iThemes Security Settings Checklist

How To Set Up the iThemes Security Plugin on Your WordPress Website

• 2018 •

iThemes Security Setup Checklist

The iThemes Security plugin includes a one-click WordPress Security check, but you may still have questions about the other settings and how to configure the plugin properly on your website. In this checklist, we walk through a complete iThemes Security setup checklist with an explanation of features and basic WordPress security fundamentals.

WordPress Security Check

- [ ] Run the Security Check to enable the recommend security settings for your site.

Note: Running the Security Check multiple times will re-enable any of the recommended settings that have been disabled.

Global Settings

- [ ] **Write to Files** - In order to take advantage of all that iThemes Security has to offer it will need permission to write to the .htaccess and wp-config.php files.
- [ ] **Host Lockout Message** - This is the customizable message that will display when an IP has been locked out.
- [ ] **User Lockout -** This is the customizable message that will display when a user has been locked out.
- [ ] **Community Lockout Message** - This is the customizable message that will display when an IP has been flagged as bad by the iThemes network.
- [ ] **Blacklist Repeat Offender** - This will allow iThemes Security to ban an IP that has reached the blacklist threshold.
- [ ] **Blacklist Threshold** - The number of lockouts allowed before a permanent ban.
- [ ] **Blacklist Lookback Period** - The length of time a lockout will count towards a permanent ban.
- [ ] **Lockout Period** - The length of time a lockout will last.

Global Settings Cont.

- ☐ **Lockout White List** - This is where you can add user's IPs to prevent them from being locked out.
- ☐ **Log Type** - Choose how you want your logs to be stored.
- ☐ **Days to Keep Database Logs** - The length of time a log entry will be stored in the database.
- ☐ **Allow Data Tracking** - We are not currently tracking any data when this feature is enabled.
- ☐ **Override Proxy Detection** - May help with identifying actual IPs instead of the proxy server's IP.
- ☐ **Hide Security Menu in Admin Bar** - Removes security options from the top bar.
- ☐ **Show Error Codes** - Decide whether or not the lockout messages should display.
- ☐ **Enable Grade Report** - This will allow the Grade Report Module to show in the security settings.

Notification Center

- ☐ **From Email** - This will be the email address used to send security notifications.
- ☐ **Default Recipients** - Select which users will be used as the default recipient list.
- ☐ **Automatic Updates Info** - The automatic update notifications will include updates made by the Version Management feature.
- ☐ **Database Backup** - Choose the email addresses that will receive database backups.
- ☐ **File Change** - The file change email will notify when a file is added, modified or removed.
- ☐ **Grade Report Change** - Receive a notification when your security grade changes.
- ☐ **Inactive Users** - The user security check notification that will send an email when a user who has not logged in for the last thirty days.
- ☐ **Magic Login Link** - Customizable message and subject used for the Magic Link email.
- ☐ **Malware Scan Results** - Receive a notification when the malware scan finds an issue or if the scan repeatedly fails.
- ☐ **Security Digest** - Choose the frequency that you will receive a summary of notifications generated by iThemes Security.
- ☐ **Settings Export** - Customize the email that contains the settings export.

Notification Center Cont.

- ☐ **Site Lockouts** - Receive a notification when an IP or user is locked out. During periods of heavy attack, iThemes Security will generate a ton of emails saying it is doing its job. Disable the lockout notifications to rely on the Digest email for lockout notifications.
- ☐ **Two-Factor Emai**l - Customize the email users will receive that contains the authentication code.
- ☐ **Two-Factor Email Confirmation** - The email a user will receive when setting up Two-Factor.
- ☐ **Two-Factor Reminder Notice** - Customize the email sent to remind users to setup two-factor.

404 Detection

Monitor and lockout users for repeatedly hitting 404s.

- ☐ **Minutes to Remember 404 Error** - How long a 404 will count towards a lockout.
- ☐ **Error Threshold** - The number of 404 errors need for a lockout.
- ☐ **404 File/Folder Whitelist** - Use the whitelist to add any file or folder you do want to count towards a lockout. Keep in mind the 404s will still be recorded in the security logs.
- ☐ **Ignored File Types** - Choose file types that you do not wish to count towards lockouts.

Away Mode

When away mode is active, all traffic trying to access the login page will be redirected to the site's homepage.

- ☐ **Type of Restriction** - Choose if you want Away Mode to occur once or daily.
- ☐ **Start Time** - The time away mode will become active and you will not be able to access the login page.
- ☐ **End Time** - The time away mode will end and you will be able to access the login page.

Banned Users

The setting module you can find all things related to permanent bans.

- ☐ **Default Blacklist** - Permanently ban a list of known bad actors.
- ☐ **Ban Hosts** - The blacklist that will include all of the IPs that iThemes Security had banned. You can also manually add IPs to this list that you would like permanently blocked.
- ☐ **Ban User Agent**s - The list you can use to permanently ban User Agents from accessing the site.

Database Backups

- ☐ **Create a database backup.**
- ☐ **Backup Full Database** - Check the box if you wish to backup everything in the database and not just tables belong to the site.
- ☐ **Backup Method** - Choose how you want your backup delivered.
- ☐ **Backups to Retain** - Set how many local backups you want to keep.
- ☐ **Compress Backup Files** - Choose if you want to have your backup zipped.
- ☐ **Exclude Tables** - Select what table you do not want to include in the backup.
- ☐ **Schedule Database Backups** - Select the frequency that a database backup is created.

File Change Detection

Enable the file change scan to detect changes made on the site.

- ☐ **Files and Folders List** - Select which files you want to exclude from the file change scan. It is common practice to exclude items that are expected to change frequently. A good example of this would be backup and cache directories.
- ☐ **Ignore File Types** - Choose file types that will not be included in the scan.
- ☐ **Display File Change Admin Warning** - Choose if you want to see an admin notification when a change is found.
- ☐ **Compare Online Files** - Compares file hashes of changed WordPress core and iThemes or WordPress.org plugins or themes to their online counterparts.

File Permissions

- [ ] See the iThemes Security suggest file permission settings and compare them to your current file permission settings

Local Brute Force Protection

Settings to mitigate brute force attacks.

- [ ] **Max Login Attempts Per Host** - The number of allowed invalid login attempts per IP before a lockout occurs.
- [ ] **Max Login Attempts Per Host** - The number of allowed invalid login attempts per User before a lockout occurs.
- [ ] **Minutes to Remember Bad Login** - The number of minutes an invalid login attempt will count towards lockout.
- [ ] **Automatically ban admin user** - Immediately LOCKOUT a host that attempts to log in using the admin username.

Network Brute Force Protection

- [ ] Enable to block IPs that have been identified by the iThemes Network as bad actors.

Password Requirements

Manage the password requirements for users.

- [ ] **Force Password Change** - Force all users to change their password on their next login attempt.
- [ ] **Strong Passwords** - Force users to use a strong password.
- [ ] **Password Expiration** - Set the length of time a password can be used.
- [ ] **Refuse Compromised Passwords** - Force users that do not appear in any passwords breaches that are tracked by Have I Been Pwned.

SSL

- [ ] If you have an SSL certificate installed, you can use this setting to redirect all HTTP traffic to HTTPs.

System Tweaks

- ☐ **System Files** - Prevent public access to the readme.html, readme.txt, wp-config.php, install.php, wp-includes, and .htaccess.
- ☐ **Directory Browser** - Prevent users from seeing a list of files in a directory when no index file is listed.
- ☐ **Request Methods** - Filter out hits with trace, delete or track request methods.
- ☐ **Suspicious Query String** - Filter our URLs with suspicious query strings
- ☐ **Non-English Characters** - Filter out non-English characters from URL.
- ☐ **Filter Long URLs** - Filter URLs longer than 255 characters.
- ☐ **Remove File Writing Permissions** - This will set the permissions settings of the wp-config.php and .htaccess files to a secure 0444.
- ☐ **Disable PHP** - Disable PHP execution in the Uploads, Themes and Plugins directory.

WordPress Salts

- ☐ Change the WordPress salts & security keys.

WordPress Tweaks

- ☐ **Windows Live Writer Header** - Remove the Windows Live header if it isn't needed.
- ☐ **EditURI Header** - Removes the RSD header.
- ☐ **Comment Spam** - Prevent comments from bots with no referrer or user-agent.
- ☐ **File Editor** - Disable the WordPress file editor and require using a different tool to edit the theme or other files.
- ☐ **XML-RPC** - Choose how you would like XML-RPC to managed on the site.
- ☐ **Rest API** - Choose how you want the REST API used on the site.
- ☐ **Login Error Messages** - Prevent login error messages from being displayed.
- ☐ **Force Unique Nickname** - Force users to use a unique nickname when updating or creating a new account.
- ☐ **Disable Extra User Archives** - Disable the author page for users with 0 posts.
- ☐ **Protect Against Tabnapping** - Protect visitors against tabnapping external links.
- ☐ **Login with Email Address or Username** - Manage what a user can use to login.
- ☐ **Mitigate Attachment File Traversal Attack** - This helps to mitigate an attack where users with the "author" role or higher could delete any file in your WordPress installation including sensitive files like wp-config.php.

Magic Links

- [ ] The Magic Links feature allows you to log in while your username is locked out by the Local Brute Force Protection feature.

Malware Scan Schedule

- [ ] Automatically scan the site twice daily for malware.

Privilege Escalation

- [ ] Temporarily give a user more access.

reCAPTCHA

- [ ] **Type** - Choose which version of reCAPTCHA you would like to use on the site.
- [ ] **Keys** - Enter your site and secret keys.
- [ ] **Use On** - Choose which pages should use reCAPTCHA.
- [ ] **Language** - Set the language for the reCAPTCHA text.
- [ ] **Use Dark Theme** - A dark theme for reCAPTCHA V2.
- [ ] **reCAPTCHA Position** - Choose the position of invisible reCAPTCHA.
- [ ] **Lockout Error Threshold** - The number of failed reCAPTCHA attempts before a lockout.
- [ ] **Lockout Check Period** - The length of time a failed reCAPTCHA attempt will count towards a lockout.

Settings Import and Export

- [ ] Import or Export a file containing iThemes settings

User Security Check

- [ ] See an overview of users using two-factor, the strength of their last login. You can also send two-factor reminder emails and change their user role.

User Logging

- [ ] Record user actions in the security logs.

Two-Factor Authentication

- ☐ **Authentications Methods** - Select which two-factor methods can be used on the site
- ☐ **Disable Forced Two-Factor Authentication for Certain User Roles** - Disable forced two-factor authentication and on-boarding for certain users.
- ☐ **Disable on First Login** - This simplifies the sign-up flow for users that require two-factor to be enabled for their account.
- ☐ **On-board Welcome Text** - The text users will see during the two-factor on-boarding flow.
- ☐ **Application Passwords** - Application Passwords are used to allow authentication via non-interactive systems, such as XML-RPC or the REST API, without providing your actual password.

Version Management

- ☐ **WordPress Updates** - Automatically update WordPress
- ☐ **Plugin and Theme Updates** - Automatically update plugin and themes. You can customize which plugin or themes to automatically update and choose to delay updates to specific plugins and themes.
- ☐ **Strengthen Site When Running Outdated Software** - When the site is running outdated software, force users to use two-factor disable the WP File Editor (which blocks people from editing plugin or theme code), XML-RPC pingbacks, and block multiple authentication attempts per XML-RPC request (both of which will make XML-RPC stronger against attacks without having to completely turn it off).
- ☐ **Scan for Old WordPress Sites** - Check for outdated WordPress installs on your hosting account.

Grade Report

- ☐ View iThemes Security recommendations to improve the security of the site.

Admin User

- ☐ Change the user ID of the user with the ID of 1
- ☐ **Warning: Only do this on fresh WordPress installs and make a database backup before making the change.**

Change Content Directory

Warning: This is an advanced feature and it will likely cause more problems than it solves.

Change Database Table Prefix

Warning: Only do this on fresh WordPress installs and make a database backup before making the change.

Hide Backend

Warning: While this can add a layer of security through obscurity by changing the login URL, you should rely more on strong passwords and two-factor authentication.

Server Config Rules

These are the iThemes Security rules that need to be written to the .htaccess.

Wp-config.php Rules

- [ ] These are the iThemes Security rules that need to be written to the wp-config.php file.

Get iThemes Security Pro

Get iThemes Security Pro, our WordPress security plugin, with 30+ ways to secure and protect your WordPress site.

Buy Now