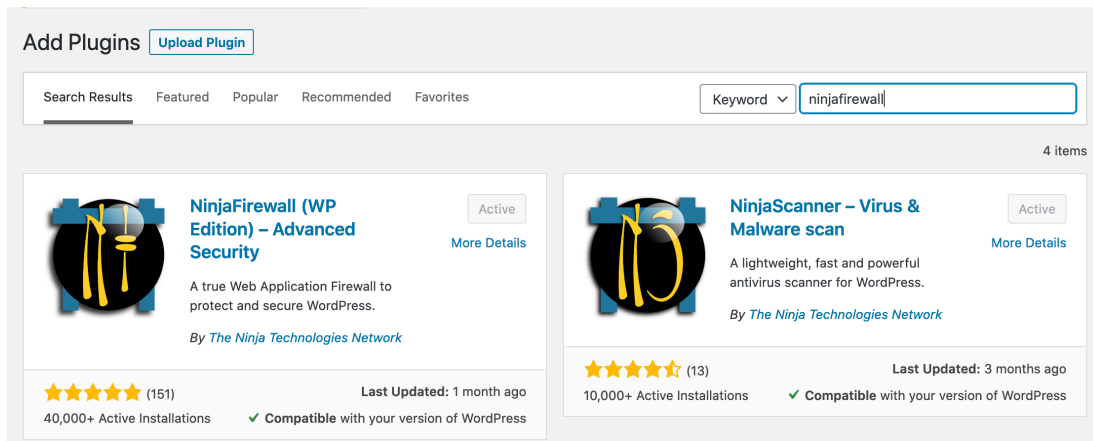
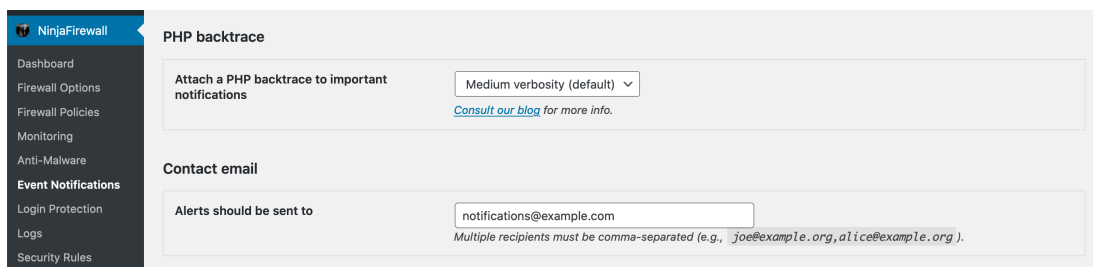


### Step 1: install and activate NinjaFirewall



### Step 2: go to NinjaFirewall – Event Notifications and copy the contact email



### Step 3: go to [ninjafirewall config browser](#)

## configuration file for NinjaFirewall WP Edition

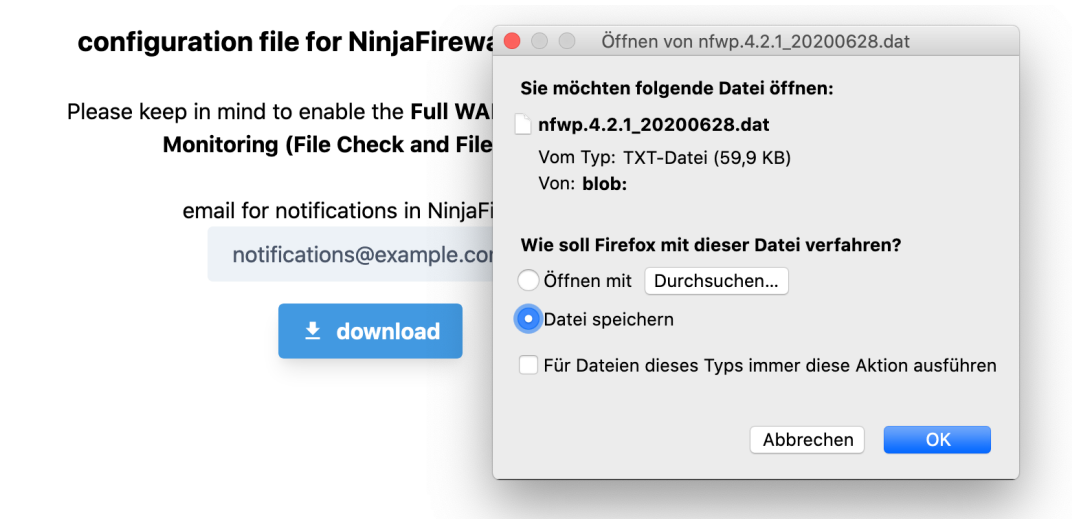
Please keep in mind to enable the **Full WAF Mode** and setup **Monitoring (File Check and File Guard)**.

email for notifications in NinjaFirewall:

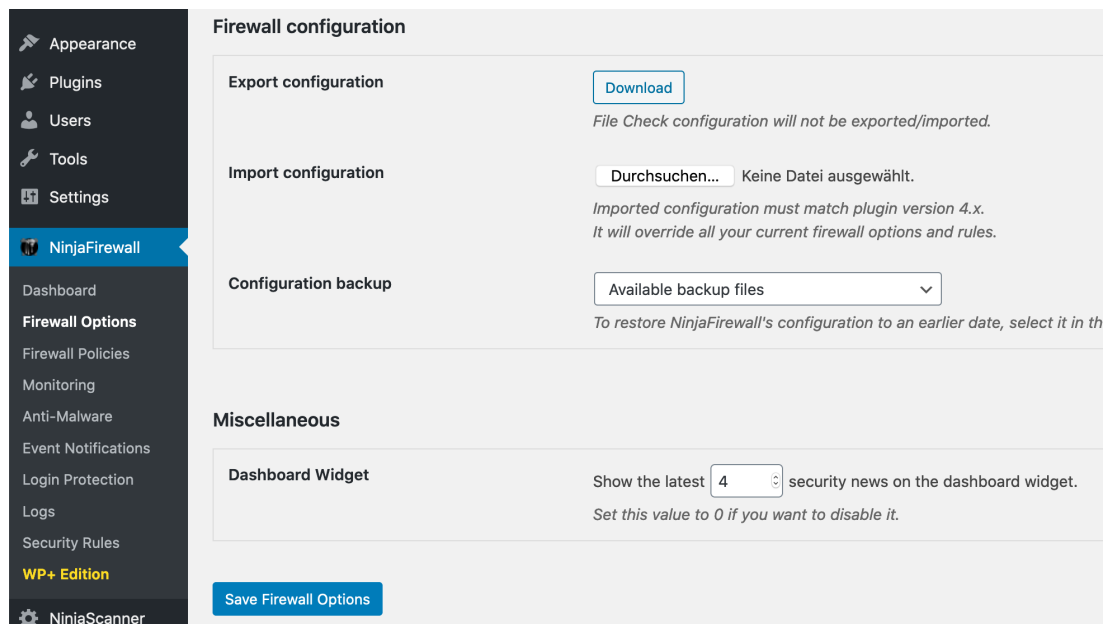
notifications@example.com

↓ download

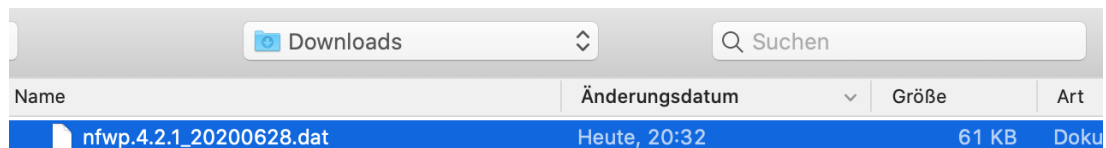
**Step 4:** insert the contact email and click the download button

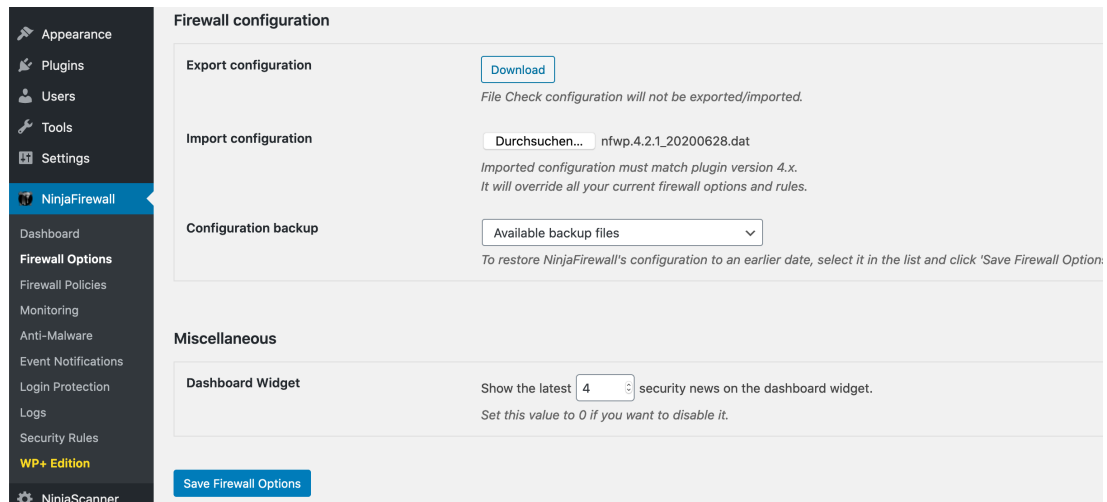


**Step 5:** go to NinjaFirewall – Firewall Options

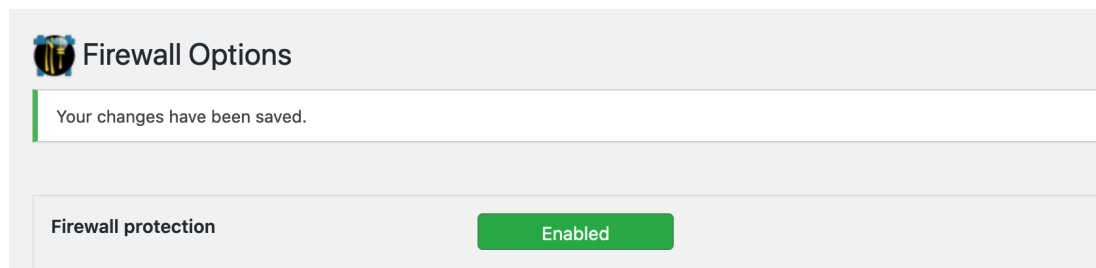


**Step 6:** import the downloaded configuration

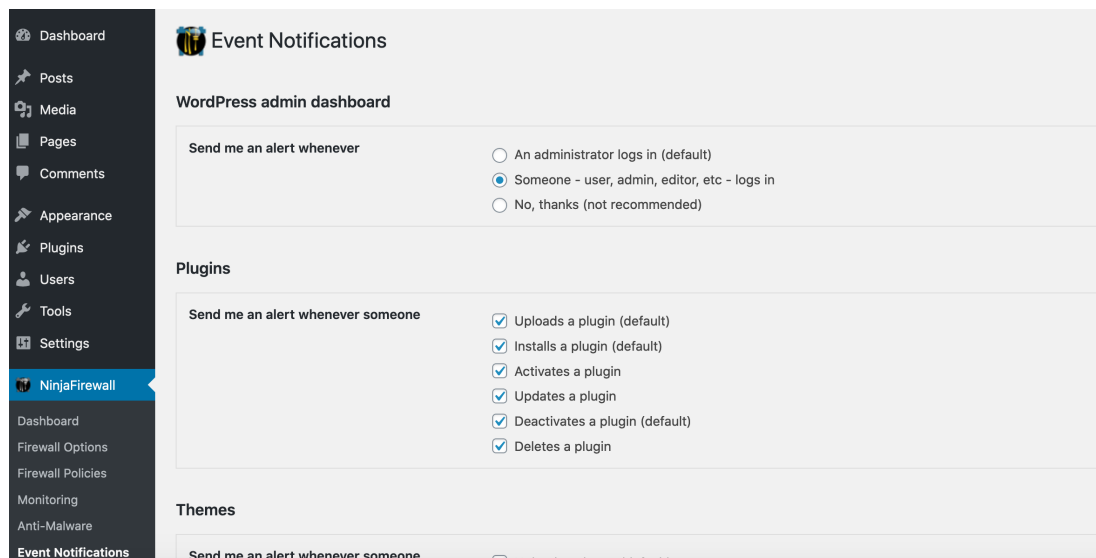




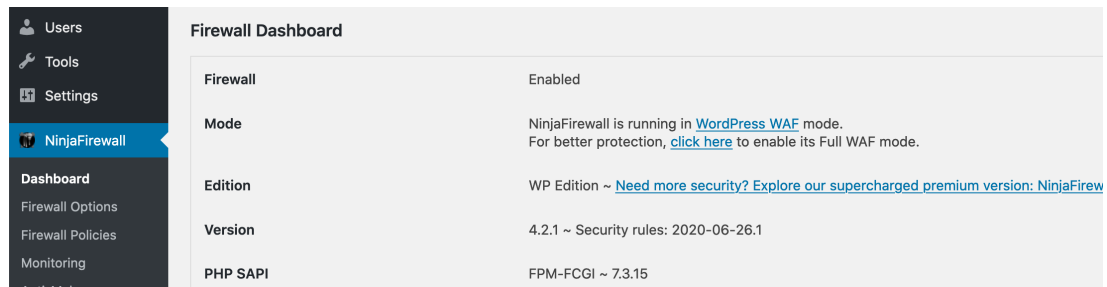
**Step 7:** submit the page (in some cases you may have to repeat step 6 and 7)



**Step 8:** go to NinjaFirewall – Event Notifications, now all events should be enabled

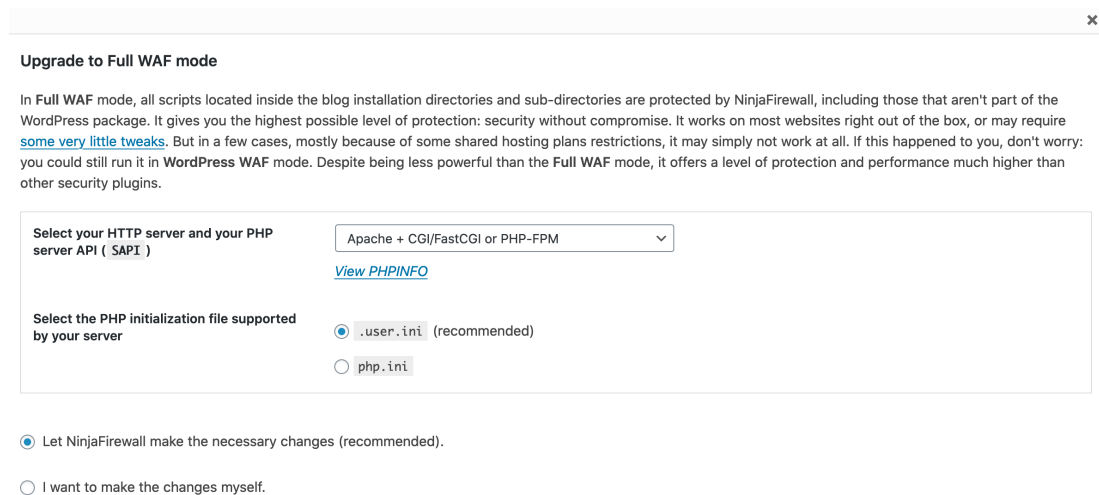


### Step 9: go to NinjaFirewall – Dashboard



Firewall Dashboard	
Firewall	Enabled
Mode	NinjaFirewall is running in <a href="#">WordPress WAF</a> mode. For better protection, <a href="#">click here</a> to enable its Full WAF mode.
Edition	WP Edition ~ <a href="#">Need more security? Explore our supercharged premium version: NinjaFirewall</a>
Version	4.2.1 ~ Security rules: 2020-06-26.1
PHP SAPI	FPM-FCGI ~ 7.3.15

### Step 10: click on “click here” to enable the Full WAF mode



**Upgrade to Full WAF mode**

In Full WAF mode, all scripts located inside the blog installation directories and sub-directories are protected by NinjaFirewall, including those that aren't part of the WordPress package. It gives you the highest possible level of protection: security without compromise. It works on most websites right out of the box, or may require [some very little tweaks](#). But in a few cases, mostly because of some shared hosting plans restrictions, it may simply not work at all. If this happened to you, don't worry: you could still run it in WordPress WAF mode. Despite being less powerful than the Full WAF mode, it offers a level of protection and performance much higher than other security plugins.

Select your HTTP server and your PHP server API ( SAPI ) Apache + CGI/FastCGI or PHP-FPM

[View PHPINFO](#)

Select the PHP initialization file supported by your server

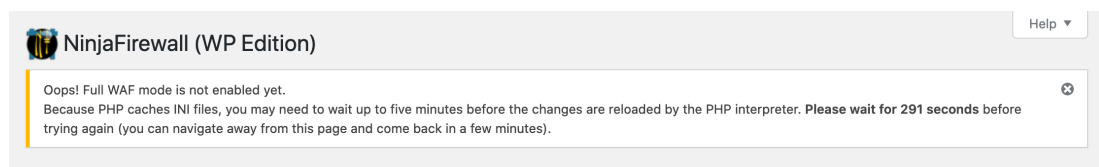
☒ .user.ini (recommended)

☐ php.ini

☒ Let NinjaFirewall make the necessary changes (recommended).

☐ I want to make the changes myself.

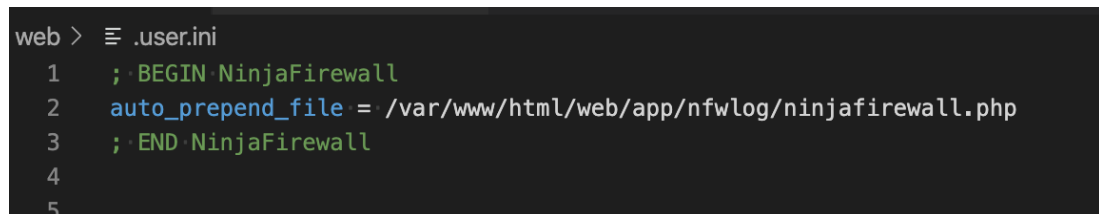
### Step 11: submit the page (scroll down to see the button, the default settings should be fine)



NinjaFirewall (WP Edition) Help

Oops! Full WAF mode is not enabled yet.  
Because PHP caches INI files, you may need to wait up to five minutes before the changes are reloaded by the PHP interpreter. Please wait for 291 seconds before trying again (you can navigate away from this page and come back in a few minutes).

### Step 12: NinjaFirewall will create a .user.ini file next to the wp-config.php file



```
web > cat .user.ini
1 ; BEGIN NinjaFirewall
2 auto_prepend_file = /var/www/html/web/app/nfwlog/ninjabfirewall.php
3 ; END NinjaFirewall
4
5
```

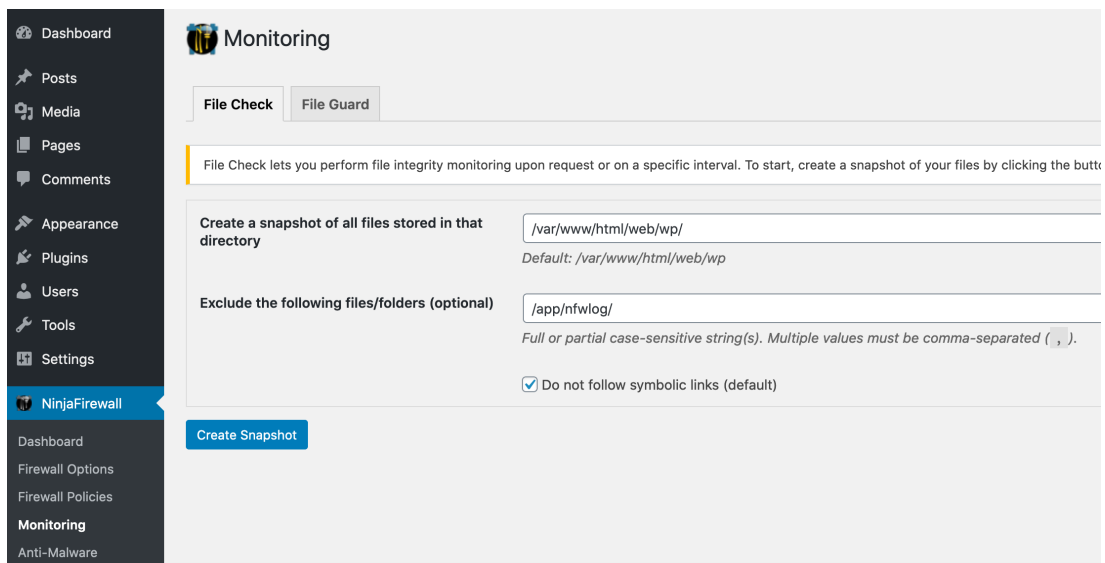
**Step 13:** after some time the status should be updated (reload the page)



The screenshot shows the 'Firewall Dashboard' with a sidebar on the left containing 'Tools', 'Settings', 'NinjaFirewall', 'Dashboard', 'Firewall Options', 'Firewall Policies', 'Monitoring', and 'Anti-Malware'. The main content area displays the following information:

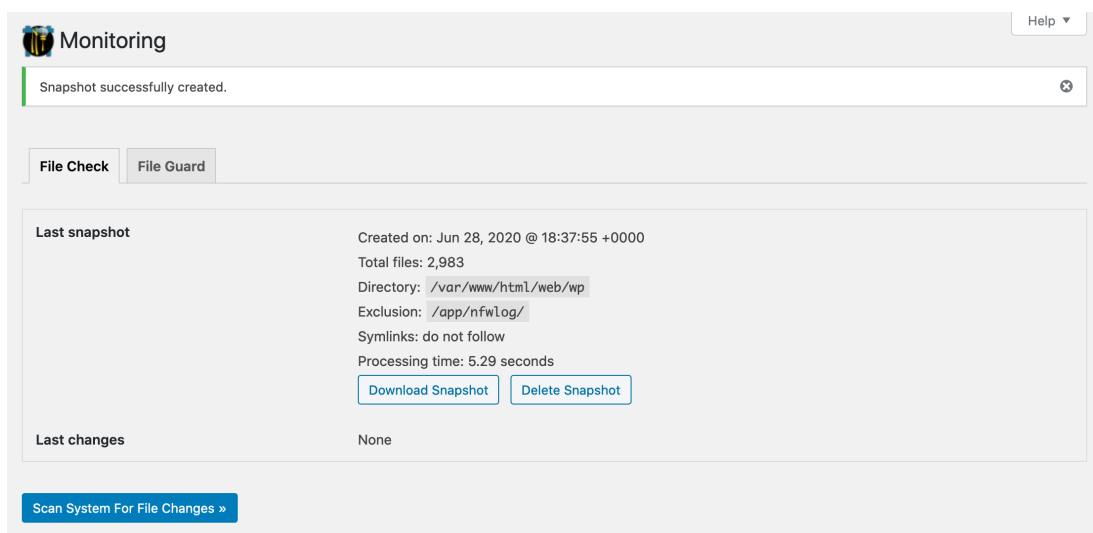
Section	Status/Details
Firewall	Enabled
Mode	NinjaFirewall is running in Full WAF mode.
Edition	WP Edition ~ <a href="#">Need more security? Explore our supercharged premium version: NinjaFirewall (WP+ Edition)</a>
Version	4.2.1 ~ Security rules: 2020-06-26.1
PHP SAPI	FPM-FCGI ~ 7.3.15

**Step 14:** go to NinjaFirewall – Monitoring



The screenshot shows the 'Monitoring' page with a sidebar on the left containing 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Appearance', 'Plugins', 'Users', 'Tools', 'Settings', 'NinjaFirewall', 'Dashboard', 'Firewall Options', 'Firewall Policies', 'Monitoring', and 'Anti-Malware'. The main content area has two tabs: 'File Check' (selected) and 'File Guard'. Below the tabs, there is a description: 'File Check lets you perform file integrity monitoring upon request or on a specific interval. To start, create a snapshot of your files by clicking the button'. The 'Create a snapshot of all files stored in that directory' section has a text input field with the value '/var/www/html/web/wp/' and a default value of '/var/www/html/web/wp'. The 'Exclude the following files/folders (optional)' section has a text input field with the value '/app/nfwlog/' and a default value of '/app/nfwlog/'. Below this, there is a checkbox labeled 'Do not follow symbolic links (default)' which is checked. A 'Create Snapshot' button is located at the bottom left of the main content area.

**Step 15:** create a snapshot

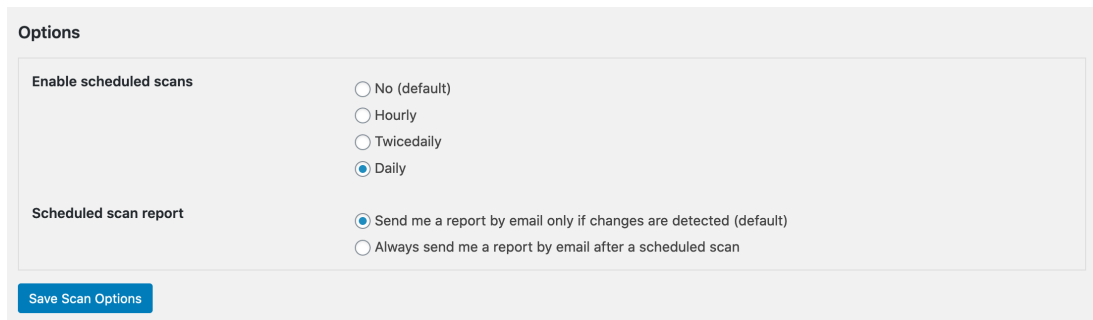


The screenshot shows the 'Monitoring' page with a sidebar on the left containing 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Appearance', 'Plugins', 'Users', 'Tools', 'Settings', 'NinjaFirewall', 'Dashboard', 'Firewall Options', 'Firewall Policies', 'Monitoring', and 'Anti-Malware'. The main content area has two tabs: 'File Check' (selected) and 'File Guard'. Below the tabs, there is a message: 'Snapshot successfully created.' with a close button. The 'Last snapshot' section displays the following information:

Section	Details
Created on:	Jun 28, 2020 @ 18:37:55 +0000
Total files:	2,983
Directory:	/var/www/html/web/wp
Exclusion:	/app/nfwlog/
Symlinks:	do not follow
Processing time:	5.29 seconds

Below the 'Last snapshot' section, there are two buttons: 'Download Snapshot' and 'Delete Snapshot'. The 'Last changes' section displays 'None'. At the bottom, there is a button labeled 'Scan System For File Changes »'.

**Step 16:** set scan schedule to daily



**Options**

**Enable scheduled scans**

☐ No (default)

☐ Hourly

☐ Twicedaily

☒ Daily

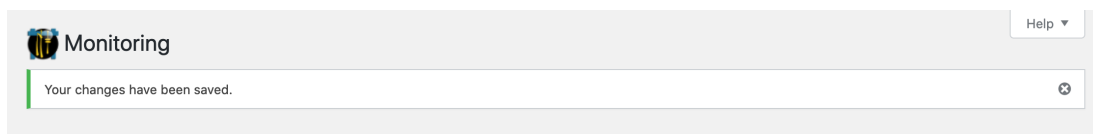
**Scheduled scan report**


☒ Send me a report by email only if changes are detected (default)

☐ Always send me a report by email after a scheduled scan

[Save Scan Options](#)

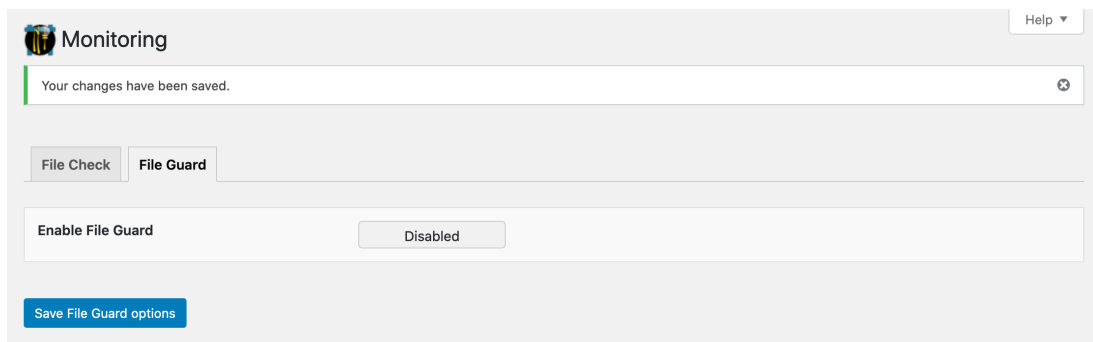
**Step 17:** click the save button




 **Monitoring** [Help](#)

Your changes have been saved.

**Step 18:** go to File Guard on the same page



 **Monitoring** [Help](#)

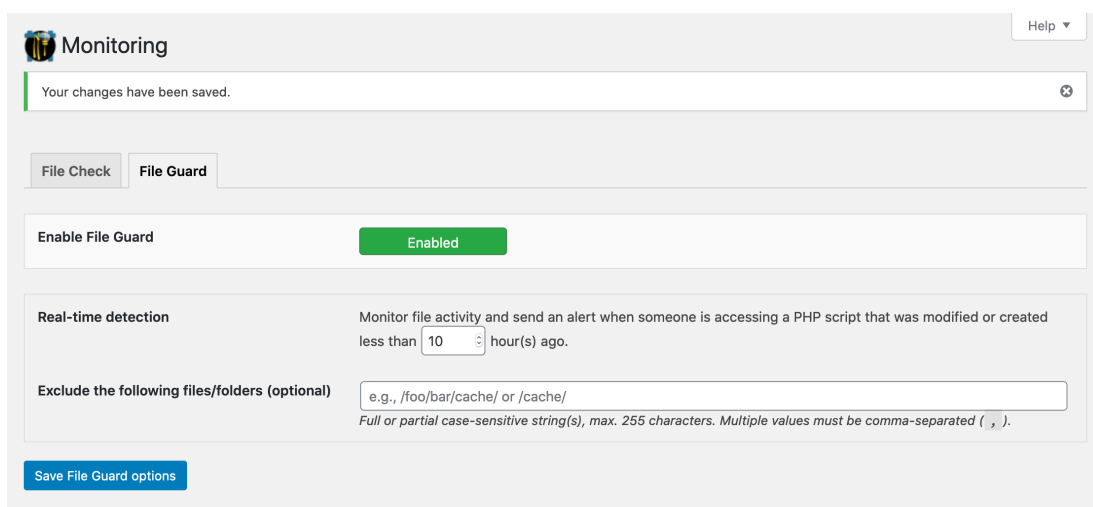
Your changes have been saved.


[File Check](#) [File Guard](#)

**Enable File Guard** [Disabled](#)

[Save File Guard options](#)

**Step 19:** enable File Guard and click the save button



 **Monitoring** [Help](#)

Your changes have been saved.

[File Check](#) [File Guard](#)

**Enable File Guard** [Enabled](#)

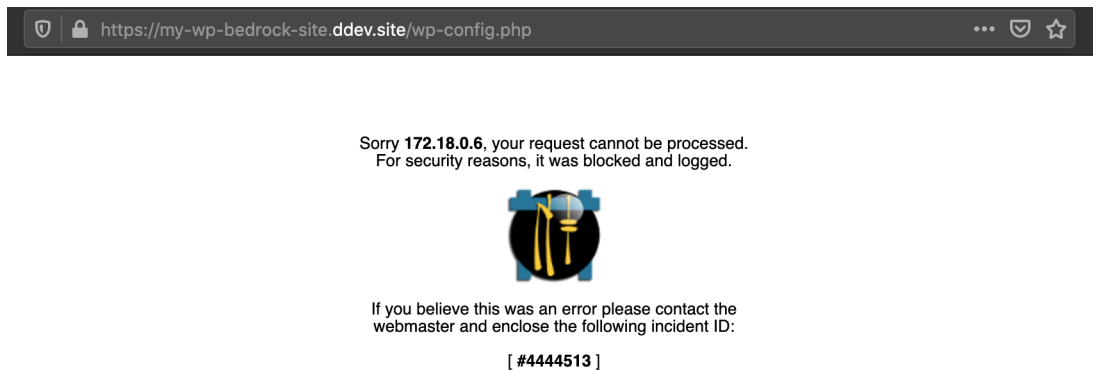
**Real-time detection** Monitor file activity and send an alert when someone is accessing a PHP script that was modified or created less than  hour(s) ago.

**Exclude the following files/folders (optional)**

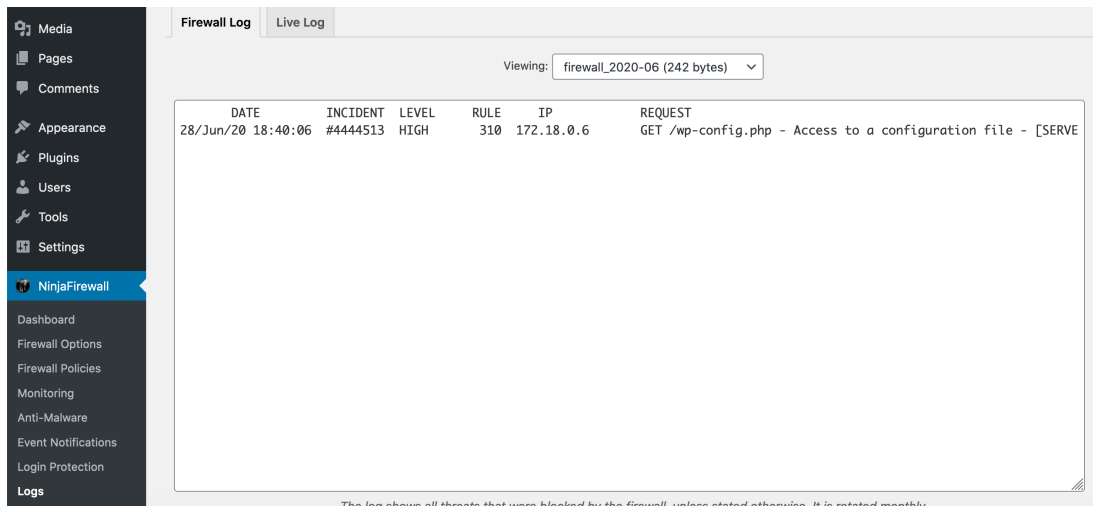
Full or partial case-sensitive string(s), max. 255 characters. Multiple values must be comma-separated ( , ).

[Save File Guard options](#)


**Step 20:** open a new incognito window and open your-domain/wp-config.php or your-domain/?%00, the request should be blocked and there should be the following information from NinjaFirewall which includes the event ID at the bottom



**Step 21:** go to NinjaFirewall – Logs, the blocked request should now appear there



**Step 22 (optional):** go to NinjaFirewall – Login Protection and use the following settings

 **Login Protection**

Enable brute force attack protection

Enabled

Type of protection

☐ Username + Password

☒ Captcha image

When to enable the protection

☒ Always enabled

☐ When under attack

Message

Type the characters you see in the picture below:

*This message will be displayed above the captcha. Max. 255 characters.*

Various options

Apply the protection to the `xmlrpc.php` script as well

Yes

Enable bot protection

Yes