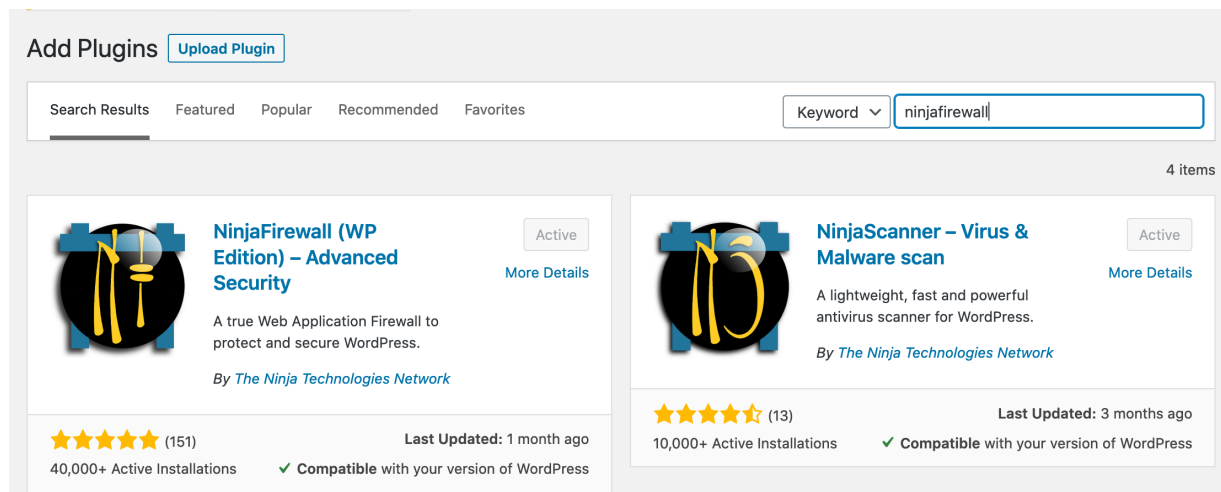
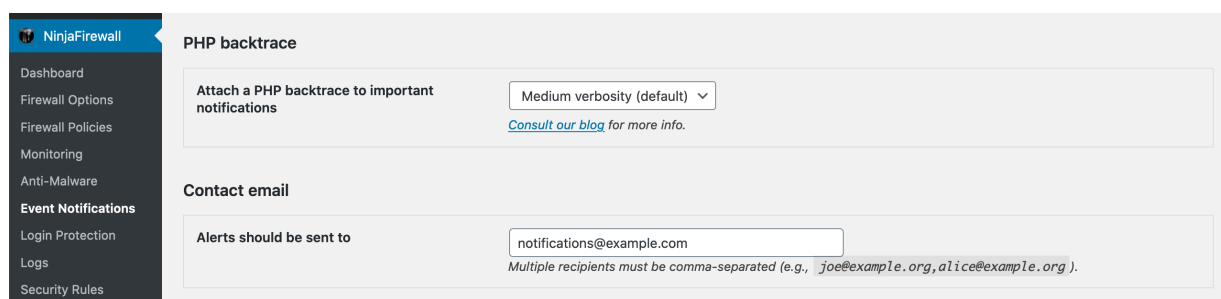


Step 1: install and activate NinjaFirewall



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

configuration file for NinjaFirewall

Please keep in mind to enable the **Full Wall**
Monitoring (File Check and File

email for notifications in NinjaFi

notifications@example.com

download



Step 5: go to NinjaFirewall – Firewall Options

Appearance

Plugins

Users

Tools

Settings

NinjaFirewall

Dashboard

Firewall Options

Firewall Policies

Monitoring

Anti-Malware

Event Notifications

Login Protection

Logs

Security Rules

WP+ Edition

NinjaScanner

Firewall configuration

Export configuration

Download

File Check configuration will not be exported/imported.

Import configuration

Durchsuchen...

Keine Datei ausgewählt.

Imported configuration must match plugin version 4.x.

It will override all your current firewall options and rules.

Configuration backup

Available backup files

To restore NinjaFirewall's configuration to an earlier date, select it in the

Miscellaneous

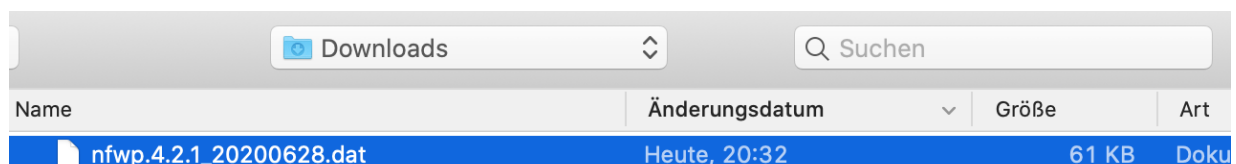
Dashboard Widget

Show the latest 4 security news on the dashboard widget.

Set this value to 0 if you want to disable it.

Save Firewall Options

Step 6: import the downloaded configuration



Firewall configuration

Export configuration [Download](#)
File Check configuration will not be exported/imported.

Import configuration [Durchsuchen...](#) nfwf.4.2.1_20200628.dat
*Imported configuration must match plugin version 4.x.
It will override all your current firewall options and rules.*

Configuration backup [Available backup files](#) ▼
To restore NinjaFirewall's configuration to an earlier date, select it in the list and click 'Save Firewall Option'.

Miscellaneous

Dashboard Widget Show the latest security news on the dashboard widget.
Set this value to 0 if you want to disable it.

[Save Firewall Options](#)

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

Firewall Options

Your changes have been saved.

Firewall protection [Enabled](#)

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

Event Notifications

WordPress admin dashboard

Send me an alert whenever ☐ An administrator logs in (default) ☒ Someone - user, admin, editor, etc - logs in ☐ No, thanks (not recommended)

Plugins

Send me an alert whenever someone ☒ Uploads a plugin (default) ☒ Installs a plugin (default) ☒ Activates a plugin ☒ Updates a plugin ☒ Deactivates a plugin (default) ☒ Deletes a plugin

Themes

Send me an alert whenever someone ☒ Updates a theme (default)

Step 9: go to NinjaFirewall – Dashboard

Firewall Dashboard	
Firewall	Enabled
Mode	NinjaFirewall is running in WordPress WAF mode. For better protection, click here to enable its Full WAF mode.
Edition	WP Edition ~ Need more security? Explore our supercharged premium version: NinjaFirewall
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)

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).

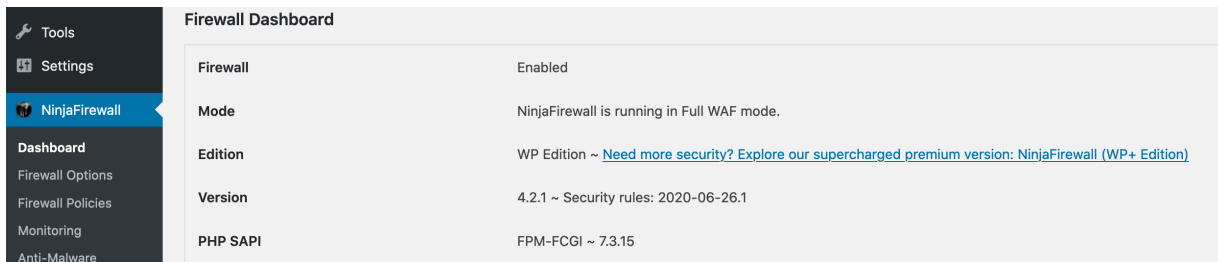
Step 12: NinjaFirewall will create a `.user.ini` file next to the `wp-config.php` file

```

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

```

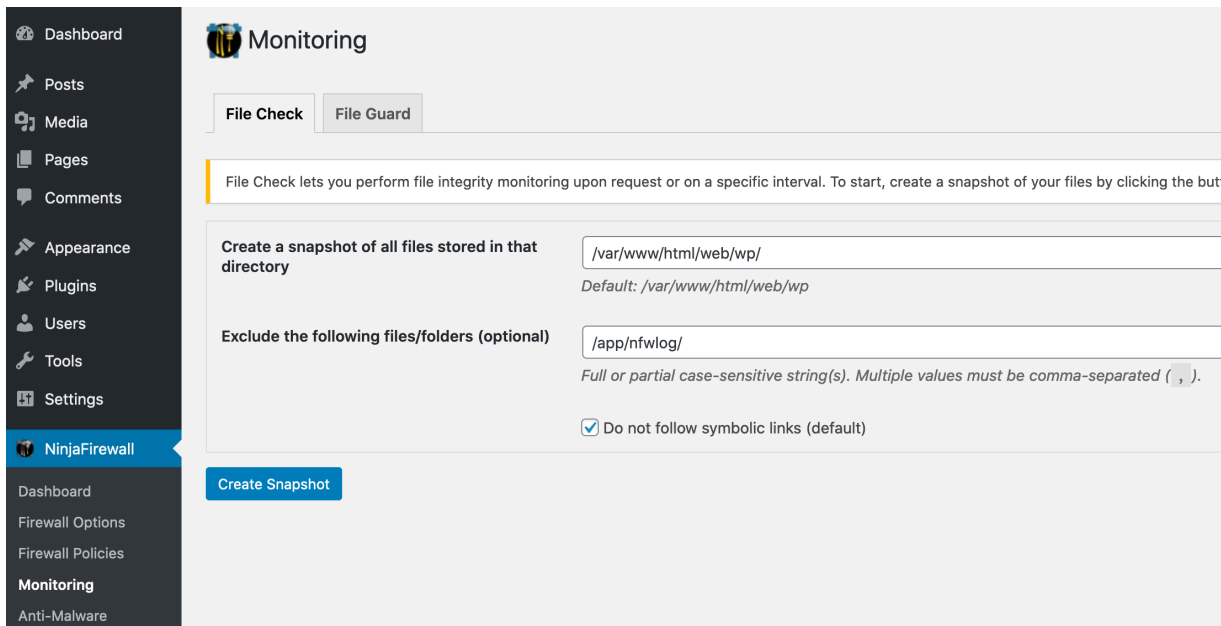
Step 13: after some time the status should be updated (reload the page)



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

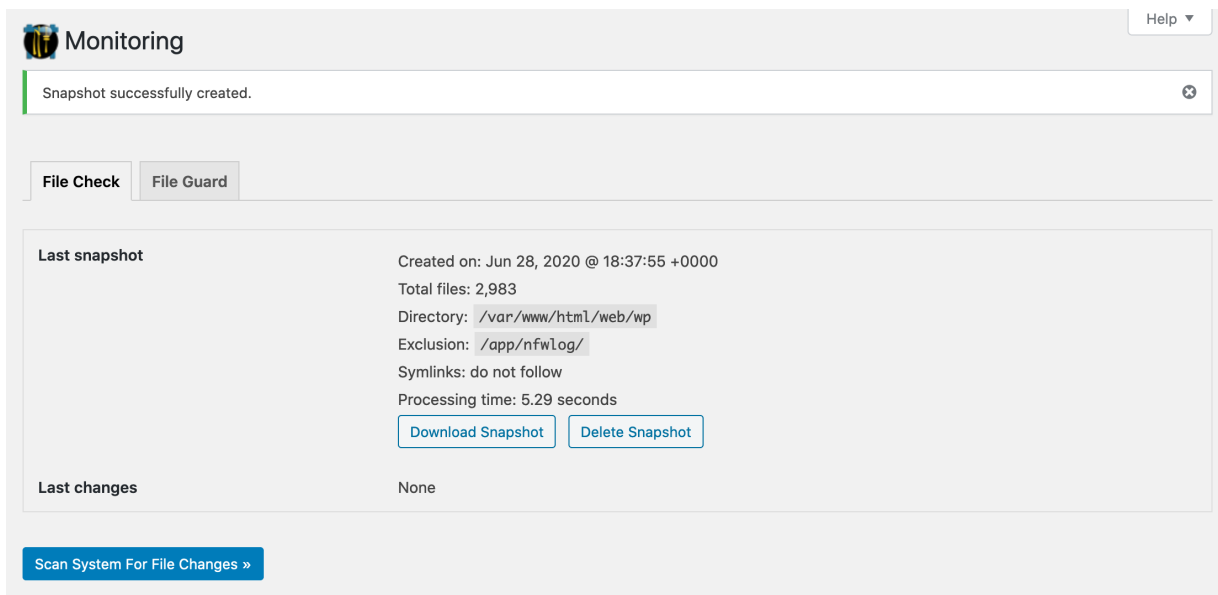
Firewall	Enabled
Mode	NinjaFirewall is running in Full WAF mode.
Edition	WP Edition ~ Need more security? Explore our supercharged premium version: NinjaFirewall (WP+ Edition)
Version	4.2.1 ~ Security rules: 2020-06-26.1
PHP SAPI	FPM-FCGI ~ 7.3.15

Step 14: go to NinjaFirewall – Monitoring



The screenshot shows the 'Monitoring' page with a sidebar on the left containing links to 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 text box explaining the File Check feature. Below that, there are two input fields: 'Create a snapshot of all files stored in that directory' with the value '/var/www/html/web/wp/' and 'Exclude the following files/folders (optional)' with the value '/app/nfwlog/'. A checkbox 'Do not follow symbolic links (default)' is checked. A 'Create Snapshot' button is at the bottom.

Step 15: create a snapshot



The screenshot shows the 'Monitoring' page with a sidebar on the left containing links to 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. Below that, there is a section 'Last snapshot' with the following information:

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 this information are two buttons: 'Download Snapshot' and 'Delete Snapshot'. Below that, there is a section 'Last changes' with the value 'None'. At the bottom, there is a button '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`, the request should be blocked and there should be the following information from NinjaFirewall which includes the event ID at the bottom



Sorry **172.18.0.6**, your request cannot be processed.
For security reasons, it was blocked and logged.



If you believe this was an error please contact the
webmaster and enclose the following incident ID:

[**#4444513**]

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


The screenshot shows the NinjaFirewall dashboard with the 'Logs' section selected. The 'Firewall Log' tab is active, displaying a table of log entries. The first entry shows a blocked request from IP 172.18.0.6 to /wp-config.php.

DATE	INCIDENT	LEVEL	RULE	IP	REQUEST
28/Jun/20 18:40:06	#4444513	HIGH	310	172.18.0.6	GET /wp-config.php - Access to a configuration file - [SERVE

Viewing: firewall_2020-06 (242 bytes) ▾

The log shows all threats that were blocked by the firewall unless stated otherwise. It is rotated monthly.

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