04 - WordPress

This will contain updates to wordpress and any plugins used.

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

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

□□ Overview

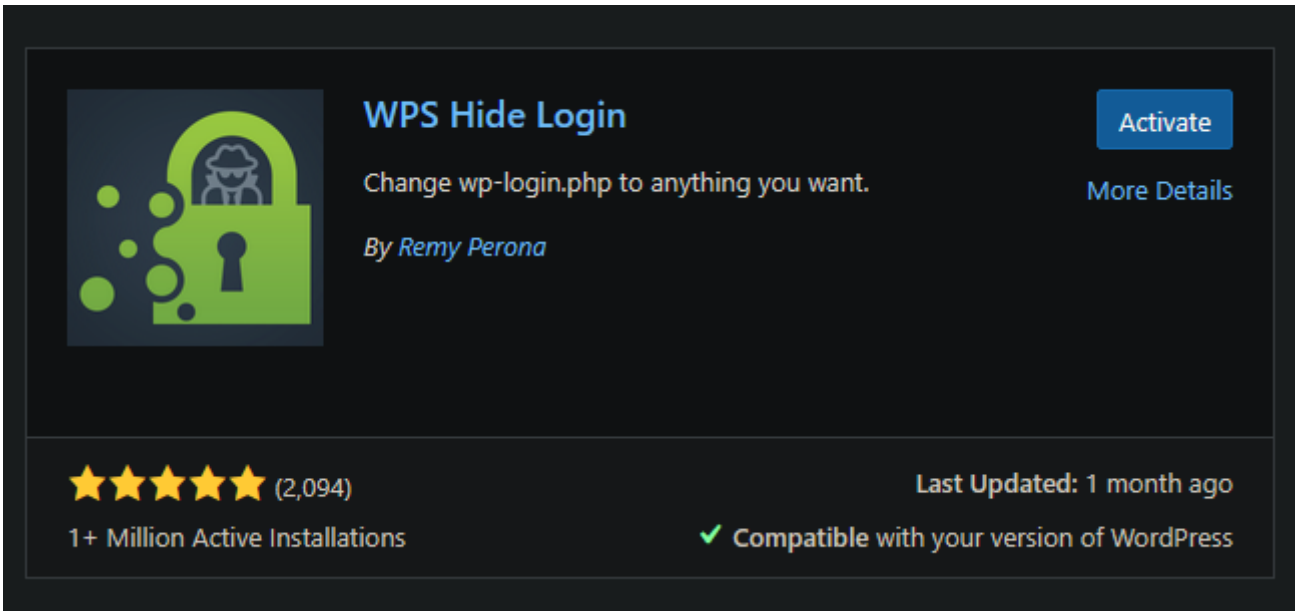
This guide explains how to harden your public WordPress site using free plugins and smart configuration. It includes login obfuscation, brute-force protection, 2FA, and XML-RPC lockdown.

□□ 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

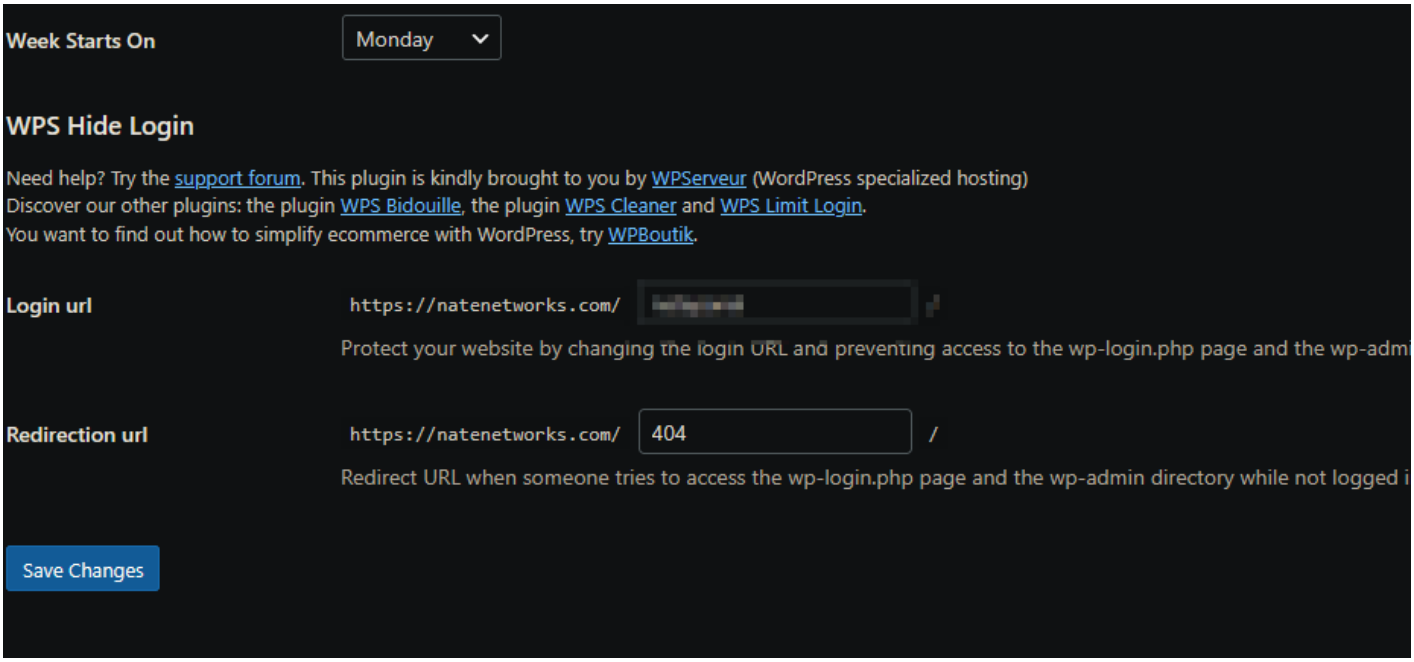
Go to **Plugins > Add New**, and search for **WPS Hide Login**.



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`.



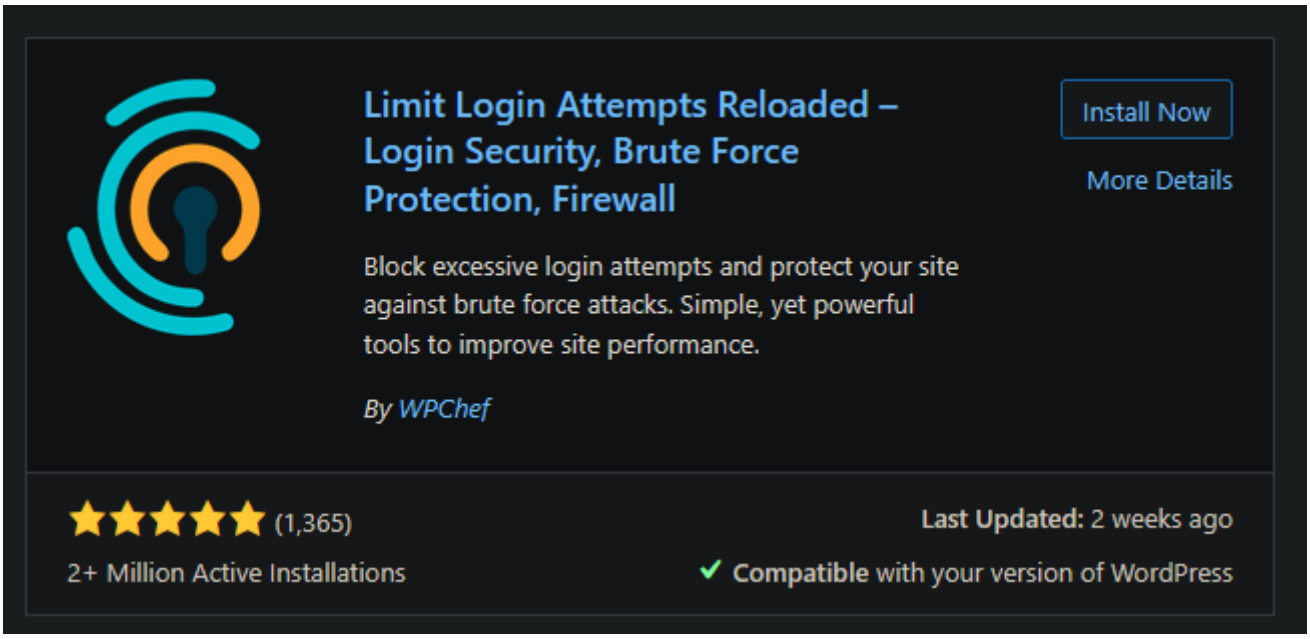
Click **Save Changes** to finalize the setting.

◫ Step 2: Rate-Limit Login Attempt

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

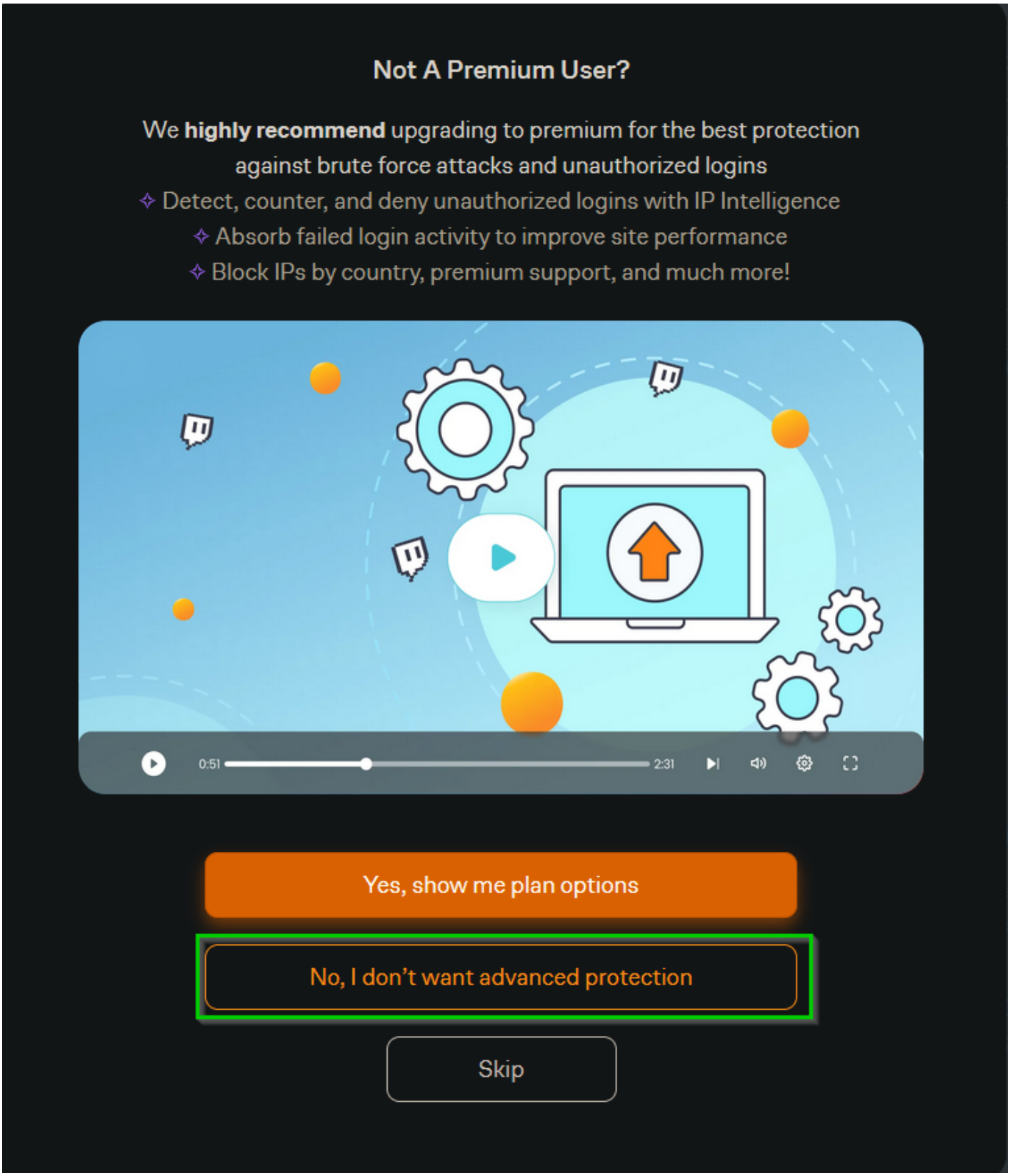
➤ Install the Plugin

Search for **Limit Login Attempts Reloaded**.



◻◻ Skip Premium Prompts

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



Then skip the email/cloud opt-in:

Cloud Opt-in - Skip

Image not found or type unknown

⚙ Set Lockout Thresholds

Once installed, configure:

- **Allowed retries**: `3`
- **Lockout time**: `20 minutes`
- **Lockout escalation**: After 4 fails, extend to `24 hours`
- **Retry reset**: `24 hours`

Use `REMOTE_ADDR` 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**:

□□ Configure Authentication Method

In the wizard:

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

Set Grace Period

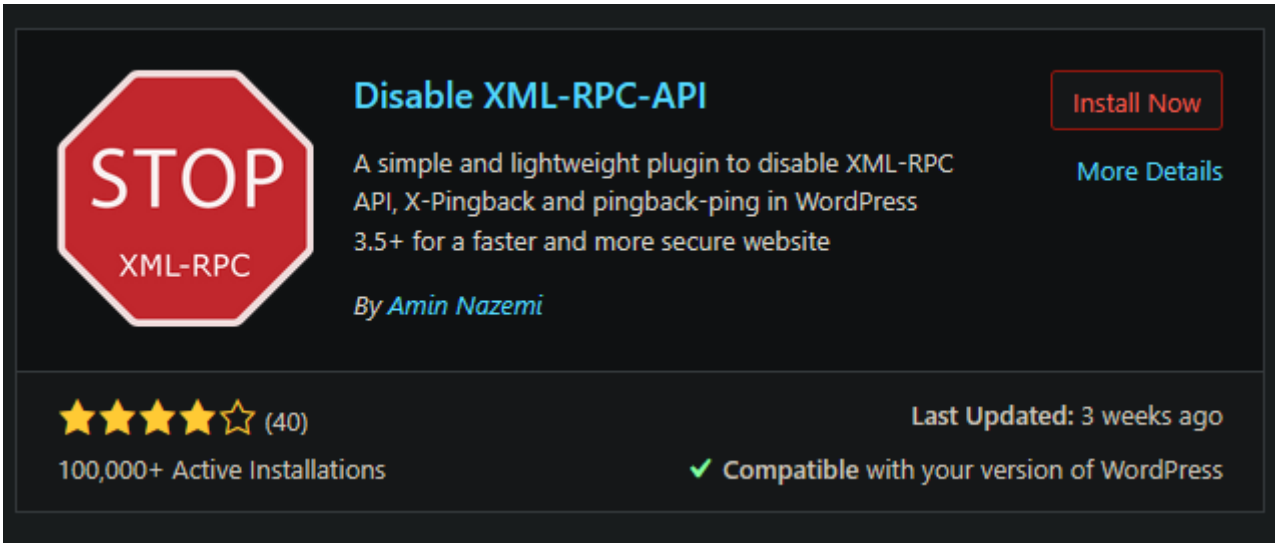
Allow users a short time (e.g., 3 hours) to configure 2FA.
Choose to block dashboard access if they don’t enroll in time.

✂ 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**:



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)