



2019



# SETUP GUIDE

A QUICK REFERENCE FOR  
WORDPRESS SECURITY SETTINGS  
& CONFIGURATION

# **TABLE OF CONTENTS**

---

**1**

**INTRODUCTION**

---

**2**

**INTRODUCING THE  
SETTINGS MODULES**

---

**3**

**SECURITY CHECK**

---

**5**

**ITHEMES SECURITY  
SETTINGS EXPLAINED**

---

**12**

**PRO SETTINGS**

---

**20**

**ADVANCED SETTINGS**

---

# INTRODUCTION

---

## ITHEMES SECURITY PLUGIN SETUP & SETTINGS

The iThemes Security plugin offers 30+ ways to secure and protect your WordPress website. In this guide, we walk through all the iThemes Security plugin settings with an in-depth explanation of the features.

# INTRODUCING THE SETTINGS MODULES

All iThemes Security settings are organized into "Modules" on the Settings page.

After installing and activating the plugin on your website, navigate to the **Settings** page within the iThemes Security plugin menu in your WordPress Admin Dashboard.

The screenshot displays the iThemes Security Settings page within a WordPress Admin Dashboard. The left sidebar shows the navigation menu with 'Security' highlighted. The main content area is titled 'iThemes Security' and includes a search bar and filters for 'All (33)', 'Recommended (27)', and 'Advanced (6)'. The settings are organized into a grid of modules, each with a brief description and action buttons. The right sidebar contains additional information, including a malware scan status and a link to create a support ticket.

Module Name	Description	Action Buttons
Security Check	Ensure that your site is using the recommended features and settings.	Show Details
Global Settings	Configure basic settings that control how iThemes Security functions.	Configure Settings
Notification Center	Manage and configure email notifications sent by iThemes Security related to various settings modules.	Configure Settings
404 Detection	Automatically block users snooping around for pages to exploit.	Learn More, Enable
Away Mode	Disable access to the WordPress Dashboard on a schedule.	Learn More, Enable
Banned Users	Block specific IP addresses and user agents from accessing the site.	Configure Settings, Disable
Database Backups	Create backups of your site's database. The backups can be created manually and on a schedule.	Configure Settings, Disable
File Change Detection	Monitor the site for unexpected file changes.	Learn More, Enable
File Permissions	Lists file and directory permissions of key areas of the site.	Show Details
Local Brute Force Protection	Protect your site against attackers that try to randomly guess login details to your site.	Configure Settings, Disable
Network Brute Force Protection	Join a network of sites that reports and protects against bad actors on the internet.	Configure Settings, Disable
Password Requirements	Manage and configure Password Requirements for users.	Configure Settings

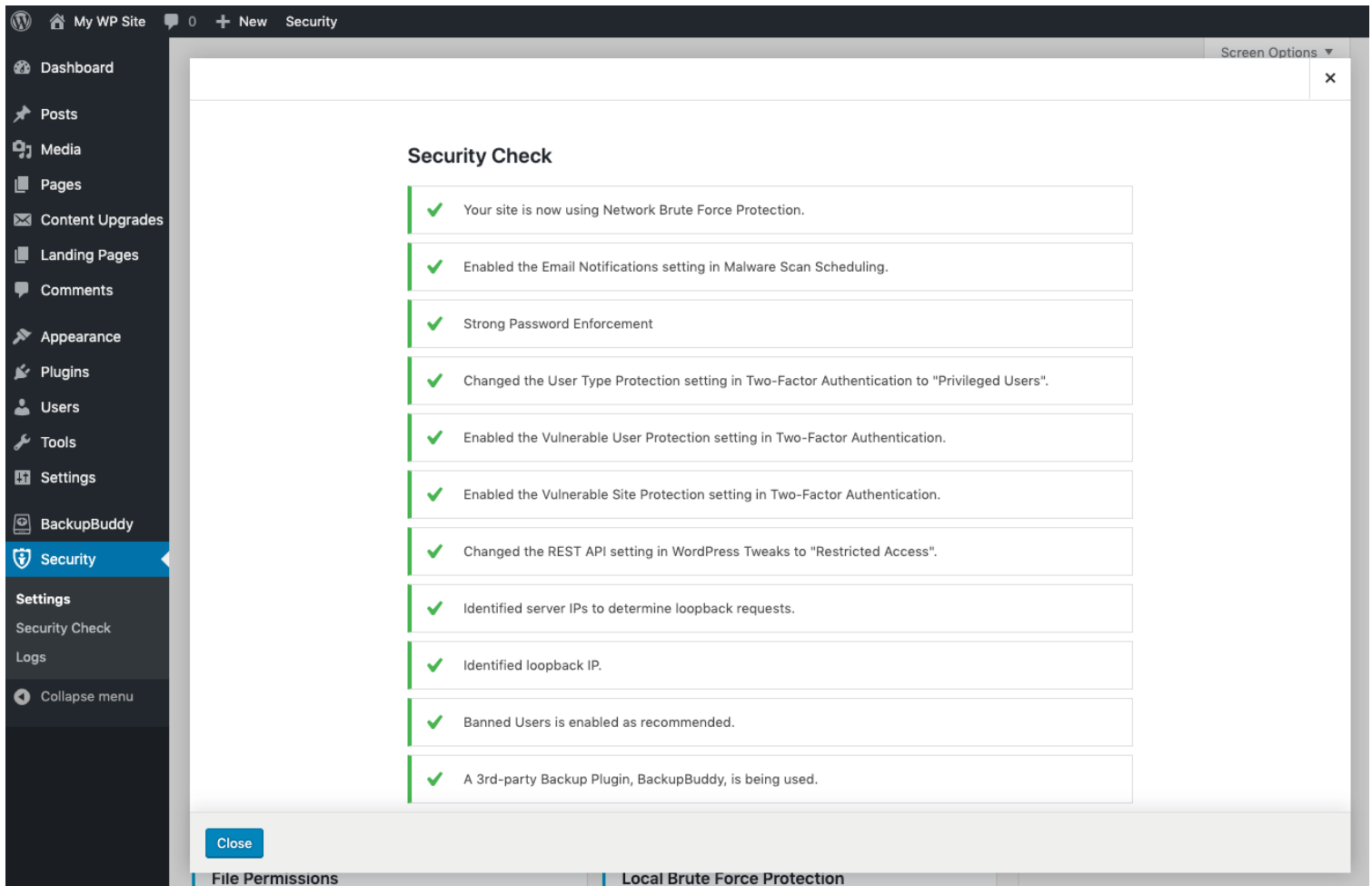
**Malware Scan**  
This malware scan is powered by [Sucuri SiteCheck](#). It checks for known malware, blacklisting status, website errors and out-of-date software. Although the Sucuri team does its best to provide thorough results, 100% accuracy is not realistic and is not guaranteed.  
Results of previous malware scans can be found on the [logs page](#).  
[Scan Homepage for Malware](#)

**Active Lockouts**  
There are no active lockouts at this time.

**Need Help Securing Your Site?**  
As an iThemes Security Pro customer, you can create a support ticket now. Our team of experts is ready to help.  
[Create a Support Ticket](#)

# SECURITY CHECK

The first module in the list is the **Security Check**. The Security Check ensures your site is using the basic recommended settings.



The screenshot displays the WordPress dashboard with the 'Security' menu item selected. The 'Security Check' module is open, showing a list of 12 security checks, all of which are passed. The checks are as follows:

- ✓ Your site is now using Network Brute Force Protection.
- ✓ Enabled the Email Notifications setting in Malware Scan Scheduling.
- ✓ Strong Password Enforcement
- ✓ Changed the User Type Protection setting in Two-Factor Authentication to "Privileged Users".
- ✓ Enabled the Vulnerable User Protection setting in Two-Factor Authentication.
- ✓ Enabled the Vulnerable Site Protection setting in Two-Factor Authentication.
- ✓ Changed the REST API setting in WordPress Tweaks to "Restricted Access".
- ✓ Identified server IPs to determine loopback requests.
- ✓ Identified loopback IP.
- ✓ Banned Users is enabled as recommended.
- ✓ A 3rd-party Backup Plugin, BackupBuddy, is being used.

At the bottom of the module, there is a 'Close' button and a progress bar with three segments: 'File Permissions', 'Local Brute Force Protection', and a third segment that is not labeled.

# SECURITY CHECK

---



Click the **Secure Site** button to run the **Security Check**.

With the Security Check, the following settings modules will be enabled and configured for you:

- Banned Users
- Database Backups
- Local Brute Force Protection
- Network Brute Force Protection
- Strong Passwords
- WordPress Tweaks
- File Change Detection
- Magic Links **PRO**
- Malware Scan Scheduling **PRO**
- Two-Factor Authentication **PRO**
- User Logging **PRO**

Note: Running the Security Check more than once will re-enable recommended settings that have been disabled.

# ITHEMES SECURITY SETTINGS EXPLAINED

---

The following pages give an in-depth explanation of each iThemes Security plugin settings module.

While this information may seem overwhelming at first glance, please note that the Security Check module is designed to handle configuring most of the recommended settings for you. Don't worry—you don't need to enable or manually configure all of these settings one by one!

The remainder of this guide is designed to be a reference for available settings within the plugin. It can also help you evaluate the advantages of the iThemes Security Pro plugin.

- Global Settings
- Notification Center
- 404 Detection
- Away Mode
- Banned Users
- Database Backups
- File Change Detection
- File Permissions
- Local Brute Force Protection
- Network Brute Force Protection
- Password Requirements
- SSL
- System Tweaks
- WordPress Salts
- WordPress Tweaks

- **PRO** Magic Links
- **PRO** Malware Scan Scheduling
- **PRO** Privilege Escalation
- **PRO** reCAPTCHA
- **PRO** Settings Import and Export
- **PRO** Security Dashboard
- **PRO** Two-Factor Authentication
- **PRO** User Logging
- **PRO** User Security Check
- **PRO** Version Management
- **PRO** Trusted Devices (Beta)
- **PRO** Grade Report

# GLOBAL SETTINGS

---

The **Global Settings** module allow you to configure basic settings that control how the iThemes Security plugin functions.

- **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.
- **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. Allow iThemes to track plugin usage via anonymous data.
- **Proxy Detection** - May help with identifying actual IPs instead of the proxy server's IP.
- **Hide Security Menu in Admin Bar** - Remove the Security Messages Menu from the admin bar and receive the messages as traditional WordPress Admin Notices.
- **Show Error Codes** - Decide whether or not the lockout messages should display.
- **Enable Grade Report** **PRO** - This will allow the Grade Report Module to show in the security settings.



# NOTIFICATION CENTER

---

The **Notification Center** settings module allows you to manage and configure all email notifications sent by iThemes Security related to other settings.

- **From Email** - iThemes Security will send notifications from this email address. Leave blank to use the WordPress default.
- **Default Recipients** - Select which users will be used as the default recipient list.
- **Automatic Updates Info** **PRO** - The [Version Management module](#) will send an email with details about any automatic updates that have been performed
- **Database Backup** - The [Database Backup module](#) will send a copy of any backups to the email addresses listed below.
- **File Change** - The [File Change Detection module](#) will email a file scan report after changes have been detected.
- **Grade Report Change** **PRO** - Receive a notification when your security grade changes. This email is generated by the [Grade Report module](#).
- **Inactive Users** - The [User Security Check module](#) sends a list of users who have not been active in the last 30 days so you can consider demoting or removing users.
- **Magic Login Link** **PRO** - Customizable message and subject used for the Magic Link email. This email is generated by the [Magic Links module](#).
- **Malware Scan Results** **PRO** - Receive a notification when the malware scan finds an issue or if the scan repeatedly fails. This email is generated by the [Malware Scan Scheduling module](#).
- **Security Digest** - Choose the frequency of notification summary emails generated by iThemes Security.
- **Settings Export** **PRO** - Customize the email that contains the settings export. This email is generated by the [Settings Import and Export module](#).
- **Site Lockouts** - Receive a notification when an IP or user is locked out. During periods of heavy attack, iThemes Security can generate a large amount of emails as it helps protect your site.
- **Two-Factor Email** **PRO** - Customize the email users will receive that contains the authentication code. This email is generated by the [Two-Factor Authentication module](#).
- **Two-Factor Email Confirmation** **PRO** - The email a user will receive when setting up Two-Factor. This email is generated by the [Two-Factor Authentication module](#).
- **Two-Factor Reminder Notice** **PRO** - Customize the email sent to remind users to setup two-factor. This email is generated by the [User Security Check module](#).
- **Unrecognized Login** **PRO** - Users receive a notification if there is a login from an unrecognized device. This email is generated by the [Trusted Devices \(Beta\) module](#).

## 404 DETECTION

---

The **404 Detection** module allows you automatically block users snooping around for pages to exploit.

- **Minutes to Remember 404 Error** - How long a 404 will count towards a logout.
- **Error Threshold** - The number of 404 errors need for a logout.
- **404 File/Folder Whitelist** - Use the whitelist to add any file or folder you do want to count towards a logout. 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

---

The **Away Mode** module disables access to the WordPress Dashboard on a schedule. 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 **Banned Users** module blocks specific IP addresses and user agents from accessing the site. Here 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 Agents** - The list you can use to permanently ban User Agents from accessing the site.

# DATABASE BACKUPS

---

From the **Database Backups** module, you can create backups of your site's database. The backups can be created manually and on a schedule.

- **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 any tables to exclude from the backup.
- **Schedule Database Backups** - Select the frequency that a database backup is created.

Note: The Database Backup module will send a copy of any backups to the email addresses listed in the Database Backup section of the **Notification Center** module. You can customize the email subject and recipients.

# FILE CHANGE DETECTION

---

The **File Change Detection** module monitors the site for unexpected file changes.

- **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.

Note: The File Change Detection module will email a file scan report after changes have been detected. From the **Notification Center** module, you can enable this email, customize the subject and select which users should receive File Change emails.

## FILE PERMISSIONS

---

The **File Permissions** module lists file and directory permissions of key areas of the site.

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

## LOCAL BRUTE FORCE PROTECTION

---

The **Local Brute Force Protection** module helps protect your site against attackers that try to randomly guess login details.

- **Max Login Attempts Per Host** - The number of allowed invalid login attempts per IP before a lockout occurs.
- **Max Login Attempts Per User** - 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

---

The **Network Brute Force Protection** module allows you to join a network of sites that reports and protects against bad actors on the internet.

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

## PASSWORD REQUIREMENTS

---

In the **Password Requirements** module, you can manage the password requirements for users.

- **Strong Passwords** - Force users to use a strong password.

## SSL

---

In the SSL module, you can configure use of SSL to ensure that communications between browsers and the server are secure.

- **If you have an SSL certificate installed, you can use this setting to redirect all HTTP traffic to HTTPS.**

## SYSTEM TWEAKS

---

The **System Tweaks** module contains advanced settings that improve security by changing the server config for this site.

- **System Files** - Prevent public access to 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 out 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 directories.

# WORDPRESS SALTS

---

The **WordPress Salts** module allows you to update the secret keys WordPress uses to increase the security of your site.

- **Change the WordPress salts & security keys.** Note that changing the salts will log you out of your WordPress site.

# WORDPRESS TWEAKS

---

The **WordPress Tweaks** module contains advanced settings that improve security by changing default WordPress behavior.

- **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 be 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.

# PRO SETTINGS

While the free version of the iThemes Security plugin will secure your website on a basic level, Pro settings are designed to add an even stronger layer of protection to your website.

Pro settings can be accessed from the **Settings** page like all other iThemes Security settings modules.

- **PRO** Magic Links
- **PRO** Malware Scan Scheduling
- **PRO** Privilege Escalation
- **PRO** reCAPTCHA
- **PRO** Settings Import and Export
- **PRO** Security Dashboard
- **PRO** Two-Factor Authentication
- **PRO** User Logging
- **PRO** User Security Check
- **PRO** Version Management
- **PRO** Trusted Devices (Beta)
- **PRO** Grade Report

The screenshot shows the iThemes Security Pro settings page within a WordPress dashboard. The left sidebar contains navigation links: Dashboard, Posts, Media, Pages, Content Upgrades, Landing Pages, Comments, Appearance, Plugins, Users, Tools, Settings, BackupBuddy, and Security (highlighted). Below the Security link are sub-links for Settings, Security Check, Logs, and a Collapse menu button. The main content area displays a grid of 12 settings modules, each with a description and action buttons. The 'PRO' label is visible in the top right corner of each module's header.

Module Name	PRO Label	Action Buttons
WordPress Tweaks	No	Configure Settings, Disable
Magic Links	Yes	Configure Settings, Disable
Malware Scan Scheduling	Yes	Configure Settings, Disable
Privilege Escalation	Yes	Learn More, Enable
reCAPTCHA	Yes	Configure Settings, Disable
Settings Import and Export	Yes	Configure Settings
Security Dashboard	Yes	Learn More, Enable
Two-Factor Authentication	Yes	Configure Settings, Disable
User Logging	Yes	Configure Settings, Disable
User Security Check	Yes	Configure Settings
Version Management	Yes	Configure Settings, Disable
Trusted Devices (Beta)	Yes	Learn More, Enable

## MAGIC LINKS **PRO**

---

From the **Magic Links** module, you can configure a setting to send an email with a Magic Link that bypasses a username lockout.

- **Enable** - The Magic Links feature allows you to log in while your username is locked out by the Local Brute Force Protection feature. When your username is locked out, you can request an email with a special login link. Using the emailed link will bypass the username lockout for you while brute force attackers are still locked out.

Note: The Magic Links module sends an email with a Magic Link that bypasses a username lockout. From the **Notification Center** module, you can customize the subject and message of this email. Basic HTML and some email tags are supported.

## MALWARE SCAN SCHEDULING **PRO**

---

With the **Malware Scan Scheduling** module, you can protect your site with automated malware scans. When this feature is enabled, the site will be automatically scanned each day. If a problem is found, an email is sent to select users.

- **Enable**

Note: The Malware Scan Scheduling module sends an email if it discovers an issue or has repeated difficulty conducting the scan. From the **Notification Center** module, you can enable this email and select recipients.

## PRIVILEGE ESCALATION **PRO**

---

With the **Privilege Escalation** module, you can allow administrators to temporarily grant extra access to a user of the site for a specified period of time.

- **Enable** - Temporarily give a user more access.



## RECAPTCHA **PRO**

---

The **reCAPTCHA** module protects your site from bots by verifying that the person submitting comments or logging in is indeed human.

- **Enable, then Configure Settings.**
  - **Type** - Choose which version of reCAPTCHA you would like to use on the site.
  - **Site Key** - To use this feature you need a free site key and secret key from Google reCAPTCHA.
  - **Secret Key** - To use this feature you need a free secret key and secret key from Google reCAPTCHA.
  - **Enable GDPR Opt-in** - To assist with GDPR compliance, iThemes Security can prompt the user to accept Google's Privacy Policy and Terms of Service before loading the reCAPTCHA API.
  - **Use on Login** - Use reCAPTCHA for user login.
  - **Use on New User Registration** - Use reCAPTCHA for user registration.
  - **Use on Comments** - Use reCAPTCHA for new comments.
  - **Language** - Set the language for the reCAPTCHA text.
  - **Use Dark Theme** - A dark theme for reCAPTCHA V2.
  - **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.
  - **Include Script** - Specify where the reCAPTCHA script should be loaded. Google recommends including the script on all pages to increase accuracy.
  - **Block Threshold** - Google reCAPTCHA assigns a score between 0 and 1 describing the legitimacy of the request. A score of 1 is most likely a human, and a score of 0 is most likely a bot.

## SETTING IMPORT & EXPORT **PRO**

---

With the **Settings Import and Export** module, you can export your iThemes Security plugin settings as a backup or to import on other sites for quicker setup.

- **Import or Export a file containing iThemes Security settings.**

Note: The Settings Import Export module sends an email with the settings export file attached. From the **Notification Center** module, you can customize the subject of this email and the message. Basic HTML and certain email tags are supported.

# SECURITY DASHBOARD

PRO

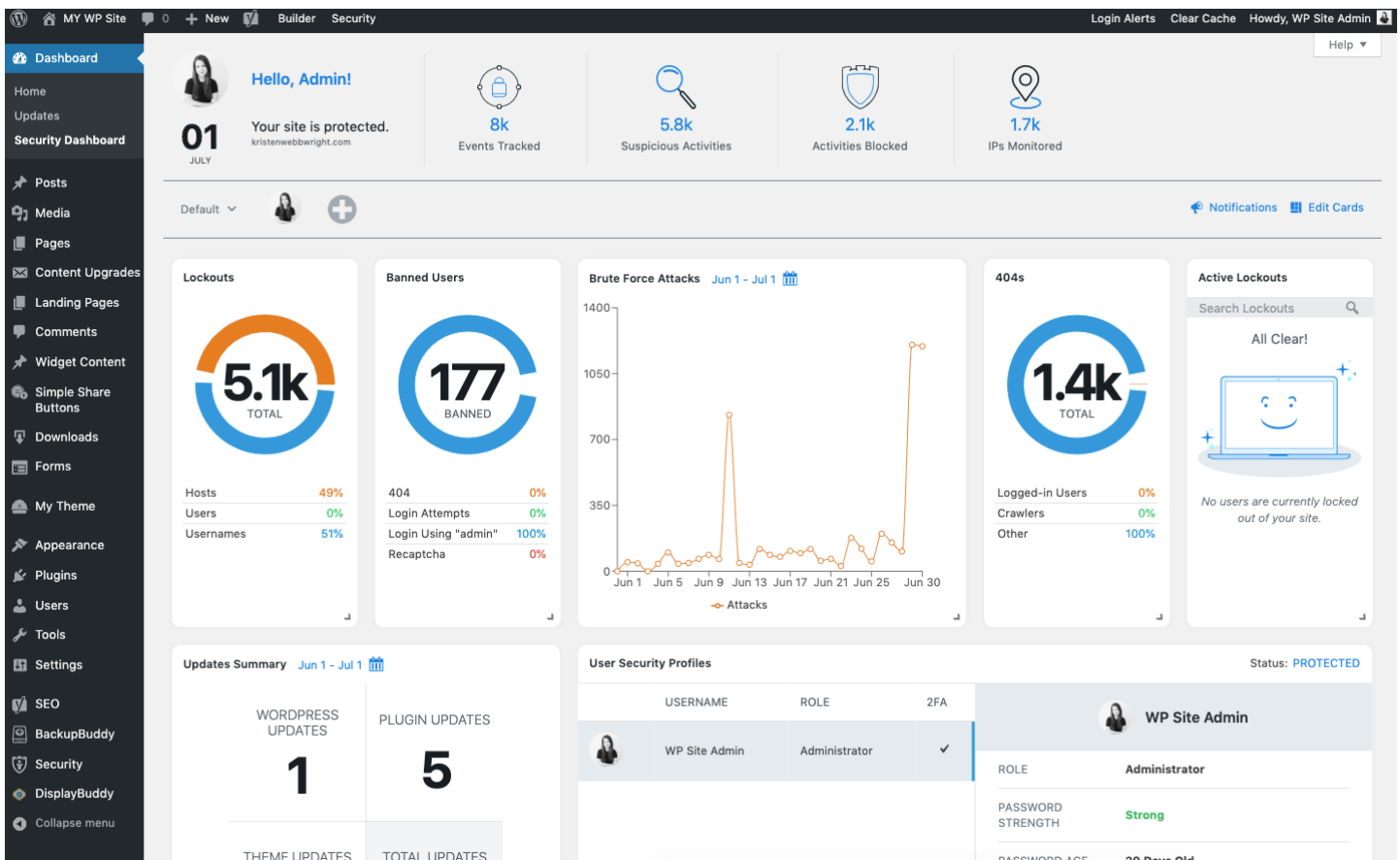
From the **Security Dashboard** module, you can see a real-time overview of the security activity on your website with this dynamic dashboard.

- **Enable, then Configure Settings:**

- **Disable Creating Dashboards for Users** - By default, any user who can manage iThemes Security can create dashboards. Prevent the selected users below from creating dashboards and from viewing/editing Security Dashboard settings.

After enabling, refresh the page to see the new **Security Dashboard** link in your WordPress admin dashboard menu. Visit this link to create your Security Dashboard with the following card options (click the **Edit Cards** link on the right side of the screen):

- User Security Profile
- Active Lockouts
- Database Backups
- 404s
- Banned Users
- Brute Force Attacks
- Lockouts
- Malware Scans
- Trusted Devices
- Updates Summary
- User Security Profiles



# TWO-FACTOR AUTHENTICATION **PRO**

---

The **Two-Factor Authentication** module allows you to enable two-factor authentication. Two-Factor Authentication greatly increases the security of your WordPress user account by requiring additional information beyond your username and password in order to log in.

- **Authentications Methods Available to Users** - Select which two-factor methods can be used on the site.
- **User Type Protection** - Require user accounts of specific roles to use two-factor if the account doesn't already do so. The "Privileged Users" setting is highly recommended as this forces users that can change site settings, software, or content to use two-factor.
- **Disable Forced Two-Factor Authentication for Certain Users** - Disable forced two-factor authentication and on-boarding for certain users.
- **Vulnerable User Protection** - Require user accounts that are considered vulnerable, such as having a weak password or for recent brute force attacks, to use two-factor if the account doesn't already do so. Enabling this feature is highly recommended.
- **Vulnerable Site Protection** - Require all users to use two-factor when logging in if the site is vulnerable, such as running outdated software or software known to be vulnerable. Enabling this feature is highly recommended.
- **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.
- **Allow Remembering Device** - Allow users to check a "Remember This Device" box that, if checked, will prompt the user for a two-factor code for the next 30 days on the current device.

Note: The Two-Factor Authentication module sends an email containing the Authentication Code for users using email as their two-factor provider. From the **Notification Center** module, you can customize the subject and message of this email.

The Two-Factor Authentication module sends an email containing the Authentication Code for users when they are setting up Two-Factor. Try to keep the email similar to the Two Factor Email. Disabling this email will disable the Two-Factor Email Confirmation flow. From the **Notification Center** module, you can customize the subject and message of this email.

## USER SECURITY CHECK **PRO**

---

See how your users might be affecting your security and take action when needed in the **User Security Check** module.

- **Enable** to see an overview of users using two-factor, and the strength of their last login. You can also send two-factor reminder emails and change their user role.

The User Security Check module allows you to remind users to setup two-factor authentication for their accounts. From the **Notification Center** module, you can customize the subject and message of this email.

## USER LOGGING **PRO**

---

With the User Logging module, you can log user actions such as login, saving content and others.

- **Enable** to record user actions in the security logs.

## VERSION MANAGEMENT **PRO**

---

With the **Version Management** module, you can protect your site when outdated software is not updated quickly enough.

- **WordPress Updates** - Automatically update WordPress.
- **Plugin and Theme Updates** - Automatically update plugins 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.

The Version Management module will send an email with details about any automatic updates that have been performed. From the **Notification Center** module, you can enable this email and select recipients.

## TRUSTED DEVICES (BETA) **PRO**

---

The **Trusted Devices** module identifies the devices users use to login and can apply additional restrictions to unknown devices.

- **Minimum Role** - Enable Trusted Devices for users with the selected minimum role.
- **Restrict Capabilities** - When a user is logged-in on an unrecognized device, restrict their administrator-level capabilities and prevent them from editing their login details.
- **Session Hijacking Protection** - Help protect against session hijacking by checking that a user's device does not change during a session.
- **Geolocation** - iThemes Security uses geolocation to improve the accuracy of Trusted Device identification. By default, a number of free GeoIP services are used. We strongly recommend enabling one of the MaxMind APIs.
- **Static Image Map API** - iThemes Security uses static image maps to display the approximate location of an unrecognized login. We recommend using either the Mapbox or MapQuest APIs.

Users can receive a notification if there is a login from an unrecognized device. From the **Notification Center** module, you can enable this email and customize the subject and message of the email.

## PASSWORD REQUIREMENTS **PRO**

---

The **Password Requirements** module includes additional settings for Pro users.

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

# GRADE REPORT PRO

The **Grade Report** module allows you to see your WordPress security grade and fix issues.

**Note: Enable Grade Report** must be selected in the **Global Settings** module for this module to display on the Settings page.

- **Enable** then Configure Settings:
  - **Disable for Users** - Disable the grade report for selected users.

Once enabled, a new **Grade Report** link will appear in your WordPress admin dashboard beneath the Security menu. Click this link to see your Security Grade Report summary. You can manage the Grade Report Change emails from the **Notification Center**.

The Grade Report module can send a notification whenever your Security Grade Report changes. From the Notification Center module, you can enable this email and then customize the subject, schedule (daily or weekly) and message of this email, along with selecting recipients.

The screenshot shows the iThemes Security Grade Report interface. The left sidebar contains the WordPress admin menu with 'Security' highlighted. The main content area is titled 'iThemes Security' and includes 'Manage Settings' and 'Support' links. The 'Grade' section shows a large green 'A' in a circle, indicating the current security grade. Below the grade, it says 'Resolve 1 issue to raise the grade to an "A+"'. A progress bar shows 40% for Software and 60% for Security Settings. The 'Summary' section shows a bar chart with 'Current Score' (blue) and 'Potential Score' (green). The 'Software' section lists various components like PHP Version, WordPress Version, and several plugins, all marked with green checkmarks. The 'Security Settings' section lists various security features like Strong Password Enforcement, Two-Factor Authentication, and Two-Factor Authentication: Available Methods, all marked with green checkmarks.

Category	Item	Status
Software	PHP Version	✓
	WordPress Version	✓
	Plugin: Advanced Code Editor	✓
	Plugin: BackupBuddy	✓
	Plugin: Beacon Plugin	✓
	Plugin: Beautiful Pull Quotes	✓
	Plugin: Classic Editor	✓
Security Settings	Two-Factor Authentication: Available Methods	✓
	Two-Factor Authentication: Disable Two-Factor for Certain Users	✓
	Two-Factor Authentication: User Type Protection	✓
	Two-Factor Authentication: Vulnerable Site Protection	✓
	Strong Password Enforcement	✓
	Two-Factor Authentication	✓

# ADVANCED SETTINGS

---

Several settings can be located by clicking the "Advanced" tab on the settings menu. **Note: These settings are to be used with caution and only by advanced users!**

## ADMIN USER

---

An advanced tool that removes users with a username of "admin" or a user ID of "1".

- 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

---

Advanced feature to rename the wp-content directory to a different name. **Warning: This is an advanced feature and it will likely cause more problems than it solves. This feature can also break custom post types and other plugins.**

## CHANGE DATABASE TABLE PREFIX

---

Change the database table prefix that WordPress uses. **Warning: Only do this on fresh WordPress installs and make a database backup before making the change.**

## HIDE BACKEND

---

Hide the login page by changing its name and preventing access to wp-login.php and wp-admin.

- Hides the login page (wp-login.php, wp-admin, admin and login) making it harder to find by automated attacks and making it easier for users unfamiliar with the WordPress platform.

**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

---

If you need to manually add the server config rules generated by iThemes Security to your server, you can find them [here](#).

## WP-CONFIG.PHP RULES

---

If you need to manually add the wp-config.php rules generated by iThemes Security to your server, you can find them [here](#).





# iThemes Security Pro

Get started with our single site iThemes Security Pro plan for just \$49\* with coupon code **SECUREMYWP**

**BUY NOW FOR \$49 →**

\*Offer good on any \*new\* iThemes Security Pro (1 site) plugin purchase.

Coupon can't be used to renew or extend an existing iThemes Security Pro (1 site) plugin membership.

