

SEM Coaching #50 WordPress Security

By Fabian Lim

Introduction

- WordPress is one of the most popular open-source Content Management Systems (CMS) in the World
- Because of its popularity, it is also a favorite target platform for hackers
- It is therefore essential to adopt sound security measures to prevent your WordPress site from getting hacked
- In doing so, you will be able to not only protect your WordPress site, but also ensure your online business does not get disrupted

WordPress Security Strategies

WordPress Security Strategies

Strategy #1 - Username

- DO NOT use 'admin' as your WordPress username
 - Ensure you use a different Display Name from your actual username

Strategy #2 – Password

- DO NOT use an easy-to-guess WordPress password
 - Use a password generator to generate an impossible-to-guess password

Strategy #3 – Login URL

- MODIFY the default WordPress login URL from: domain.com/wp-admin to domain.com/somethingelse
 - Prevents brute force attempts on your site

WordPress Security Strategies

Strategy #4 – User Registration

DISABLE the default WordPress user registration link (wp-signup.php)

- This prevents subscription spam on your site

Strategy #5 – Database Security

- MODIFY the wp table pre-fix from: ‘wp_’ to ‘somethingelse’
 - This prevents hackers from modifying code on your site via SQL injection

Strategy #6 – File & Folder Permissions

- ENSURE the correct file and folder permissions are used
 - This prevents hackers from accessing and modifying file settings

WordPress Security Strategies

Strategy #7 – Comments Form

- INSTALL a captcha to prevent comment spam

Strategy #8 – Security Plugins & Services

- INSTALL WordPress security plugins to help manage your site security and scan for malware
- Paid services offer backup and restore services, proactively monitor the health of your site and scan your site regularly for security breaches

Strategy #9 – Update WordPress Core, Theme & Plugins

- UPDATE to the latest versions regularly

Solution



EST.

imarketing.courses
BEST PLACE TO LEARN!

2021

Recommended Password Manager

- 1Password.com

The screenshot shows the AgileBits 1Password website. At the top, it says "AgileBits Welcome!" and features the 1Password logo. Below the logo, the text reads: "Have you ever forgotten a password? We all have. With 1Password, it will never happen again." It describes 1Password as a password manager that integrates with web browsers to automatically log in, enter credit card info, fill forms, and generate strong passwords. It also stores confidential information like identities and credit cards in one secure place. The site mentions availability on Mac, Windows, iPhone, iPad, and Android, with "Download..." and "Learn more..." buttons. A section for "Knox" is shown, which complements 1Password for file storage. On the right, there's a sidebar titled "Announcements" with two entries: "1Password for Mac Tips: How to update your passwords" and "Fifth AgileBits team trip finishes with great 1Password plans but not enough labadoozies". The sidebar also contains a paragraph about AgileBits employees traveling.

Announcements

1Password for Mac Tips: How to update your passwords

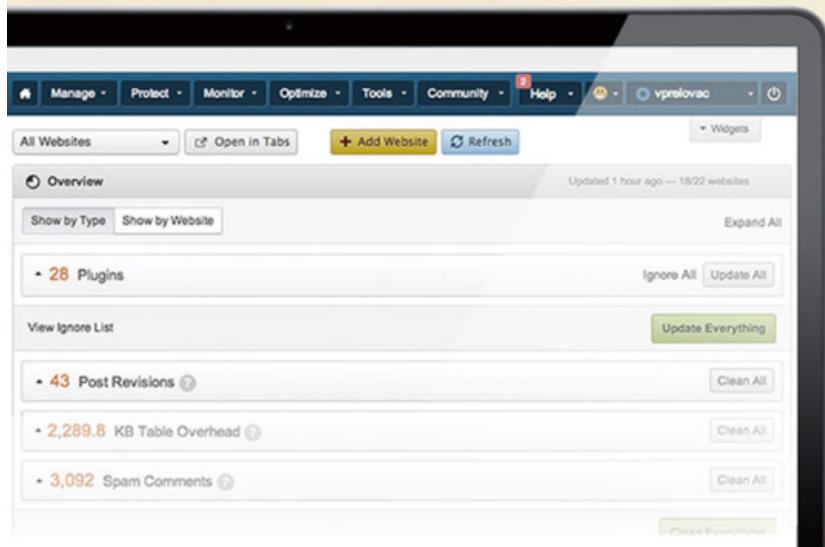
Maybe you have some weak passwords from The Old Days, or maybe a password was stolen in a recent breach. Fortunately, the 1Password extension now makes it easier than ever to change passwords, right in your browser.

Fifth AgileBits team trip finishes with great 1Password plans but not enough labadoozies

Every year, AgileBits likes to get its employees out of the home office. Also the new office, as it were. We usually prefer someplace warm, and this year it was both warm and mobile.



Recommended WordPress Manager - ManageWP.com



Manage all your WordPress sites from one powerful dashboard

- ✓ **ONE-CLICK UPDATES**
Updating your sites and plugins is accomplished with a single click!
- ✓ **AUTOMATED BACKUP & MONITORING**
When things are at their worst, your sites are at their best: safe and secure.
- ✓ **24/7 FIRST-CLASS SUPPORT**
Our average human response time is 35 minutes. This is 30 times better than the industry average.
- ✓ **HIGH SECURITY**
We go above & beyond industry standards to keep your sites protected.

Used by over 5,000 companies

Email address

TRY IT FOR FREE

Some of our clients:

GEORGIAN  WIRED  UCLA

Recommended WordPress Plugin

- All In One WP Security

[Dashboard](#)[System Info](#)

For information, updates and documentation, please visit the [AIO WP Security & Firewall Plugin](#) Page

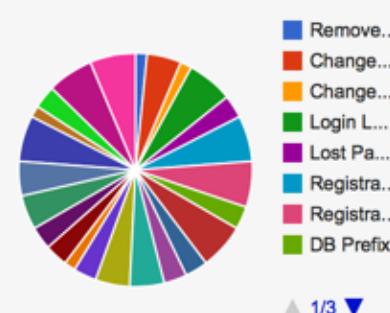
[Follow us](#) on Twitter, Google+ or via Email to stay up to date about the new security features of this plugin.

Security Strength Meter



Total Achievable Points: 410
Current Score of Your Site: 315

Security Points Breakdown



Critical Feature Status

Below is the current status of the critical features that you should activate on your site to achieve a minimum level of recommended security

Admin Username

ON **OFF**

Login Lockdown

ON **OFF**

File Permission

ON **OFF**

Basic Firewall

ON **OFF**

Last 5 Logins



Recommended WordPress Plugin - Sucuri Free



Sucuri SiteCheck Malware Scanner

Scan your site for malware using [Sucuri SiteCheck](#) right in your WordPress dashboard.

Scan this site now!

If you have any questions about these checks or this plugin, contact us at info@sucuri.net or visit sucuri.net

Is your website infected with malware? Blacklisted by Google?

Don't know where to start? Get cleared today by [Sucuri Security!](#)

[Read more »](#)



Recommended Monitoring Service - Sucuri.net



The image shows the homepage of the Sucuri website. At the top, there is a navigation bar with links for HOME, SERVICES, TOUR, PRICING, SUPPORT, COMPANY, BLOG, SIGNUP, and LOGIN. Below the navigation bar, a large green button says "GET CLEAN NOW!!" with the subtext "CLEAN YOUR WEBSITES TODAY WITH SUCURI". To the right of this button is a screenshot of a computer monitor displaying the "Sucuri Tour" page, which includes a video player and some text about the service. Below the main content area, there are three buttons: "SCAN YOUR WEBSITE FOR FREE", "What's your domain?", and "SCAN THIS SITE".

Some Sucuri supported platforms:



TESTIMONIALS

Sucuri Live Chat +

Recommended Monitoring Service - CodeGuard.com

The image shows the homepage of the CodeGuard website. At the top left is the CodeGuard logo. The top navigation bar includes links for Home, Pricing, How It Works, Blog, Get Started (which is highlighted in green), and Login. The main headline reads "Get a time machine for your website." Below it, a sub-headline says "Backup, monitor, and undo changes on your website. Start your free trial today!" There are two buttons: a green "Sign Up" button and a white "What Is CodeGuard?" button with a play icon. To the right of the text is a large, stylized illustration of a time machine. The machine has a large circular clock face at the top with Roman numerals. The date "17/08" is displayed above the number "2012" on the front panel. The machine is surrounded by various mechanical components, pipes, and gauges, all set against a dark background.



‘All In One WP Security’ Plugin User Guide



1. Login to your WordPress admin at 'yourdomain.com/wp-admin'

2. Assuming you have created a WordPress site with the default username 'admin', enter your username and password to login

3. Click 'Log In' to proceed

The screenshot shows the WordPress dashboard. On the left, a sidebar menu includes links for Dashboard, Home, Updates, Posts, Media, Pages, Comments, Appearance, Plugins (which is highlighted with a red box), Users, Tools, Settings, and Collapse menu. A yellow callout points to the 'Plugins' link. Below the sidebar, a sub-menu for 'Plugins' is open, showing 'Installed Plugins' (empty), 'Add New' (highlighted with a red box), and 'Editor'. The main content area features a 'Welcome to WordPress!' message and a 'Next Steps' section with links to write a blog post, add an About page, and view the site. A 'More Actions' section includes links to manage widgets, turn comments on or off, and learn more about getting started. A 'Quick Draft' sidebar allows users to enter a title and what's on their mind, with a 'Save Draft' button. A 'Wordpress News' sidebar mentions a maintenance release on January 23, 2014.

Welcome to WordPress!

We've assembled some links to get you started:

1. Click 'Plugins' on the left hand menu, and then click on 'Add New'

Next Steps

- Write your first blog post
- Add an About page
- View your site

More Actions

- Manage widgets or menus
- Turn comments on or off
- Learn more about getting started

Quick Draft

Title

What's on your mind?

Save Draft

Wordpress News

WordPress 3.8.1 Maintenance Release January 23, 2014

After six weeks and more than 9.3 million downloads of WordPress 3.8, we're

Howdy, 

Screen Options ▾ Help ▾

Install Plugins

Search | Upload | Featured | Popular | Newest | Favorites

Plugins extend and expand the functionality of WordPress. You may automatically install plugins from the [WordPress Plugin Directory](#) or upload a plugin in .zip format via [this page](#).

Search

1. Type in 'all in one wp security'

2. Click 'Search Plugins' button

Popular tags

You may also like:

admin, content, email, Facebook, feed, gallery, google, image, images, javascript, jquery, link, links, login, media, page, pages, photo, photos, plugin, Post, posts, rss, seo, shortcode, sidebar, social, spam, stats, twitter, video, **widget**, widgets, wordpress, youtube

Thank you for creating with WordPress.

Version 3.8.1

Howdy, 

aickl.com 0 + New

Screen Options ▾ Help ▾

Install Plugins

Search | Search Results | Upload | 

Keyword  all in one wp security

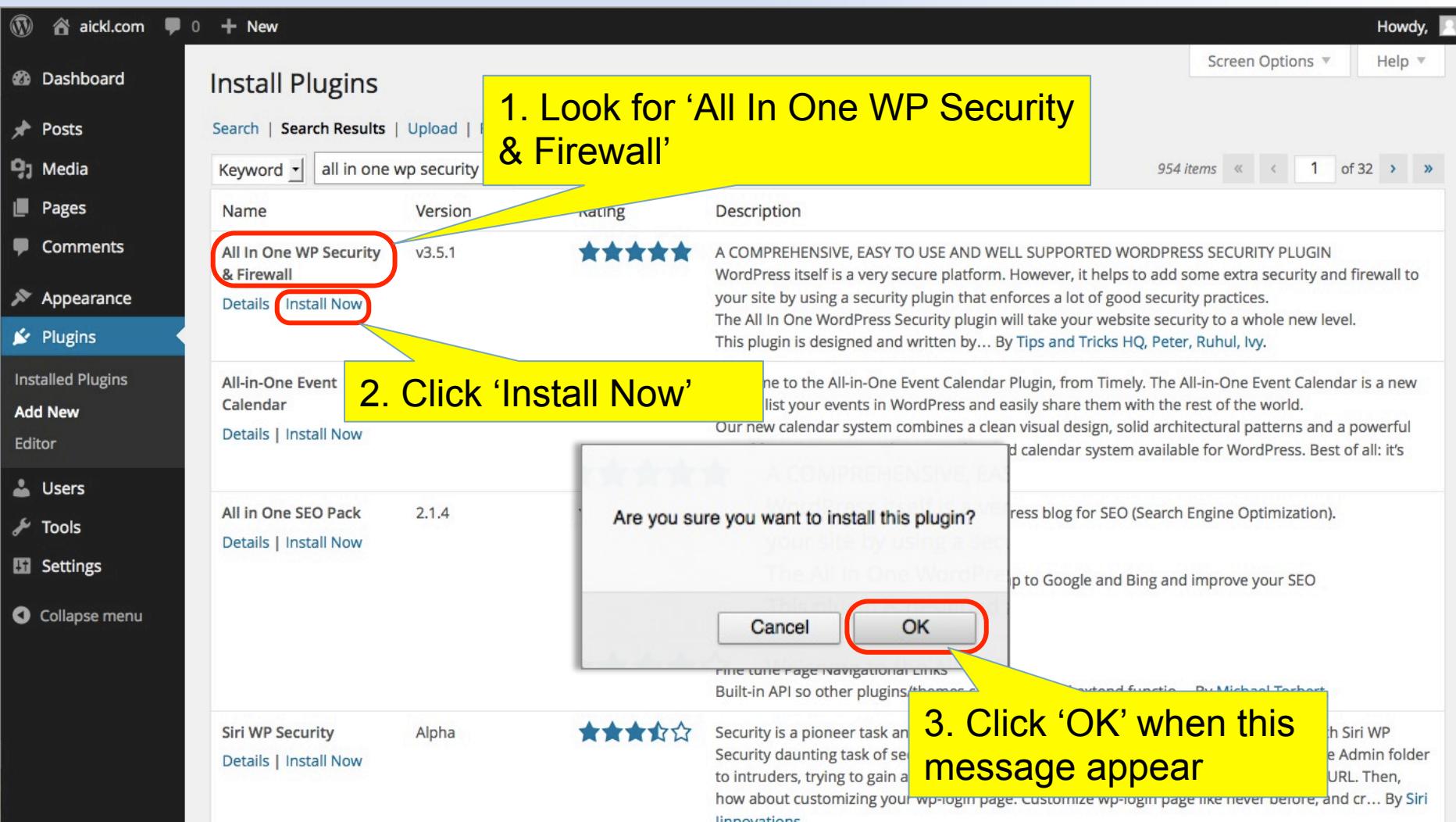
954 items < < 1 of 32 > >

Name	Version	Rating	Description
All In One WP Security & Firewall	v3.5.1		A COMPREHENSIVE, EASY TO USE AND WELL SUPPORTED WORDPRESS SECURITY PLUGIN WordPress itself is a very secure platform. However, it helps to add some extra security and firewall to your site by using a security plugin that enforces a lot of good security practices. The All In One WordPress Security plugin will take your website security to a whole new level. This plugin is designed and written by... By Tips and Tricks HQ , Peter, Ruhul, Ivy.
All-in-One Event Calendar			he to the All-in-One Event Calendar Plugin, from Timely. The All-in-One Event Calendar is a new list your events in WordPress and easily share them with the rest of the world. Our new calendar system combines a clean visual design, solid architectural patterns and a powerful d calendar system available for WordPress. Best of all: it's
All in One SEO Pack	2.1.4		ress blog for SEO (Search Engine Optimization). p to Google and Bing and improve your SEO
Siri WP Security	Alpha		Security is a pioneer task and a daunting task of securing your website from intruders, trying to gain access to your Admin folder via URL. Then, how about customizing your wp-login page. Customize wp-login page like never before, and cr... By Siri Innovations .

1. Look for 'All In One WP Security & Firewall'

2. Click 'Install Now'

3. Click 'OK' when this message appear



Howdy, 

aickl.com 0 + New

Dashboard Posts Media Pages Comments Appearance Plugins

Installed Plugins Add New Editor

Users Tools Settings

Collapse menu

Installing Plugin: All In One WP Security & Firewall v3.5.1

Downloading install package from <https://downloads.wordpress.org/plugin/all-in-one-wp-security-and-firewall.zip...>

Unpacking the package...

Installing the plugin...

Successfully installed the plugin All In One WP Security & Firewall v3.5.1.

[Activate Plugin](#) | [Return to Plugin Installer](#)

1. Click 'Activate Plugin'

Thank you for creating with WordPress.

Version 3.8.1

The screenshot shows the WP Security plugin dashboard. On the left sidebar, 'WP Security' is highlighted with a red box. The main area features a 'Security Strength Meter' with a needle pointing to 'Strength' and a value of '5'. Below it, a message says 'Total Achievable Points: 410' and 'Current Score of Your Site: 5'. To the right, there's a 'Critical Feature Status' section with four items: 'Admin Username' (ON), 'Login Lockdown' (ON), 'File Permission' (ON), and 'Basic Firewall' (ON). A large yellow callout box points to the 'Admin Username' button with the text '2. This meter displays your current WordPress security strength'. Another yellow callout box points to the 'ON' button for 'Admin Username' with the text '4. Click on the 'ON' button'. A third yellow callout box points to the 'Admin Username' section with the text '3. Work on these four items first, starting with 'Admin Username''. The top right corner of the dashboard shows 'Howdy, [Profile Picture]'.

2. This meter displays your current WordPress security strength

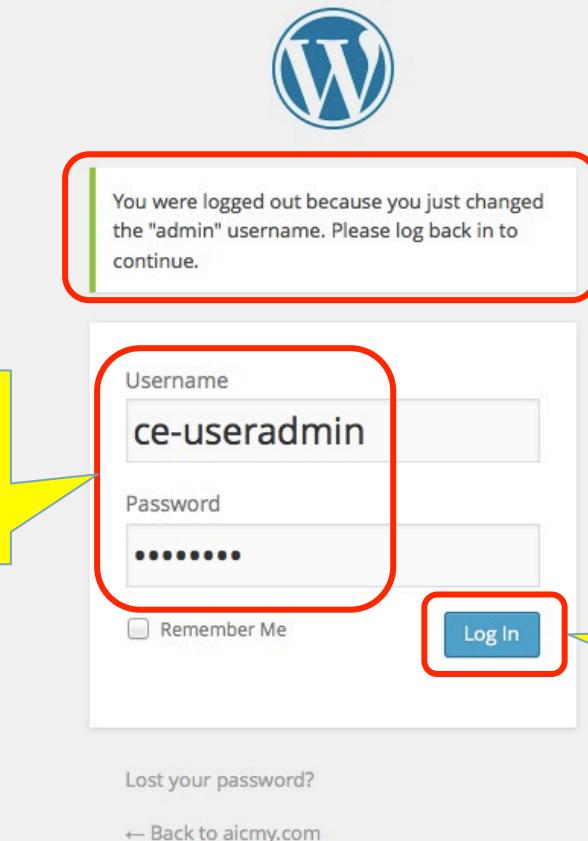
4. Click on the 'ON' button

3. Work on these four items first, starting with 'Admin Username'

1. This is your current admin username

2. Key in your new admin username here, eg: 'ce-useradmin'

3. Click on 'Change Username' button to proceed



2. Login again using
your NEW username
and existing password

1. You will be logged out
from WordPress admin
area

3. Click 'Log In'
button to proceed

The screenshot shows the WordPress dashboard with a sidebar on the left containing various menu items: Dashboard, Posts, Media, Links, Pages, Comments, Appearance, Plugins (with 1 update), Users (highlighted with a red box), All Users, Add New, Your Profile (highlighted with a red box), Tools, Settings, WP Security, and Collapse menu.

The main content area shows a 'New Password' form. It includes fields for 'New Password' and 'Repeat New Password', both of which are highlighted with red boxes. A note above the fields says, 'If you would like to change the password type a new one. Otherwise leave this blank.' Below the fields, a green bar indicates the password strength as 'Strong'. A hint box provides guidance: 'Hint: The password should be at least seven characters long. To make it stronger, use upper and lower case letters, numbers and symbols like ! ? \$ % ^ &).'

Yellow callout boxes with black text provide the following instructions:

1. Next, ensure you have a **STRONG** password. To change your existing password, go to 'Users' then click on 'Your Profile' on the left hand menu
2. Key in your new password twice here
3. Use this guideline to create a strong password
4. Click 'Update Profile' to proceed

Howdy, ce-useradmin

Dashboard Posts Media Links Pages Comments Appearance Plugins 1 Users Tools Settings WP Security

1. Click 'WP Security' on the left hand menu to go back to its settings

Dashboard System Info

For information, updates and documentation, please visit the [AIO WP Security & Firewall Plugin Page](#)
[Follow us](#) on Twitter, Google+ or via Email to stay up to date about the new security features of this plugin.

Security Strength Meter

Security Points Breakdown

Critical Feature Status

Below is the current status of the critical features that you should activate on your site to achieve a minimum level of recommended security

Admin Username	ON	OFF
Login Lockdown	ON	OFF
File Permission	ON	OFF
Basic Firewall	ON	OFF

Last 5 Logins

Last 5 logins summary:

User	Date	IP
ce-useradmin	2014-02-22 09:13:41	223.27.129.66

Maintenance Mode Status

Maintenance mode is currently off.

Logged In Users

Maintainence mode is currently off.

2. Click 'ON' for 'Login Lockdown'

One of the ways hackers try to compromise sites is via a **Brute Force Login Attack**. This is where attackers use repeated login attempts until they guess the password. Apart from choosing strong passwords, monitoring and blocking IP addresses which are involved in repeated login failures in a short period of time is a very effective way to stop these types of attacks. You may also want to checkout our [Cookie-Based Brute Force Login Prevention](#) feature for another secure way to protect against these types of attacks.

Login Lockdown Options

Basic 0/20

Enable Login Lockdown Feature: Check this if you want to enable the login lockdown feature and apply the settings below

Allow Unlock Requests: Check this if you want to allow users to generate an automated unlock request link which will unlock their account

Max Login Attempts: 3 Set the value for the maximum login retries before IP address is locked out

Login Retry Time Period (min): 5 If the maximum number of failed login attempts for a particular IP address occur within this time period the plugin will lock out that address

Time Length of Lockout (min): 60 Set the length of time for which a particular IP address will be prevented from logging in

Display Generic Error Message: Check this if you want to show a generic error message when a login attempt fails

Instantly Lockout Invalid Usernames: Check this if you want to instantly lockout login attempts with usernames which do not exist on your system

Notify By Email: One has been locked out due to maximum failed login attempts
Email address

Save Settings



User Registration Settings

Manually Approve New Registrations

If your site allows people to create their own accounts via the WordPress registration form, then you can minimize SPAM or bogus registrations by manually approving each registration. This feature will automatically set a newly registered account to "pending" until the administrator activates it. Therefore undesirable registrants will be unable to log in without your express approval. You can view all accounts which have been newly registered via the handy table below and you can also perform bulk activation/deactivation/deletion tasks on each account.

Enable manual approval of new registrations: Check this if you want to automatically disable all newly registered accounts so that you can approve them manually.

Save Settings

Approve Registered Users

Bulk Actions ▾ Apply

Name	Email	Register Date	Account Status

1. Click 'User Registration' on the left hand menu

2. Check this box

3. Click 'Save Settings'

The screenshot shows the WIA dashboard with the 'Database Security' menu item highlighted. The main content area displays the 'Change Database Prefix' plugin settings. A yellow box highlights the 'Change DB Prefix' button. Another yellow box highlights the checkbox for generating a random prefix. A third yellow box highlights the success message at the bottom.

1. Click 'Database Security' on the left hand menu
2. Check this box
3. Click 'Change DB Prefix'
4. You will see this message once the change has been completed

Your WordPress DB is the most important asset of your website because it contains a lot of your site's precious information. The DB is also a target for hackers via methods such as SQL injections and malicious and automated code which targets certain tables. One way to add a layer of protection for your DB is to change the default WordPress table prefix from "wp_" to something else which will be difficult for hackers to guess. This feature allows you to easily change the prefix to a value of your choice or to a random value set by this plugin.

Change Database Prefix

Table Prefix: wp_ Your site's prefix Check this if you want the plugin to generate a random 6 character string for the table prefix OR Choose your own DB prefix by specifying a string which contains letters and/or numbers and/or underscores. Example: xyz.

Starting DB prefix change operation... Your WordPress system has a total of 15 tables. A backup copy of your wp-config.php file was created successfully! 15 tables had their prefix updated successfully! wp-config.php file was updated successfully! The options table records which had references to the old DB prefix were updated successfully! The usermeta table records which had references to the old DB prefix were updated successfully! DB prefix change tasks have been completed.

Howdy, ce-useradmin

Dashboard Posts Media Links Pages Comments Appearance Plugins 1 Users Tools Settings WP Security

File Permissions PHP File Editing WP File Access Host System Logs

File Permissions Scan

Your WordPress file and folder permission settings. Your WP installation already comes with reasonably. However, sometimes people or other plugins modify. This feature will scan the critical WP core folders and

WP Directory and File Permissions Scan Result

Basic 20/20

Name	File/Folder	Current Permissions	Recommended	Recommended Action
root directory	/home/jefftang/public_html/test/	0755	0755	No Action Required
wp-includes/	/home/jefftang/public_html/test/wp-includes	0755	0755	No Action Required
.htaccess	/home/jefftang/public_html/test/.htaccess	0	0644	Set Recommended Permissions
wp-admin	test/wp-admin/index.php	0644	0644	No Action Required
wp-admin	test/wp-admin/js/	0755	0755	No Action Required
wp-con	test/wp-content/themes	0755	0755	No Action Required
wp-admin	test/wp-content/plugins	0755	0755	No Action Required
wp-admin	test/wp-admin	0755	0755	No Action Required
wp-content/	/home/jefftang/public_html/test/wp-content	0755	0755	No Action Required
wp-config.php	/home/jefftang/public_html/test/wp-config.php	0644	0644	No Action Required
Name	File/Folder	Current Permissions	Recommended Permissions	Recommended Action

1. Click 'Filesystem Security' on the left hand menu

2. Check that every file permission indicates 'No Action Required'. Else, click 'Set Recommended Permissions' to set the recommended permissions

The screenshot shows the 'WP Security' plugin settings page for a WordPress site. The left sidebar lists various security features like Dashboard, Settings, User Accounts, etc. The main area shows the 'WP File Access' tab selected. A yellow callout box points to the 'WP File Access' tab with the instruction: '1. Click on 'WP File Access''. Another yellow callout box points to the 'Prevent Access to Default WP Files' section with the instruction: '2. Check this box'. A third yellow callout box points to the 'Save Setting' button with the instruction: '3. Click 'Save Setting''. A red box highlights the 'WP File Access' tab, another red box highlights the checkbox in the 'Prevent Access to WP Default Install Files' section, and a third red box highlights the 'Save Setting' button.

1. Click on 'WP File Access'

2. Check this box

3. Click 'Save Setting'



The screenshot shows the 'Firewall' settings page in the WIA admin interface. A sidebar on the left lists various security modules, with 'Firewall' highlighted by a red box. The main content area has tabs for 'Basic Firewall Rules', 'Additional Firewall Rules', '5G Blacklist Firewall Rules', and 'Internet Bots'. The 'Basic Firewall Rules' tab is active. It displays 'Firewall Settings' with a note about activating basic firewall security via .htaccess rules. Below this is the 'Basic Firewall Settings' section, which includes a 'Basic' tab (selected) and a 'Pingback Protection' tab. Under 'Basic', there's a checkbox labeled 'Check this if you want to apply basic firewall protection to your site.' Under 'Pingback Protection', there's a checkbox labeled 'Check this if you are not using the WP XML-RPC functionality and you want to enable protection against WordPress pingback vulnerabilities.' Both checkboxes are checked. A large yellow box contains four numbered steps: 1. Click 'Firewall' on the left hand menu; 2. Check this box (pointing to the first checkbox); 3. Check this box (pointing to the second checkbox); and 4. Click on 'Save Basic Firewall Settings' (pointing to the blue button at the bottom).

1. Click 'Firewall' on the left hand menu
2. Check this box
3. Check this box
4. Click on 'Save Basic Firewall Settings'

WIA World Internet Acad
World Class Internet Marketing T

www.imarketing.courses

1. Click 'Additional Firewall Rules'

2. Check this box

3. Check this box

4. Check this box

5. Check this box

6. Check this box

7. Click 'Save Additional Firewall Settings'

Basic Firewall Rules Additional Firewall Rules SG Blacklist Firewall Rules Internet Bots

Additional Firewall Rule Creation

Enable advanced firewall settings to your site.
via the insertion of special code to your currently active .htaccess file.
erred to the .htaccess file, this feature may break some functionality for certain plugins and you are

Intermediate 0/5

Disable Index Views: Check this if you want to disable directory and file listing. + More Info

Advanced 0/10

Disable Trace and Track: Check this if you want to disable trace and track. + More Info

Advanced 0/10

Forbid Proxy Comment Posting: Check this if you want to forbid proxy comment posting. + More Info

Advanced 0/15

Deny Bad Query Strings: This will help protect you against malicious queries via XSS. + More Info

Advanced 0/15

Enable Advanced Character String Filter: This will block bad character matches from XSS. + More Info

Save Additional Firewall Settings



EST.

imarketing.courses
BEST PLACE TO LEARN!

2021

The screenshot shows the WordPress dashboard with the URL `aicmy.com` in the address bar. The left sidebar has a dark theme with various menu items: Dashboard, Posts, Media, Links, Pages, Comments, Appearance, Plugins (with 1 notification), Users, Tools, Settings, and WP Security (which is currently selected). The main content area shows the 'WP Security' plugin's 'Firewall Settings' page. At the top, there are tabs: Basic Firewall Rules, Additional Firewall Rules, **5G Blacklist Firewall Rules** (which is highlighted with a red box and has a yellow callout pointing to it), and Internet Bots. The '5G Blacklist Firewall Rules' section contains the following text:

This feature allows you to activate the 5G firewall security protection rule.

The 5G Blacklist is a simple, flexible blacklist that helps reduce the number of malicious URL requests that hit your website.

The added advantage of applying the 5G firewall to your site is that it has been tested and confirmed by the people at PerishablePress.com to be an optimal and least disruptive way to protect your site from malicious traffic.

Therefore the 5G firewall rules should not have any impact on your site's general functionality but if you wish you can take a [backup](#) of your .htaccess file before proceeding.

Below this, the '5G Blacklist/Firewall Settings' section includes:

Advanced | **0/20**

Enable 5G Firewall Protection: Check this if you want to apply the 5G Blacklist firewall protection from perishablepress.com to your site. [+ More Info](#)

Save 5G Firewall Settings

Three yellow callouts with arrows point to specific actions:

1. Click '5G Blacklist Firewall Rules'
2. Check this box
3. Click 'Save 5G Firewall Settings'

1. Click 'Internet Bots'

Internet Bot Settings

What is an Internet Bot?

A bot is a piece of software which runs on the Internet and performs automatic tasks. For example when Google indexes your pages it uses automatic bots to achieve this task.

A lot of bots are legitimate and non-malicious but not all bots are good and often you will find some which try to impersonate legitimate bots such as "Googlebot" but in reality they

Although most of the bots out there are relatively harmless sometimes website owners want to have more control over which bots they allow into their site.

This feature allows you to block bots which are impersonating as a Googlebot but actually aren't. (In other words they are fake Google bots)

Googlebots have a unique identity which cannot easily be forged and this feature will identify any fake Google bots and block them from reading your site's pages.

Attention: Sometimes non-malicious Internet organizations might have bots which impersonate as a "Googlebot".

Just be aware that if you activate this feature the plugin will block all bots which use the "Googlebot" string in their User Agent information but are NOT officially from Google (irrespective of the organization).

All other bots from other organizations such as "Yahoo", "Bing" etc will not be affected by this feature.

Block Fake Googlebots

Advanced 0/5

Block Fake Googlebots: Check this if you want to block all fake Googlebots. + More Info

Save Internet Bot Settings

The screenshot shows the 'Rename Login Page' tab selected in the WIA WordPress plugin settings. The page contains the following text:

An effective Brute Force prevention technique is to change the default WordPress login page URL. Normally if you wanted to login to WordPress you would type your site's home URL followed by wp-login.php. This feature allows you to change the login URL by setting your own slug and renaming the last portion of the login URL which contains the wp-login.php to any string that you like. By doing this, malicious bots and hackers will not be able to access your login page because they will not know the correct login page URL.

You may also be interested in the following alternative brute force prevention features:

1. Click 'Brute Force' on the left hand menu

2. Check this box

3. Fill this box with some text such as 'userlogin-admin', this changes the admin login URL from 'yourdomain.com/wp-admin' to 'yourdomain.com/userlogin-admin'

4. Click 'Save Settings'

The screenshot shows the WIA dashboard with the 'WP Security' menu item highlighted. The main content area displays 'Comment SPAM Settings' and 'Comment SPAM IP Monitoring' tabs. Under 'Comment SPAM Settings', there is a section titled 'Add Captcha To Comments Form' with a note about reducing SPAM comments. Below it, under 'Enable Captcha On Comment Forms:', there is a checkbox labeled 'Check this if you want to insert a captcha field on the comment forms'. A yellow callout bubble points to this checkbox with the text '2. Check this box'. Another yellow callout bubble points to the 'Save Settings' button at the bottom of the page with the text '4. Click \'Save Settings\''. The left sidebar lists various security features, with 'SPAM Prevention' also highlighted by a red box.

1. Click 'SPAM Protection' on the left hand menu
2. Check this box
3. Check this box
4. Click 'Save Settings'

Howdy, ce-useradmin

Dashboard System Info

For information, update Follow us on Twitter, G

2. By now your security strength should be around 245

Security Strength Meter

Total Achievable Points: 410 Current Score of Your Site: 245

Security Points Breakdown

Critical Feature Status

Below is the current status of the critical features you should activate on your site to achieve the minimum level of recommended security.

Admin Username	ON	OFF
Login Lockdown	ON	OFF
File Permission	ON	OFF
Basic Firewall	ON	OFF

3. Notice also all settings here should be 'ON' by now

Last 5 Logins

Last 5 logins summary:

User	Date	IP
ce-useradmin	2014-02-22 09:13:41	223.27.129.66

Maintenance Mode Status

Maintenance mode is currently off.

Maintenance Mode

ON	OFF
----	-----

1. Go back to 'Dashboard' on the left hand menu

Dashboard Settings

User Accounts User Login User Registration Database Security Filesystem Security WHOIS Lookup Blacklist Manager Firewall Brute Force SPAM Prevention Scanner Maintenance

Rename Login Page

The [Rename Login Page](#) feature is currently active. Your new WordPress login URL is now: <http://aicmy.com/test/?userlogin-admin>

Logged In Users

There are no other users currently logged in.

Questions?