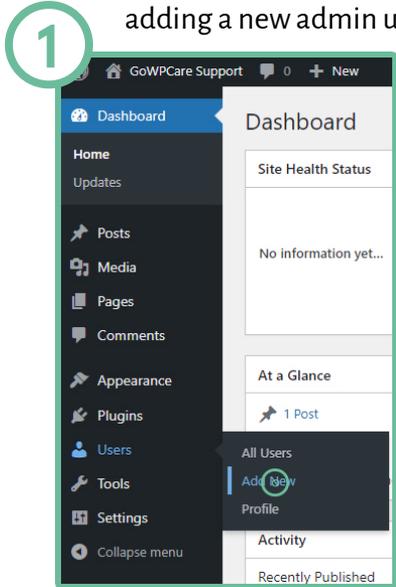


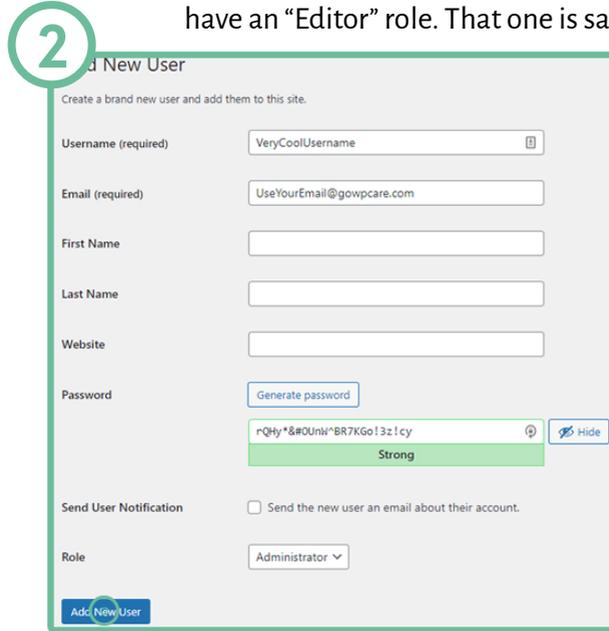
Please follow these instructions as they go. This is more than a usual checklist.
Note that in case your site is already hacked, it's already late to do these steps. Get in touch with us.

1 Let us start with switching admin username and giving it a good password.

1) Login to your dashboard, and then hover over users so you can click under "Add New" - what we are doing here is adding a new admin user



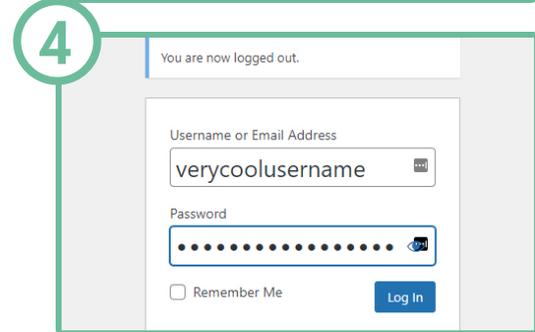
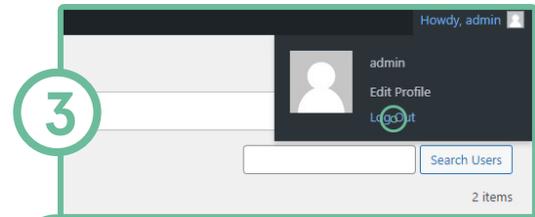
2.1) Make sure you create a good username. Don't use your First or Last Name. In case you wish to publish articles under your name, the easiest and safest way would be to create a user which will have an "Editor" role. That one is safe.



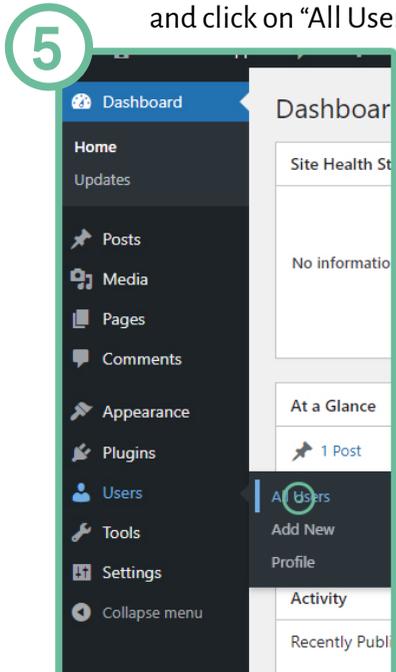
2.2) Password is all here. Make sure it is good and strong as you see in the picture. You won't remember it, but most of the browsers support saving.

2.3) Select Administrator Role and click "Add a user".

3) Log Out, so you can log in using your new username (4)

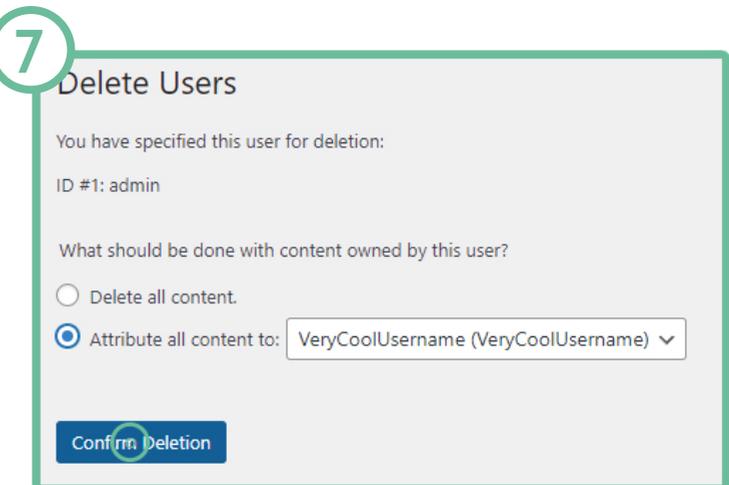
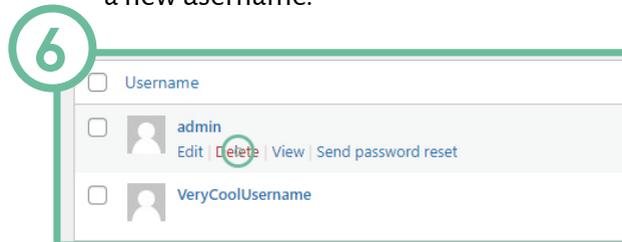


5) Hover over "Users" and click on "All Users"



6) Remove "admin" username

7) This will save your current content under a new username.



*! Of course, update passwords for all admin accounts to something secure.

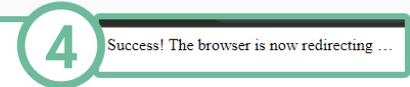
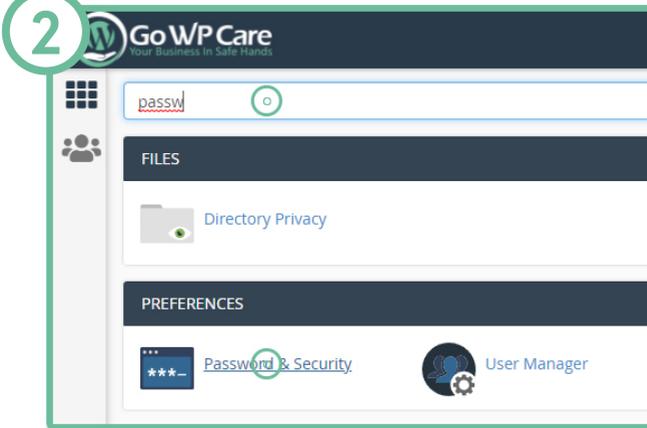
2

Other Passwords. If you are reading this, you are probably on a shared hosting plan with a large hosting company that runs on WHM/cPanel. We will use it as an example.

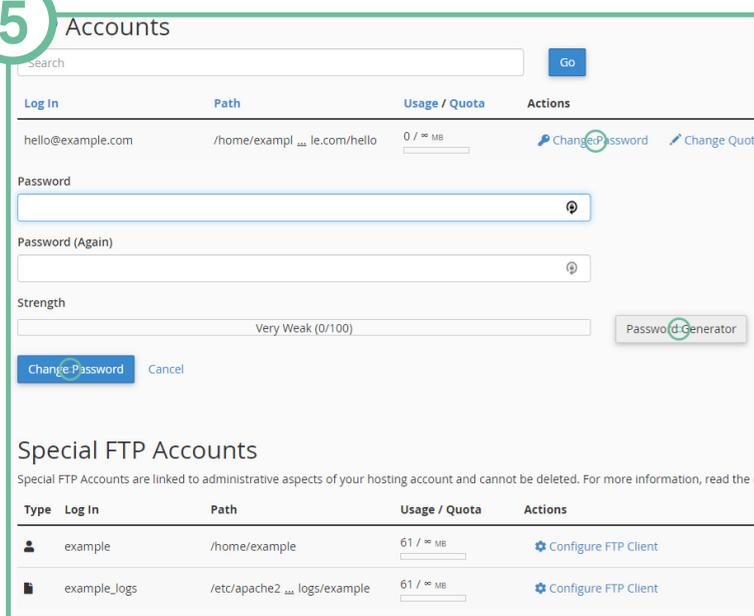
1) cPanel Password Login to your cPanel

2) In the search field, type “password” and click on “Password & Security”

3) Make sure your password is very strong
4) Once you hit change, you will be redirected to login page



5



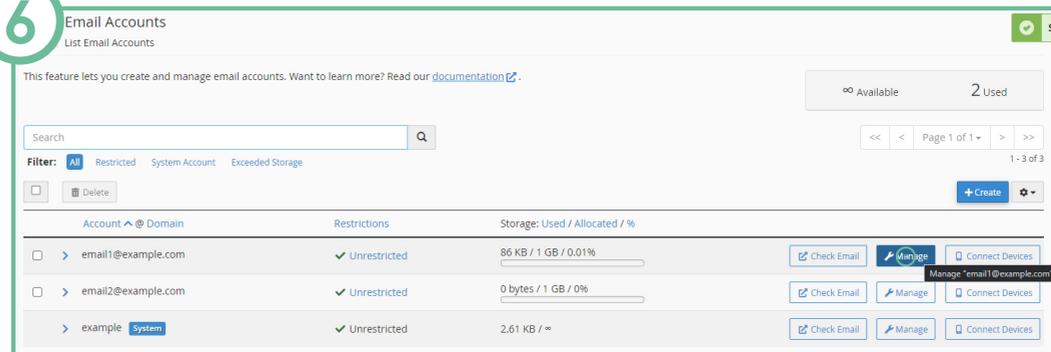
FTP Passwords

5) In search field (3) type FTP and open “FTP Accounts”. Clicking on “Change Password” will pop options to update the password. Again, 100% strong and Click “Change Password”

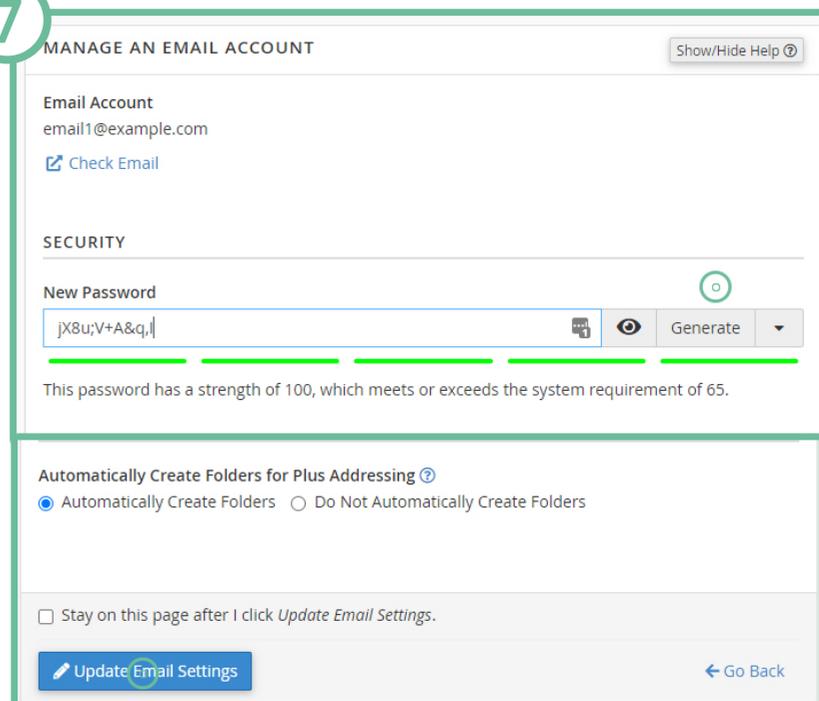
Email passwords

6) In search field (2) type “Email Accounts” open and click on “Manage”
7) Make a 100% strong one and click “Update Email Settings” - need to scroll down

6



7



You might be asking why email accounts? Short answer, if your email gets compromised and you have cPanel account bound to it, hackers can easily request “Forgot password” and get ahold of your cPanel account. When they have access to it, then nothing is safe.

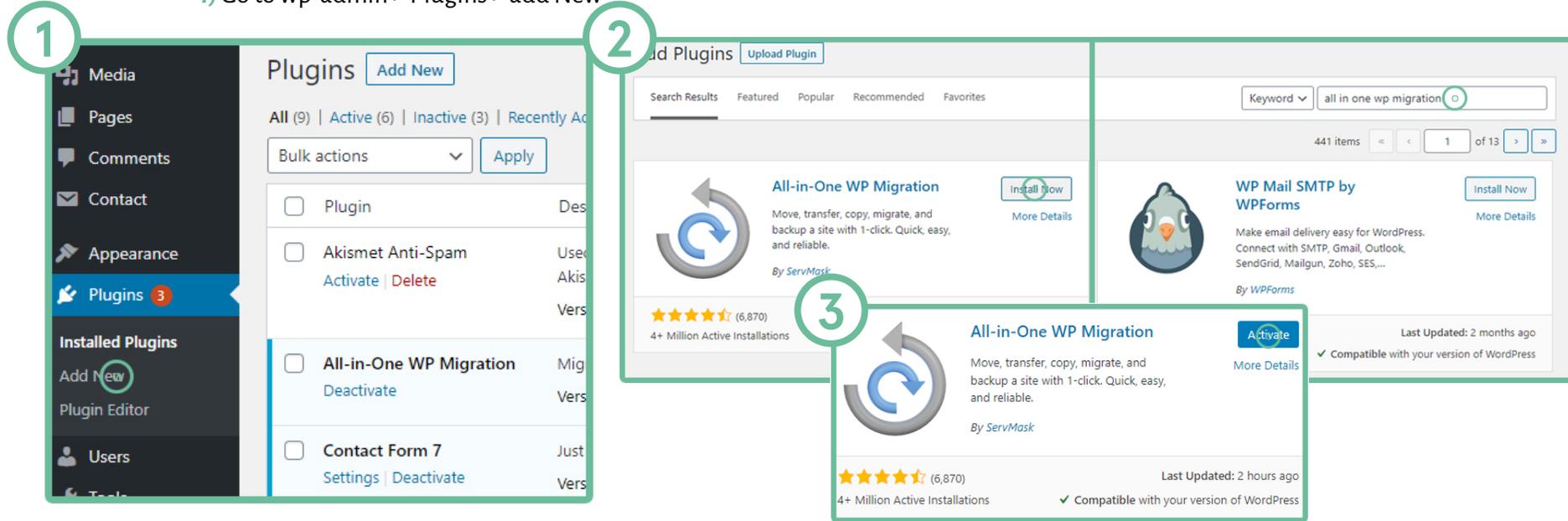
3

○ Before we continue with updates, we must make backups in case something goes bad. While there are many backup options, we prefer two of them. The first is All-in-One WP Migration and the second is UpdraftPlus. For this case, we will use All in One. What is good about All in One is that it takes care of everything at once. It's a backup solution you would use when you make a backup that will last. So if your site doesn't have any updates (blog posts, products, etc) on a daily or weekly basis, this one is good. The downside is maybe you will need a paid version, but it's worth it if you are doing it all by yourself.

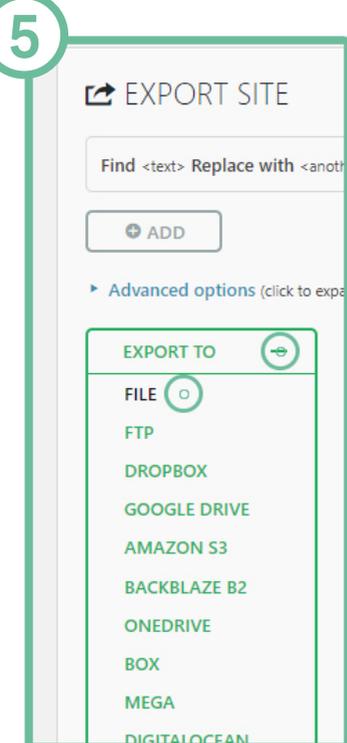
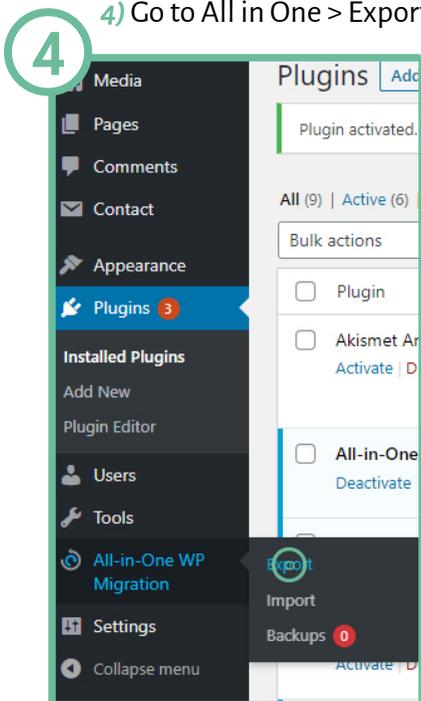
We are going to install a plugin

1) Go to wp-admin > Plugins > add New

2) Search for all in one wp migration Click "install now" > Click "Activate" (3)

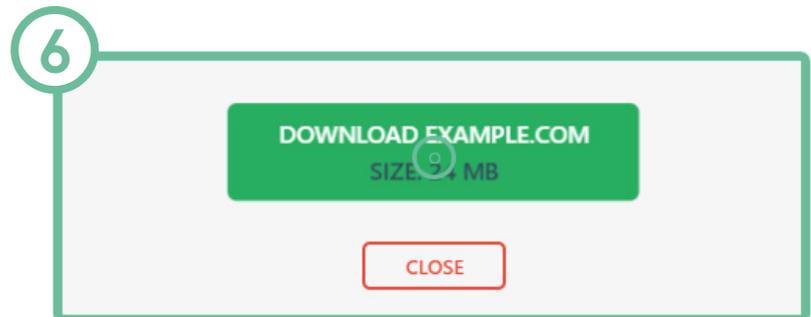


4) Go to All in One > Export



5) Click Export To > File

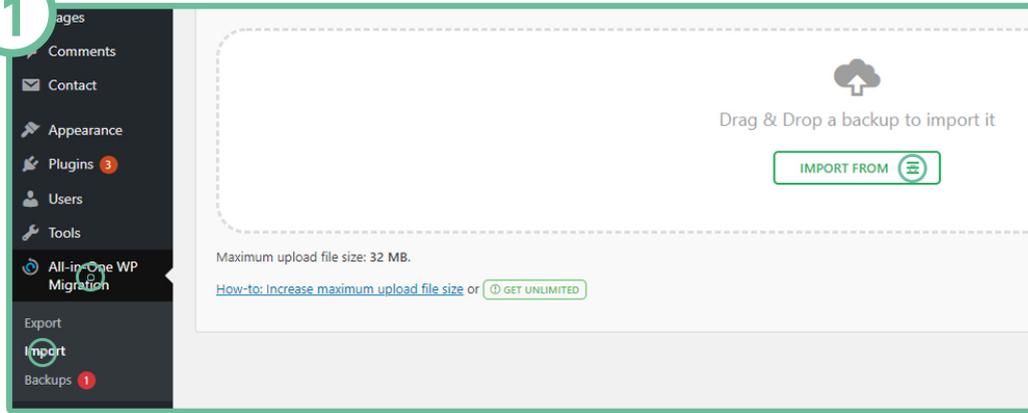
6) Once completed, click Download



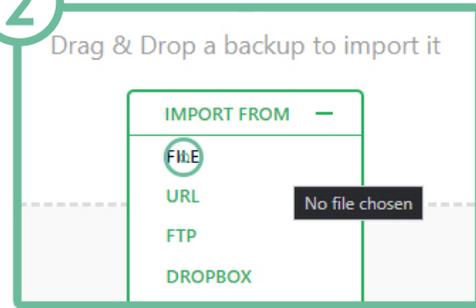
And that's how it works. On paid version you can restore a backup from the server, but on free we have to export/import.

Next is how:

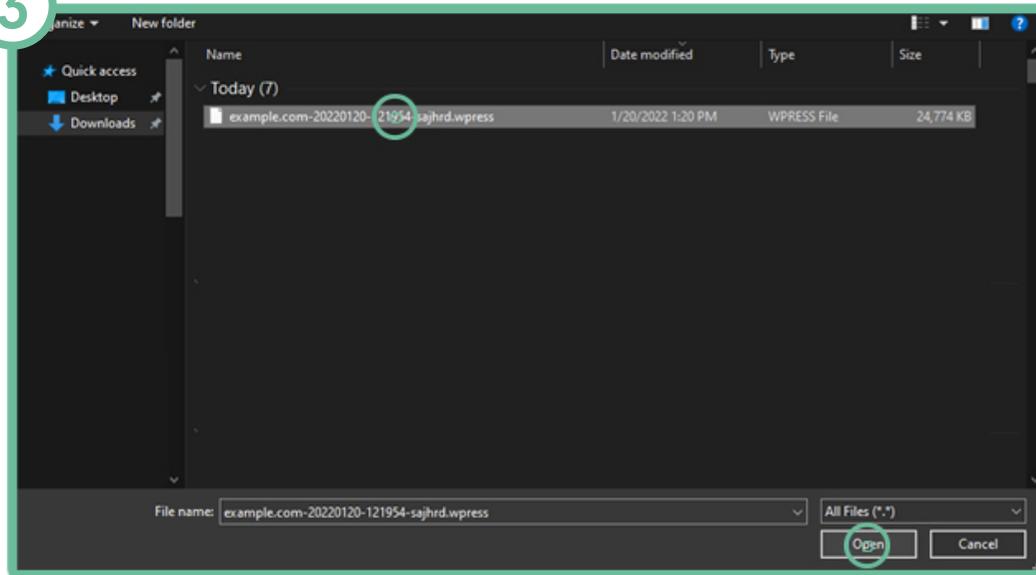
1) Go to All in One > Import > Click “Import from” so the dropdown will pop



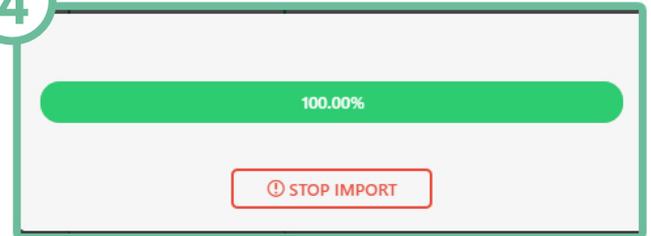
2) Select “File”



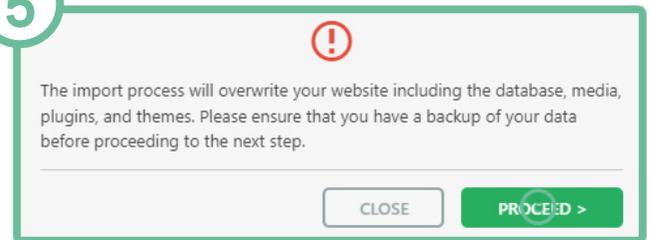
3) Find the file in your saved folder from previous steps. Click “Open”



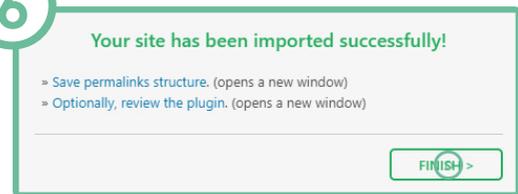
4) Wait for the upload to complete



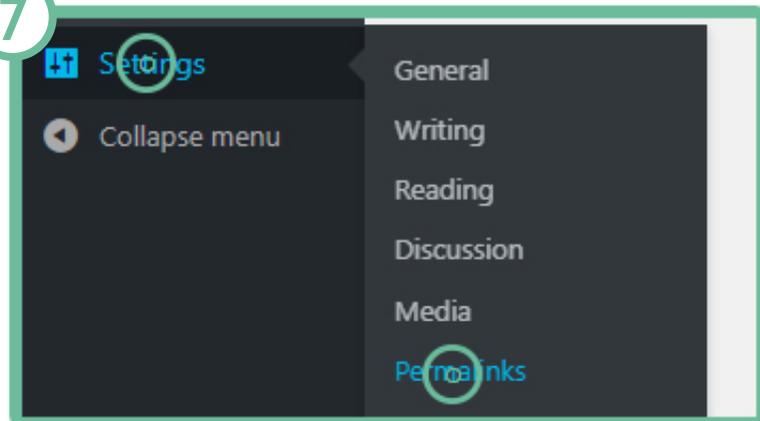
5) Click “Proceed”



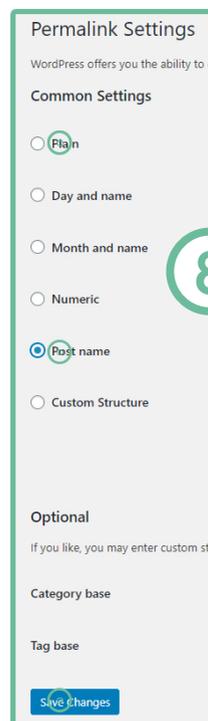
6) Click “Finish”



7) When it's done, on any backup, import/export it is recommended to update permalinks. Click on Settings in WP-Admin > Permalinks



8) Say your original was “Plain”, what you would do is click on “Post Name”, Click on “Post Name”, click “Save” and then go back, once the page is refreshed, click “Plain” and click “Save”. You are all done!

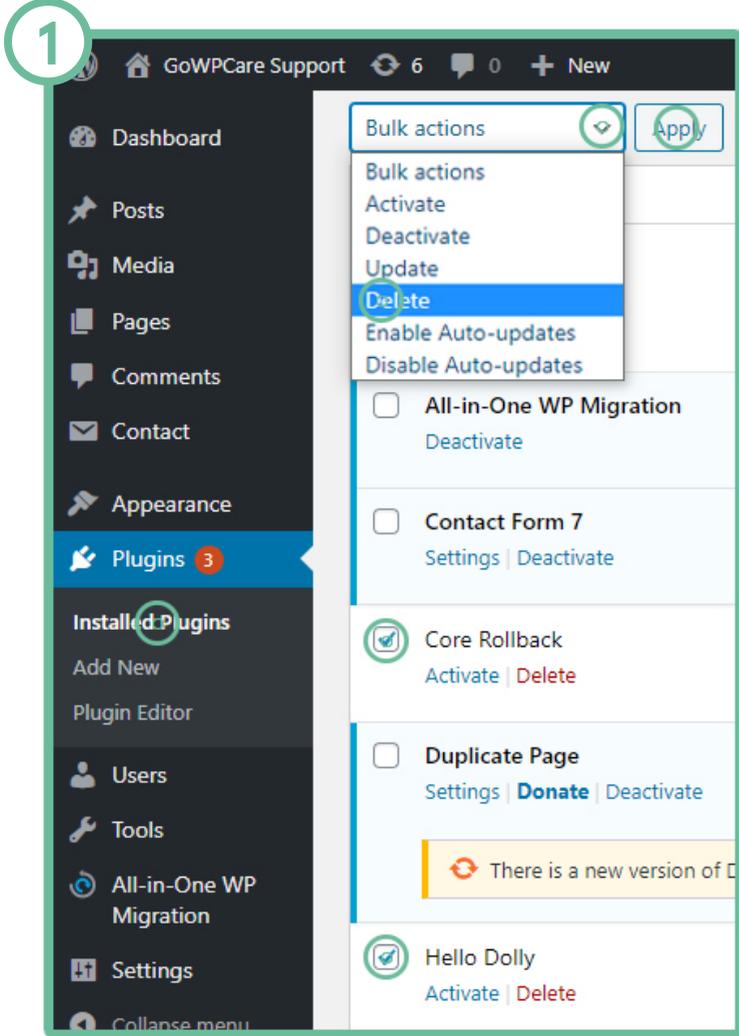


4

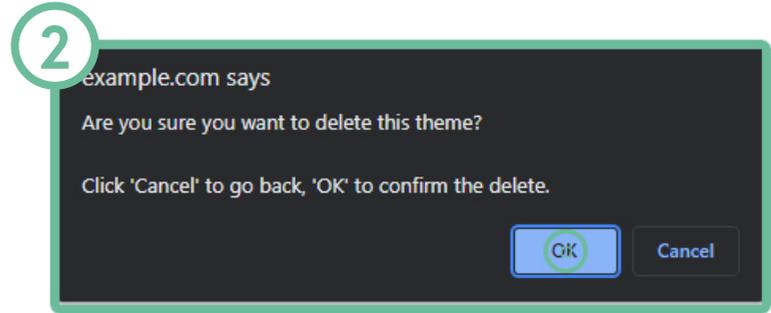
Now we can safely proceed to updates.

Let us start with removing unused plugins and themes first.

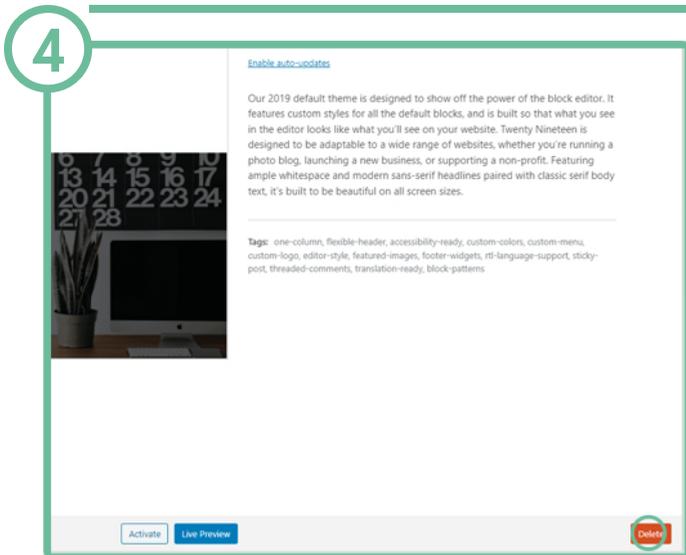
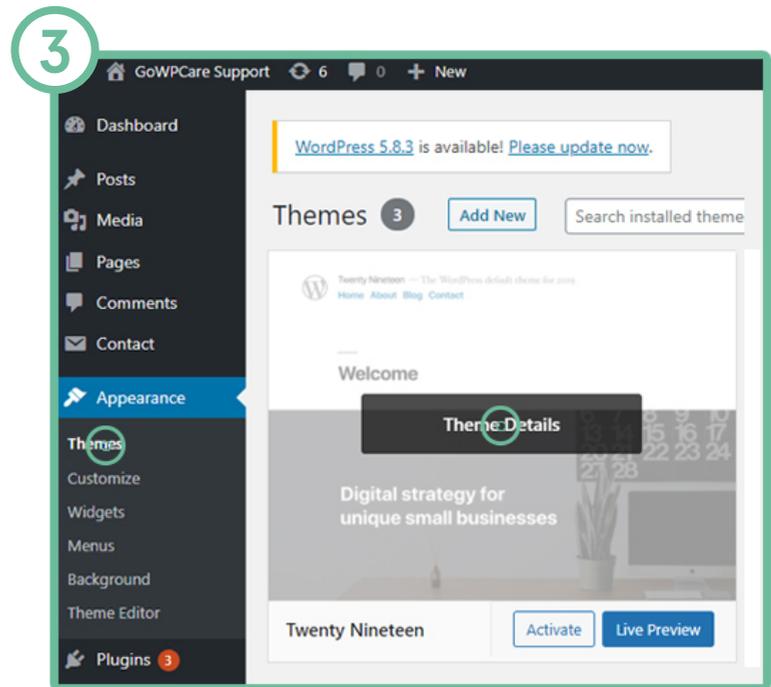
- 1) Go to WP-Admin > Plugins > Installed plugins
Checkmark all the ones that are not in use.
From the dropdown select “Delete” and hit “Apply”



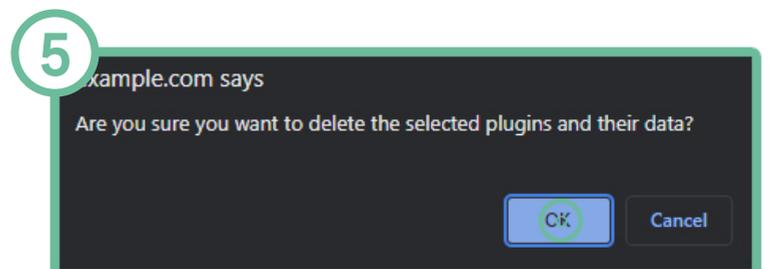
- 2) a pop up will display confirmation, click “OK”.



- 3) Go to Appearance > Themes and click on “Theme Details” on a theme that is not in use.

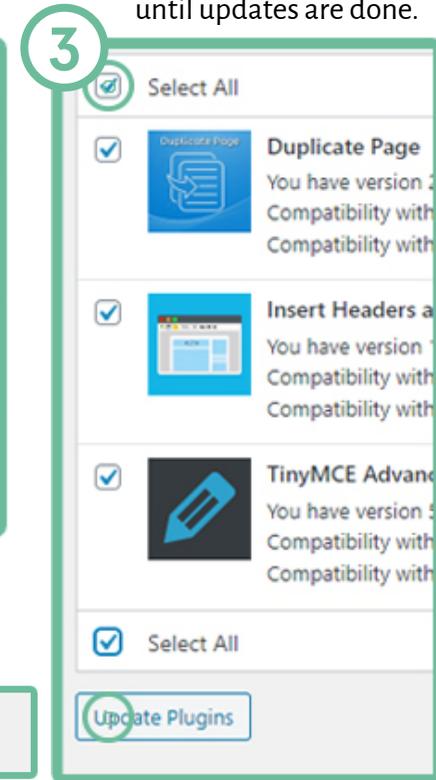
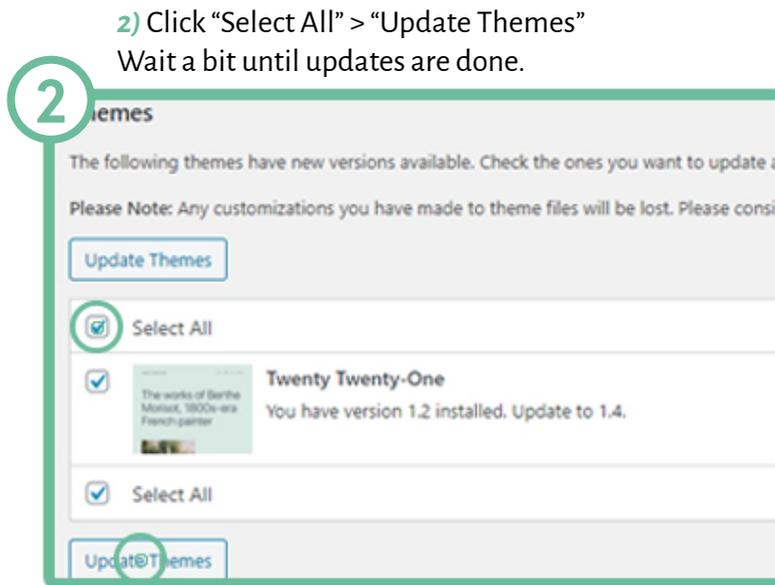
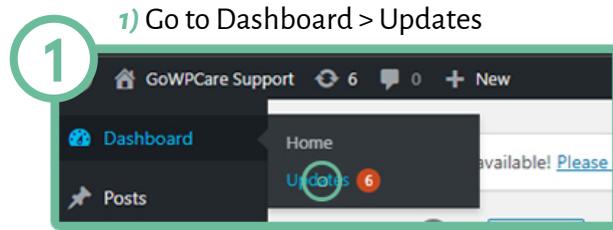


- 4) In the bottom of the popped screen you will see a red “delete” button. Click it and another confirmation popup will appear (5), click “OK”. Repeat for all extra ones.



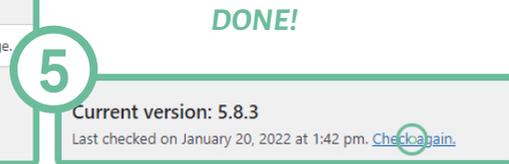
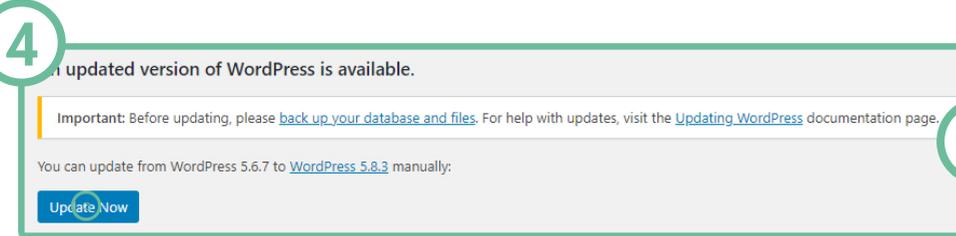
5 We always recommend updating themes and plugins before updating core. Simply because we saw a lot of outdated plugins on clients' sites.

3) Go back to updates **(1)** and this time click “Select All” > “Update Plugins”. Wait a bit until updates are done.



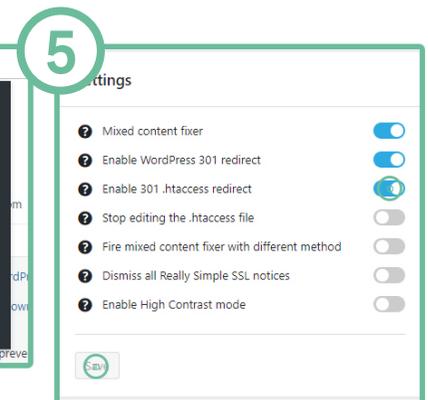
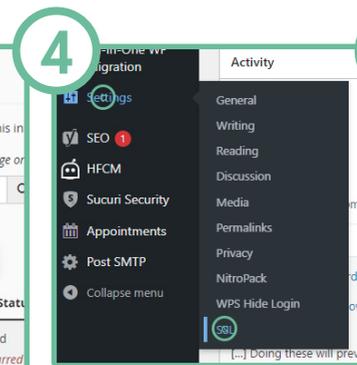
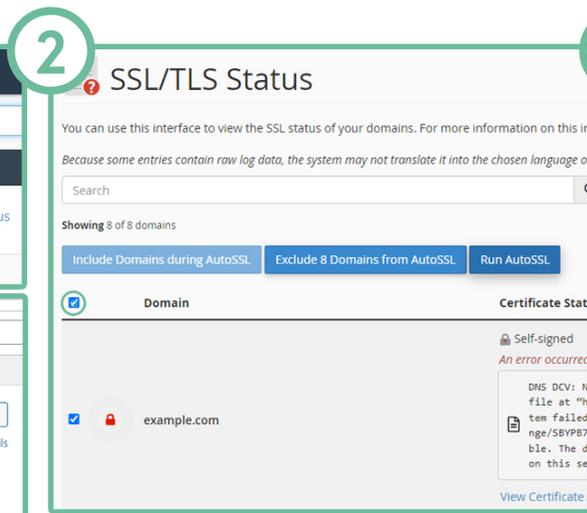
Time for Core WP update.

4) Go to Updates **(1)** > Click “Update Now”. Once completed, go back to **(1)** and hit “Check again” **(5)**. This will re-check any updates that were not available in your previous WP version. If needed, update again.



5 SSL instalation. In most cases, you will already have SSL installed. If not, follow these steps.

- 1)** Go to your cPanel account > Search > SSL/TLS Status.
- 2)** Click on the checkbox next to “Domain” to select everything and click “Run AutoSSL”.
- 3)** Go to your WordPress dashboard Plugins > Add New and search for “SSL” Plugin called “Really Simple SSL” will pop. Install and activate it.
- 4)** Go to Settings > SSL
- 5)** Apply to enable redirect in .htaccess file and hit save.

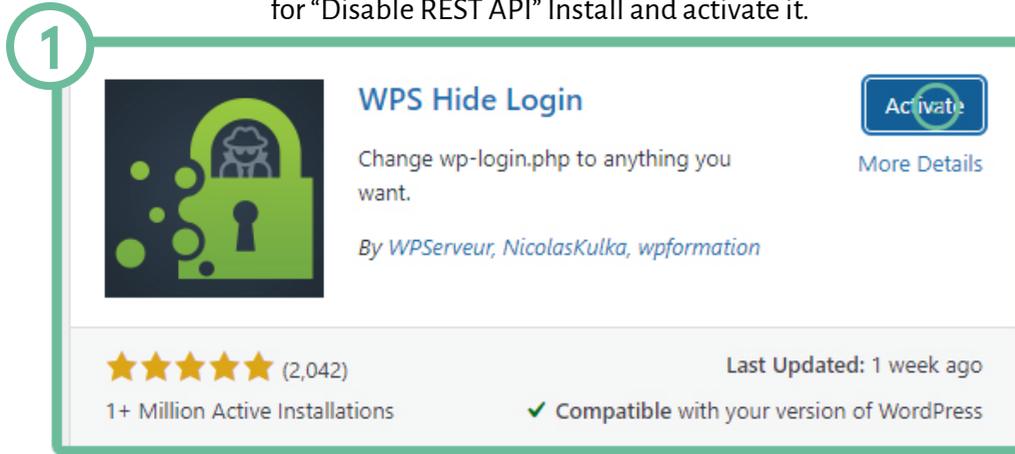


In some cases, you would need a paid certificate. Unless you are a really big ecom site, there is no need for it. If you do need it, contact your hosting provider.

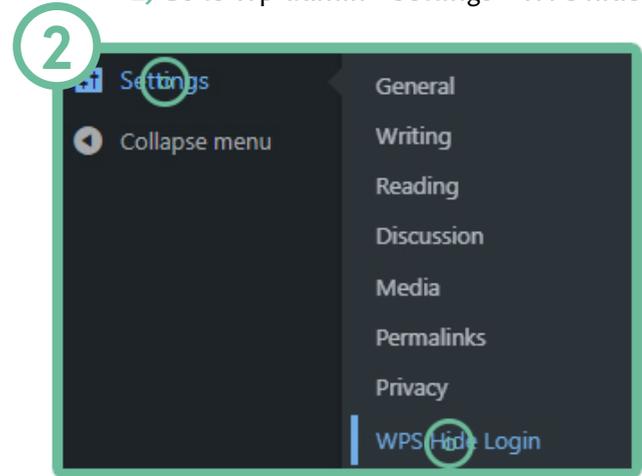
7

Updating wp-admin login URL

1) Go to wp-admin > Plugins > Add New and search for “Disable REST API” Install and activate it.



2) Go to Wp-admin > Settings > WPS hide login

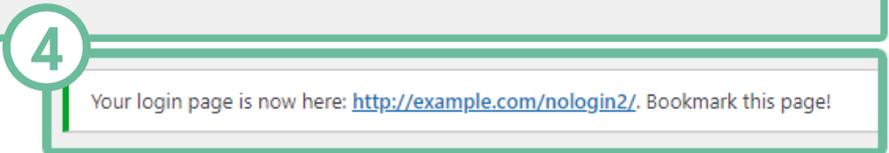
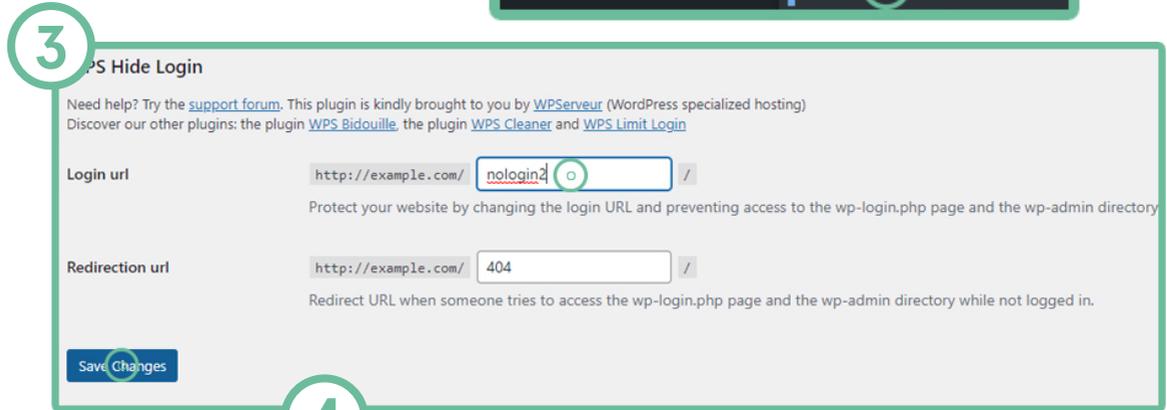


3) When you scroll all the way down, you will see these options.

Make sure your new url is not something like login, or admin or something, but use a good one.

4) Once you hit save, it will tell you new login and advice you to bookmark your new URL.

Obviously now, you would need to remove visible login links from the theme.



8

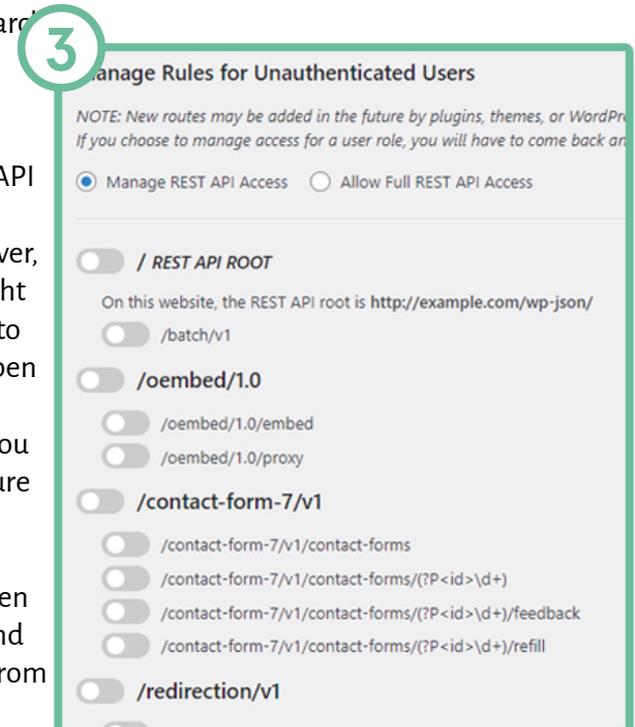
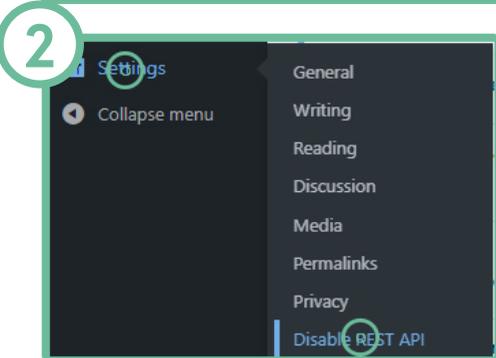
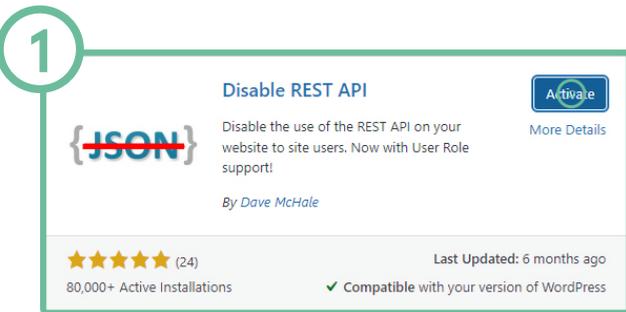
Disabling the REST API on WordPress

1) Go to wp-admin > Plugins > Add New and search for “Disable REST API” Install and activate it.

2) Go to Wp-admin > Settings > Disable REST API

3) By default, it is activated and that’s it. However, depending on how your site is made, you might need to disable some features. The best way to figure out which ones are set to disable is to open your site in an incognito window open site and see if everything works. If not, you can go back and by using trial and error to figure out what to enable.

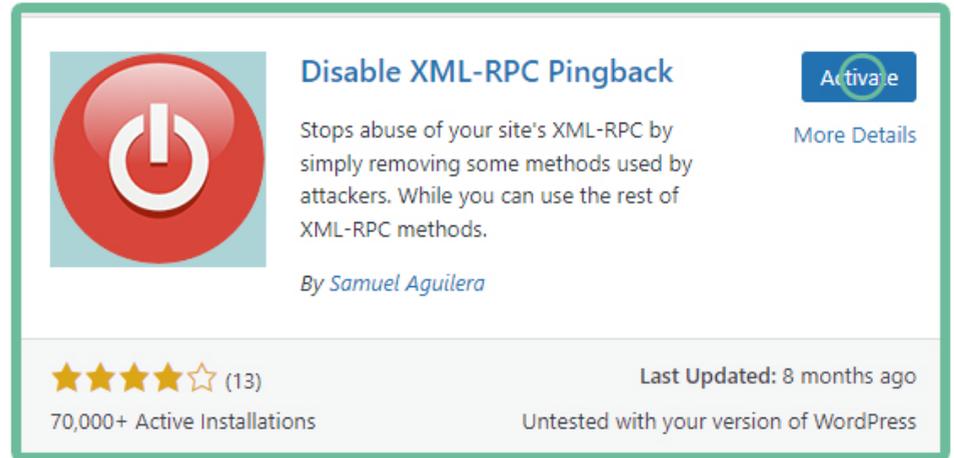
If you aren’t sure which way to go with this, then you should contact your website developer and ask. if they tell you it isn’t important get away from them.



9 Disabling the XML-RPC on WordPress

If you require remote access to WordPress don't do this. Depending on how they are coded, it might stop working.

Go to wp-admin > Plugins > Add New and search for "Disable XML-RPC" Install and activate it. That's it



Disable XML-RPC Pingback Activate
[More Details](#)

Stops abuse of your site's XML-RPC by simply removing some methods used by attackers. While you can use the rest of XML-RPC methods.

By *Samuel Aguilera*

★★★★☆ (13) Last Updated: 8 months ago
70,000+ Active Installations Untested with your version of WordPress

10 Let's move onto security plugins. First one is Sucuri.

1) Go to wp-admin > Plugins > Add New and search for "Sucuri" Install and activate it.



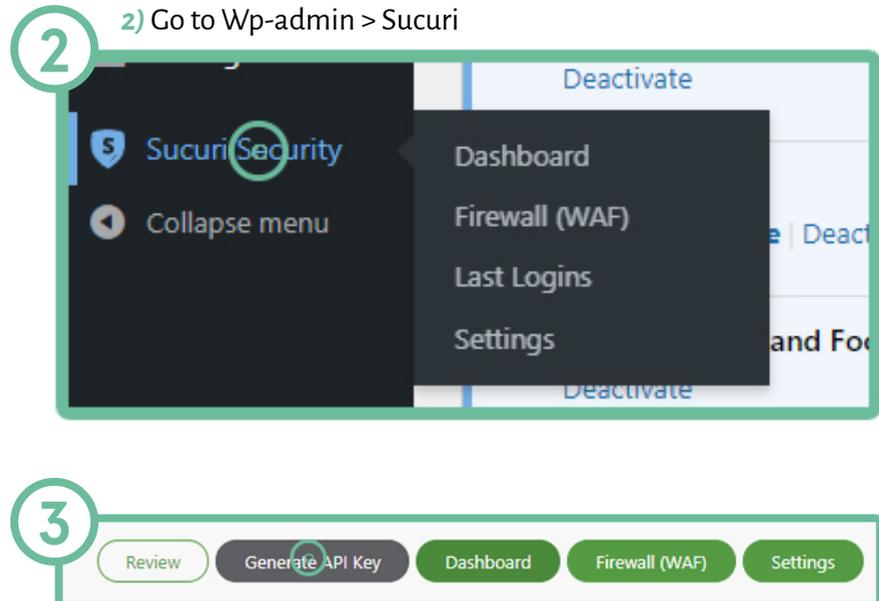
Sucuri Security – Auditing, Malware Scanner and Security Hardening Activate
[More Details](#)

The Sucuri WordPress Security plugin is a security toolset for security integrity monitoring, malware detection and security hardening.

By *Sucuri Inc.*

★★★★☆ (360) Last Updated: 4 months ago
800,000+ Active Installations ✓ Compatible with your version of WordPress

2) Go to Wp-admin > Sucuri



Dashboard
Firewall (WAF)
Last Logins
Settings

Review Generate API Key Dashboard Firewall (WAF) Settings

3) First we will need to generate API Key. Click the grey button in the top-right side of the screen.

4) Popup will open. Checkmark boxes and hit "Submit".

4 Generate API Key

An API key is required to activate some additional tools available in this plugin. The keys are free and you can virtually generate an unlimited number of them as long as the domain name and email address are unique. The key is used to authenticate the HTTP requests sent by the plugin to an API service managed by Sucuri Inc.

If you experience issues generating the API key you can request one by sending the domain name and email address that you want to use to info@sucuri.net. Note that generating a key for a website that is not facing the Internet is not possible because the API service needs to validate that the domain name exists.

WEBSITE:

E-MAIL:

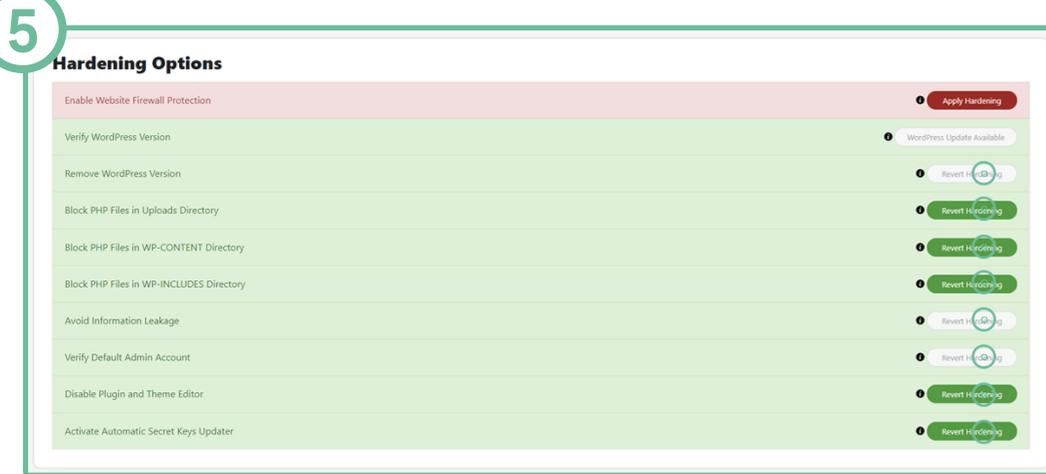
DNS LOOKUPS Enable DNS Lookups On Startup

I agree to the [Terms of Service](#).

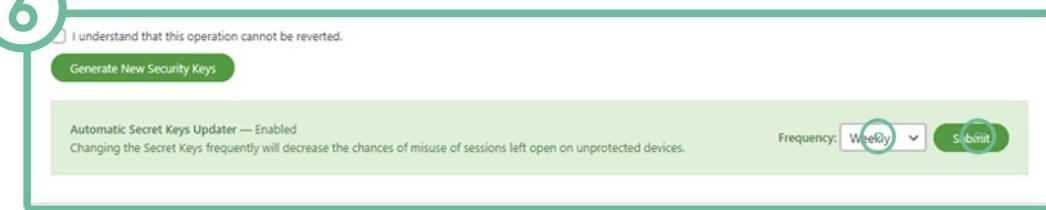
I have read and understand the [Privacy Policy](#).

Let's do a quick setup

5) Go to Wp-admin > Sucuri (2) > Settings > Hardening
In there, click "Apply Hardening" on all except Firewall.



6) Go to Wp-admin > Sucuri (2) > Settings > Post-Hack
Scroll down a bit, select Weekly and hit "Submit"

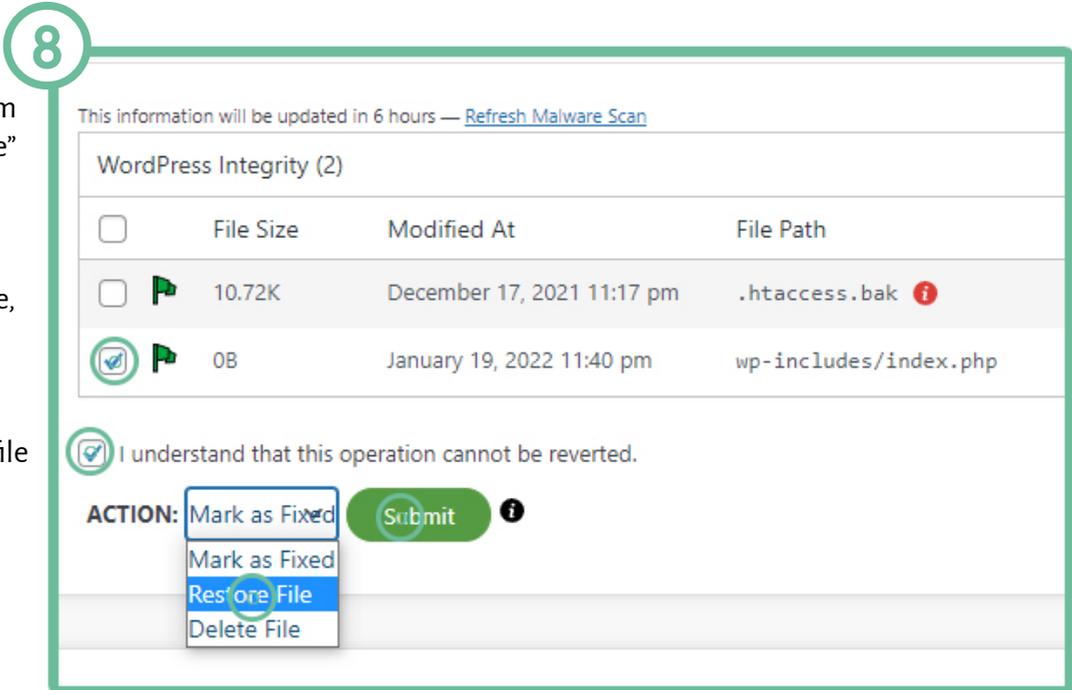


8) Checking files Integrity must be our favorite feature.
Almost all core WP files, in 99.9% cases remain untouched.
As hackers use them to exploit parts of wp-core, this is a good method to see if your site is all clean or not. In case scanners comes with files, here is what to do:

When you see files, you would always want to have them restored first. Checkmark the files and click "Restore File" Click "Submit". The plugin will tell you if the file can be restored or not.

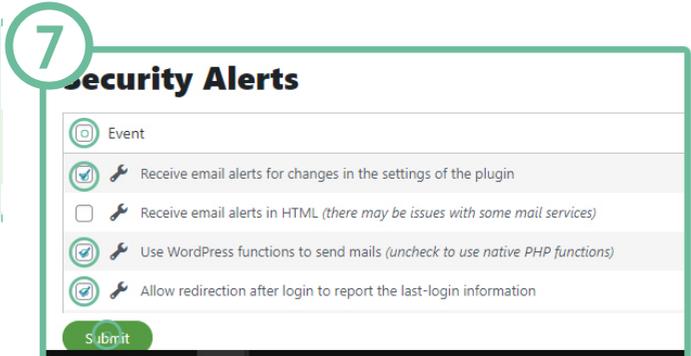
Once you tried restoring them and they still appear here, checkmark them and select "Delete File", hit "Submit".

Notice! In some cases, your developer can leave extra files there. You might even have a seperate .html/.php file in there. It is a good idea to check with your developer what you can remove and whatnot.
Or, shoot us a message!



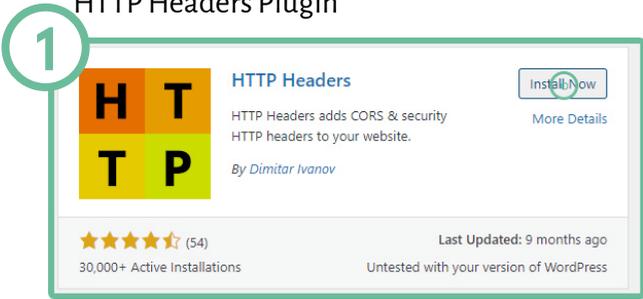
7) Go to Wp-admin > Sucuri (2) > Settings > Alerts
Here is what we have on on, but feel free to add more alerts which you may prefer.

- Receive email alerts for changes in the settings of the plugin
- Use WordPress functions to send mails (uncheck to use native PHP functions)
- Allow redirection after login to report the last-login information
- Receive email alerts for available updates
- Receive email alerts for new user registration
- Receive email alerts for successful login attempts
- Receive email alerts when the WordPress version is updated
- Receive email alerts when your website settings are updated
- Receive email alerts when a file is modified with theme/plugin editor
- Receive email alerts when a plugin is installed
- Receive email alerts when a theme is installed

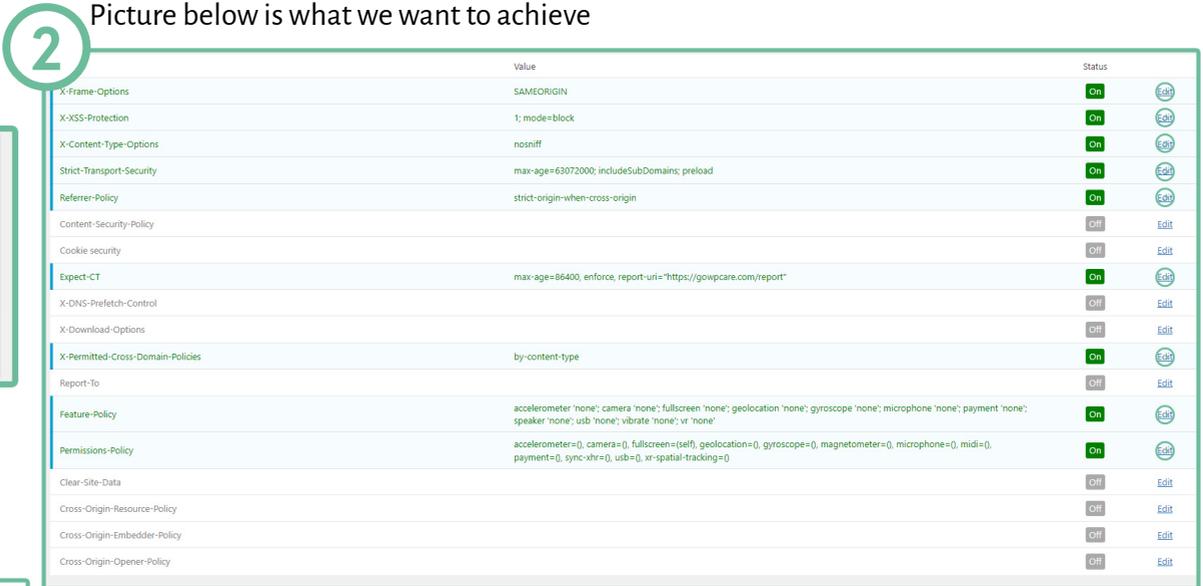


Header Security Options

1) Login to your Admin Dashboard and install HTTP Headers Plugin

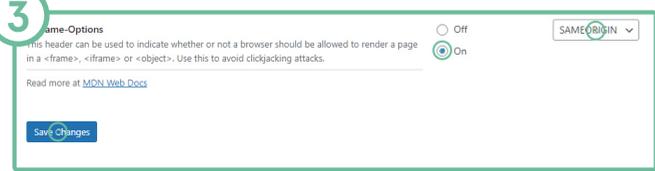


2) Go to Dashboard > Settings > HTTP Headers > Security
Picture below is what we want to achieve



Header	Value	Status
X-Frame-Options	SAMEORIGIN	On
X-XSS-Protection	1; mode=block	On
X-Content-Type-Options	nosniff	On
Strict-Transport-Security	max-age=63072000; includeSubDomains; preload	On
Referrer-Policy	strict-origin-when-cross-origin	On
Content-Security-Policy		Off
Cookie security		Off
Expect-CT	max-age=86400, enforce, report-uri="https://gowpcare.com/report"	On
X-DNS-Prefetch-Control		Off
X-Download-Options		Off
X-Permitted-Cross-Domain-Policies	by-content-type	On
Report-To		Off
Feature-Policy	accelerometer 'none'; camera 'none'; fullscreen 'none'; geolocation 'none'; gyroscope 'none'; microphone 'none'; payment 'none'; speaker 'none'; usb 'none'; vibrate 'none'; vr 'none'	On
Permissions-Policy	accelerometer=(), camera=(), fullscreen=(self), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), midi=(), payment=(), sync-xhr=(), usb=(), xr-spatial-tracking=()	On
Clear-Site-Data		Off
Cross-Origin-Resource-Policy		Off
Cross-Origin-Embedder-Policy		Off
Cross-Origin-Opener-Policy		Off

3) X-Frame-Options: click on “Edit” (2)
In there, select on and from dropdown select “SAMEORIGIN” > Hit “Save Changes”



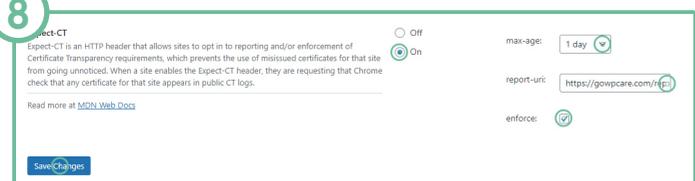
4) X-XSS-Protection: click on “Edit” (2)
In there, select on and from dropdown select “1; mode=block” > Hit “Save Changes”



5) X-Content-Type-Options: click on “Edit” (2)
In there, select on and from dropdown select “nosniff” > Hit “Save Changes”



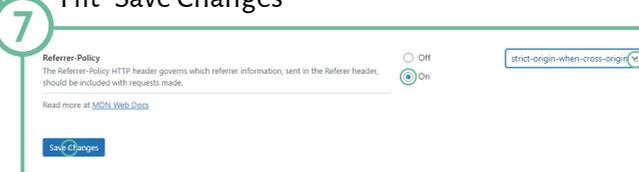
8) Expect-CT: click on “Edit” (2)
In there, select on and from dropdown select “1 day” in report URL write your domain and add /report checkmark “enforce” > Hit “Save Changes”



6) Strict-Transport-Security : click on “Edit” (2)
In there, select on and from dropdown select “2 years” checkmark “includeSubDomains” checkmark “preload” hit “Save Changes”



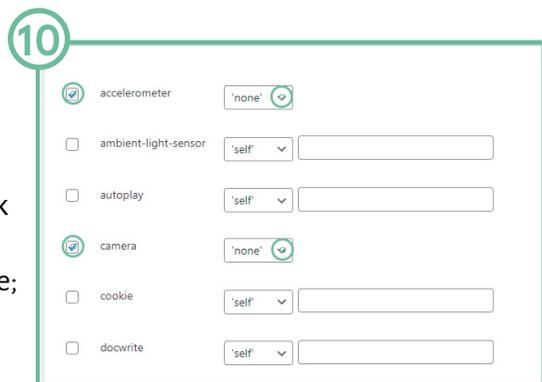
7) Referrer-Policy : click on “Edit” (2)
In there, select on and from dropdown select “strict-origin-when-cross-origin” > Hit “Save Changes”



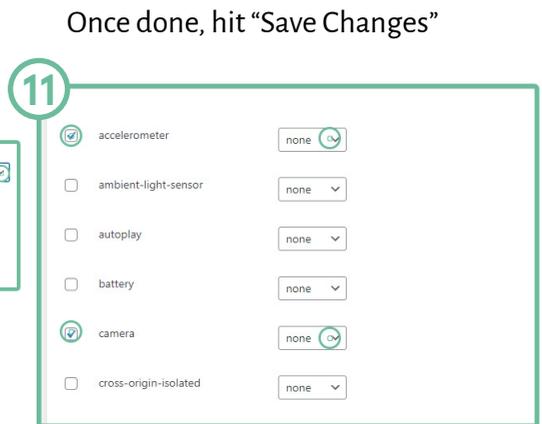
9) X-Permitted-Cross-Domain-Policies: click on “Edit” (2)
In there, select on and from dropdown select “ by-content-type” > Hit “Save Changes”



10) Feature-Policy : click on “Edit” (2)
In there, select on. Next we will only checkmark following options: accelerometer; camera; fullscreen; geolocation; gyroscope; microphone; payment; speaker; usb; vibrate; vr
Once done, hit “Save Changes”



11) Permissions-Policy : click on “Edit” (2)
In there, select on. Next we will only checkmark following options: accelerometer; camera; geolocation; gyroscope; magnetometer; microphone; midi; payment; sync-xhr; usb; xr-spatial-tracking.
On “fullscreen” option, select “self”



Once done, hit “Save Changes”



To Be Continued.

We are always working on adding more tips here. Since you already downloaded our document, you will be notified as soon as the updated version takes place.

Thank you for downloading and hopefully, you made your site more secure than before!

For any comments/help please reach out to us:

email: support@gowpcare.com

support url: <https://gowpcare.com/contact-us/>