Enabling LiteSpeed reCAPTCHA Bot Protection

Tom Matthews - 2026-02-24 - Website Hosting

How to Enable reCAPTCHA Bot Protection on LiteSpeed Web Server

LiteSpeed Web Server includes a powerful built-in feature that uses Google reCAPTCHA v2 to protect your websites from bots, brute-force attacks, spam submissions, and other automated abuse. When suspicious activity is detected, visitors see a simple “I’m not a robot” checkbox challenge.

This step-by-step guide shows you exactly how to set it up yourself.

Prerequisites

- Access to your LiteSpeed WebAdmin Console (https://YOUR-SERVER-IP:7080)
- A Google account

Step 1: Create Your Google reCAPTCHA v2 Keys

1. Go to the Google reCAPTCHA Creation Dashboard: https://docs.cloud.google.com/recaptcha/docs/create-key-website
2. Sign in with your Google account if prompted.
3. Fill in the form with these recommended settings:
    - **Label**: Enter something descriptive (e.g., “LiteSpeed Bot Protection – example.com”)
    - **reCAPTCHA type**: Select **reCAPTCHA v2 → “Invisible reCAPTCHA badge”** *(This is the required v2 checkbox version for LiteSpeed)*
    - **Domains**: Add your Server’s Hostname (e.g., hostname.example.com).
4. **Important**: In the advanced settings, make sure **“Verify the origin of reCAPTCHA solutions” is unticked** (unchecked). This setting must be disabled for the protection to work correctly across multiple domains or server-wide.
5. Click **Submit**.
6. Copy both keys that appear:
    - **Site Key** (public)
    - **Secret Key** (private – keep this secure)

Tip: Store the keys safely. You will need them in the next step.

Step 2: Log in to the LiteSpeed WebAdmin Console

1. Open your browser and go to: https://YOUR-SERVER-IP:7080 (Replace YOUR-SERVER-IP with your actual server IP address.)
2. Log in with your LiteSpeed admin username and password.

Note: If the page does not load, port 7080 may be blocked by your server's firewall.

Step 3: Configure reCAPTCHA Protection

1. In the left-hand menu, navigate to **Configuration → Server → Security**.
2. Scroll down to the **reCAPTCHA Protection** section.
3. Update the following settings:
    - **Enable reCAPTCHA**: Set to **Yes**
    - **Site Key**: Paste the Site Key from Google
    - **Secret Key**: Paste the Secret Key from Google
    - **Trigger Sensitivity**: Integer 0-100 0 = disabled. 100 = trigger on every request. Higher value = more aggressive.
    - **Max Tries**: Max reCAPTCHA attempts before IP is blocked (403). Default: 3. Raise to 4-5 if legitimate users fail too often.
    - **Verification Expires (secs)**: How long a successful reCAPTCHA remains valid. Default: 86,400 (24 hours). Lower for more frequent challenges.
    - **Allowed Robot Hits**: Hits per 10 seconds allowed for good bots before they may trigger reCAPTCHA. Default: 3. Increase to 10–20 if crawlers are being challenged.
4. (Optional) If you have a **bot whitelist**, add trusted bots, user-agents, or IP addresses here (one per line). Examples:
    - Googlebot
    - Bingbot
    - 192.168.1.100

    Google and Bing bots are automatically whitelisted by default.
5. Click **Apply** (top right), then **Save**.

6. Restart LiteSpeed:
    - Go to the main dashboard or top menu and select **Graceful Restart** (recommended) or **Restart**.

Your bot protection is now active!