shows the 'WPS Hide Login' plugin card. On the left is a green icon of a padlock with a person inside. The title 'WPS Hide Login' is in blue. Below it, the description reads 'Change wp-login.php to anything you want.' and the author is 'By Remy Perona'. On the right, there is a blue 'Activate' button and a link for 'More Details'. At the bottom, there are five yellow stars with '(2,094)' next to them, '1+ Million Active Installations', and 'Last Updated: 1 month ago'. A green checkmark icon is followed by the text 'Compatible with your version of WordPress'.

Click **Activate** and proceed to **Settings > General** to configure.

⚙️ Configure Login Path

Change the login path to something unique like <secret panel> and redirect unauthorized users to `/404`.



The screenshot shows the 'WPS Hide Login' settings page. At the top, 'Week Starts On' is set to 'Monday'. Below the title, there is a help section with links to a support forum and other plugins. The 'Login url' field is set to 'https://natenetworks.com/' followed by a blurred path. Below it, a note says 'Protect your website by changing the login URL and preventing access to the wp-login.php page and the wp-admin'. The 'Redirection url' field is set to 'https://natenetworks.com/ 404 /'. Below it, a note says 'Redirect URL when someone tries to access the wp-login.php page and the wp-admin directory while not logged in'. At the bottom left, there is a blue 'Save Changes' button.

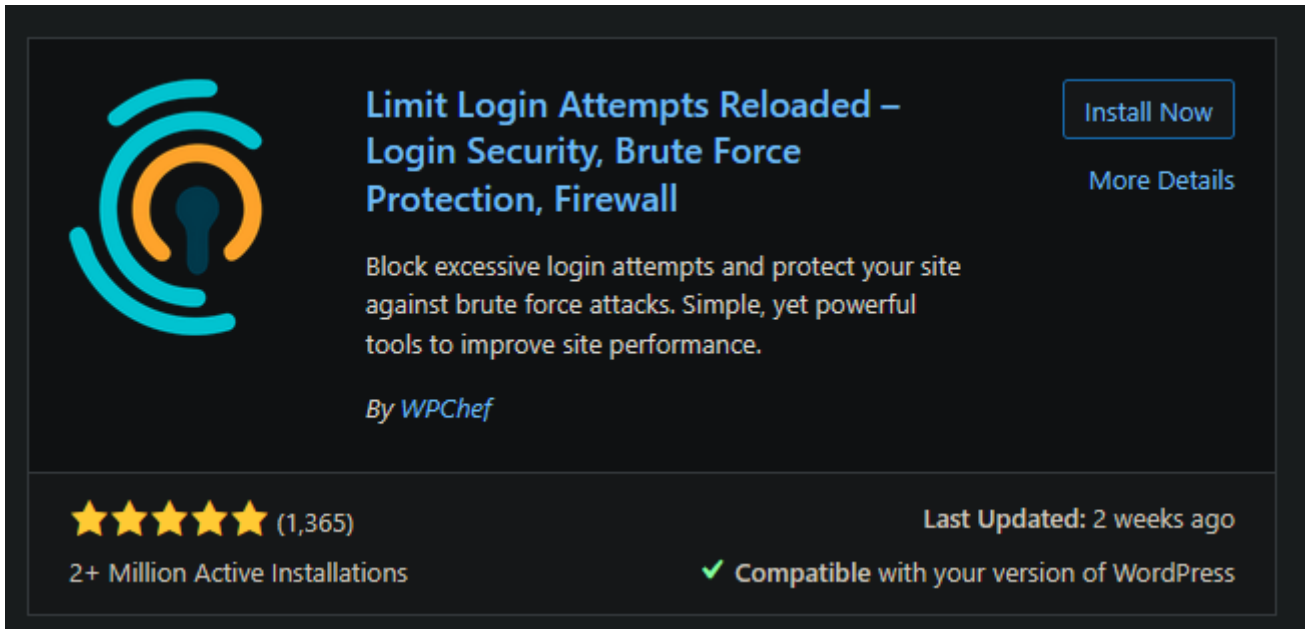
Click **Save Changes** to finalize the setting.

📄 Step 2: Rate-Limit Login Attempt

Block bots and brute-force attempts using **Limit Login Attempts Reloaded**.

► Install the Plugin

Search for **Limit Login Attempts Reloaded**.



The screenshot shows the WordPress plugin page for "Limit Login Attempts Reloaded". On the left is a logo consisting of three concentric circles in blue and orange with a keyhole in the center. The main title is "Limit Login Attempts Reloaded – Login Security, Brute Force Protection, Firewall". Below the title is a description: "Block excessive login attempts and protect your site against brute force attacks. Simple, yet powerful tools to improve site performance." The author is listed as "By WPChef". On the right side, there are two buttons: "Install Now" and "More Details". At the bottom left, there are five yellow stars and the text "(1,365)" and "2+ Million Active Installations". At the bottom right, it says "Last Updated: 2 weeks ago" and "Compatible with your version of WordPress" with a green checkmark.

☐ Skip Premium Prompts

Click “No, I don’t want advanced protection” during setup:

Not A Premium User?

We **highly recommend** upgrading to premium for the best protection against brute force attacks and unauthorized logins

- ✦ Detect, counter, and deny unauthorized logins with IP Intelligence
 - ✦ Absorb failed login activity to improve site performance
 - ✦ Block IPs by country, premium support, and much more!



Yes, show me plan options

No, I don't want advanced protection

Skip

Then skip the email/cloud opt-in:

Cloud Opt-in Skip
Google Analytics or Type unknown

⚙️ Set Lockout Thresholds

Once installed, configure:

- **Allowed retries:**
- **Lockout time:**
- **Lockout escalation:** After 4 fails, extend to
- **Retry reset:**

Use for trusted IP origins.

☐☐ Step 3: Enforce Two-Factor Authentication (2FA)

Add strong login protection with time-based one-time codes using **WP 2FA**.

➤ Install the Plugin

Search and install **WP 2FA**:



The screenshot shows the WordPress plugin marketplace entry for 'WP 2FA – Two-factor authentication for WordPress'. The plugin is by Melapress and has a rating of 4.5 stars from 145 reviews. It has over 70,000 active installations and was last updated 4 weeks ago. A green checkmark indicates it is compatible with the user's version of WordPress. The 'Install Now' button is highlighted with a blue border.

WP 2FA – Two-factor authentication for WordPress

Get better WordPress login security; add two-factor authentication (2FA) for all your users with this easy-to-use plugin.

By Melapress

★★★★☆ (145)

70,000+ Active Installations

Last Updated: 4 weeks ago

✓ Compatible with your version of WordPress

[Install Now](#)

[More Details](#)

☐☐ Configure Authentication Method

In the wizard:

- Enable **TOTP App** (Google Authenticator, Authy, etc.)
- Optionally enable **Email fallback**

□ Set Grace Period

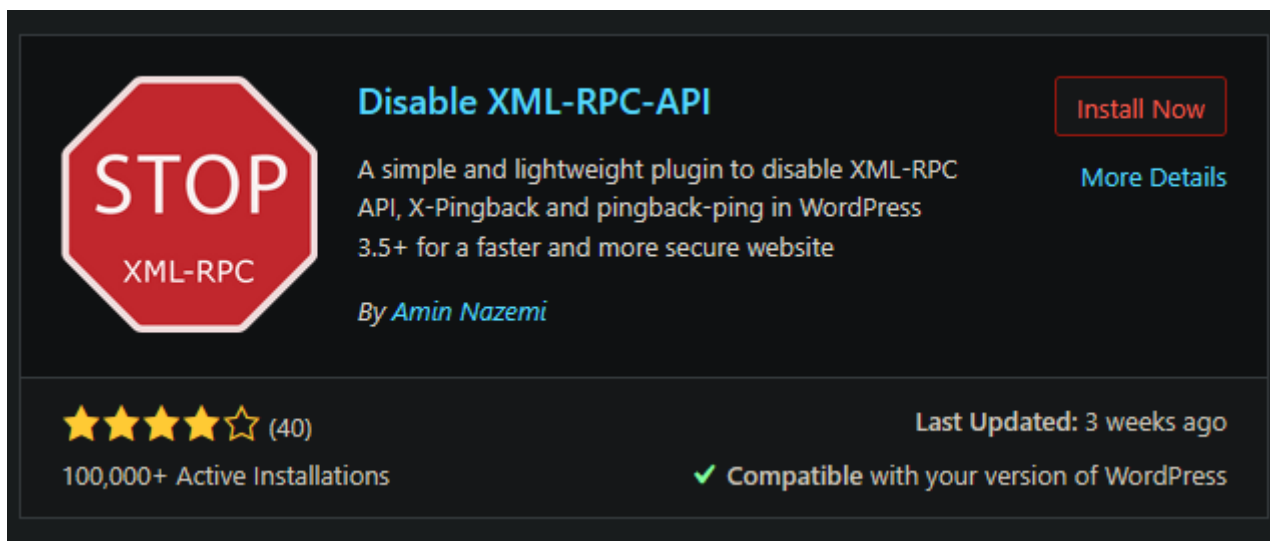
Allow users a short time (e.g., 3 hours) to configure 2FA.
Choose to block dashboard access if they don't enroll in time.

✂ Step 4: Disable XML-RPC

XML-RPC is often abused and rarely needed unless you're using remote publishing or Jetpack.

► Install the Plugin

Search for **Disable XML-RPC-API** by **Amin Nazemi**:



The screenshot shows the WordPress plugin directory listing for "Disable XML-RPC-API" by Amin Nazemi. On the left is a red octagonal "STOP XML-RPC" icon. The title "Disable XML-RPC-API" is in blue. Below it is a description: "A simple and lightweight plugin to disable XML-RPC API, X-Pingback and pingback-ping in WordPress 3.5+ for a faster and more secure website". The author is listed as "By Amin Nazemi". On the right, there is a red "Install Now" button and a blue "More Details" link. At the bottom left, there are five yellow stars (4.5 rating) and "(40)" reviews, with "100,000+ Active Installations" below. At the bottom right, it says "Last Updated: 3 weeks ago" and "✓ Compatible with your version of WordPress".

Activate it — no configuration required.

□ Final Notes

You've now:

- Hidden your login URL
- Enabled brute-force protection
- Enforced 2FA
- Disabled a major backdoor vector (XML-RPC)

Revision #1

Created 13 May 2025 00:20:16 by Nate Nash

Updated 13 May 2025 00:26:49 by Nate Nash