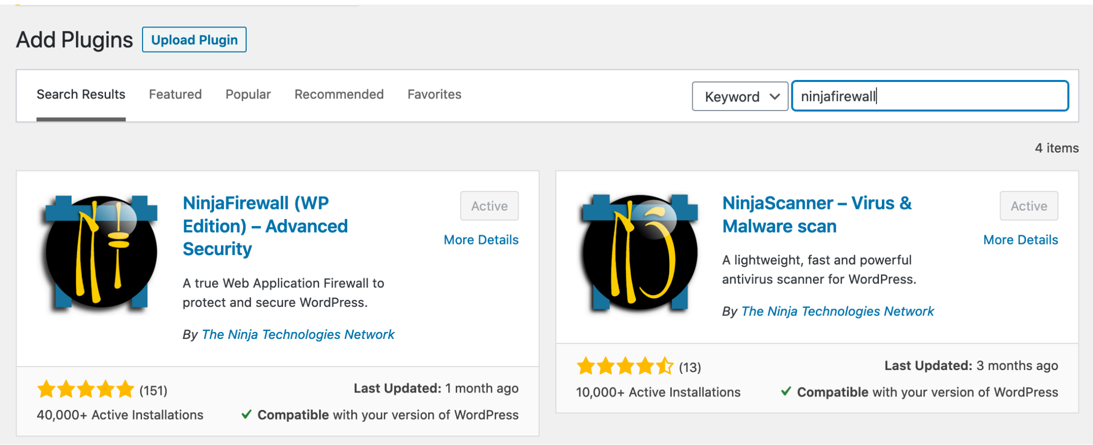
Schritt 1: installiere und aktiviere NinjaFirewall

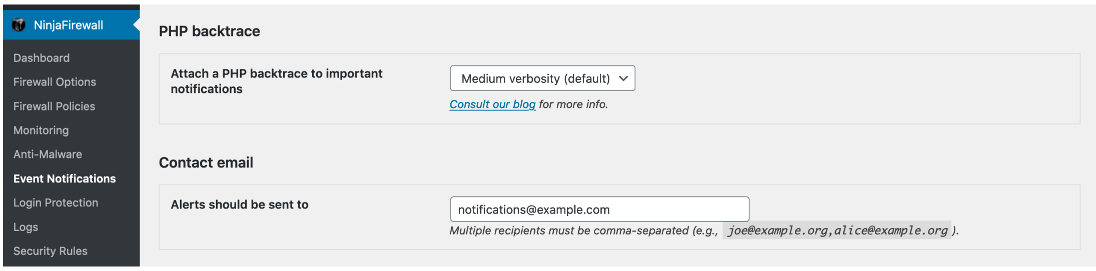


Search: ninjafirewall

NinjaFirewall (WP Edition) – Advanced Security
A true Web Application Firewall to protect and secure WordPress.
By *The Ninja Technologies Network*
★★★★★ (151)
40,000+ Active Installations
Last Updated: 1 month ago
✓ **Compatible** with your version of WordPress

NinjaScanner – Virus & Malware scan
A lightweight, fast and powerful antivirus scanner for WordPress.
By *The Ninja Technologies Network*
★★★★☆ (13)
10,000+ Active Installations
Last Updated: 3 months ago
✓ **Compatible** with your version of WordPress

Schritt 2: gehe zu NinjaFirewall – Event Notifications und kopiere die Kontakt-Emailadresse



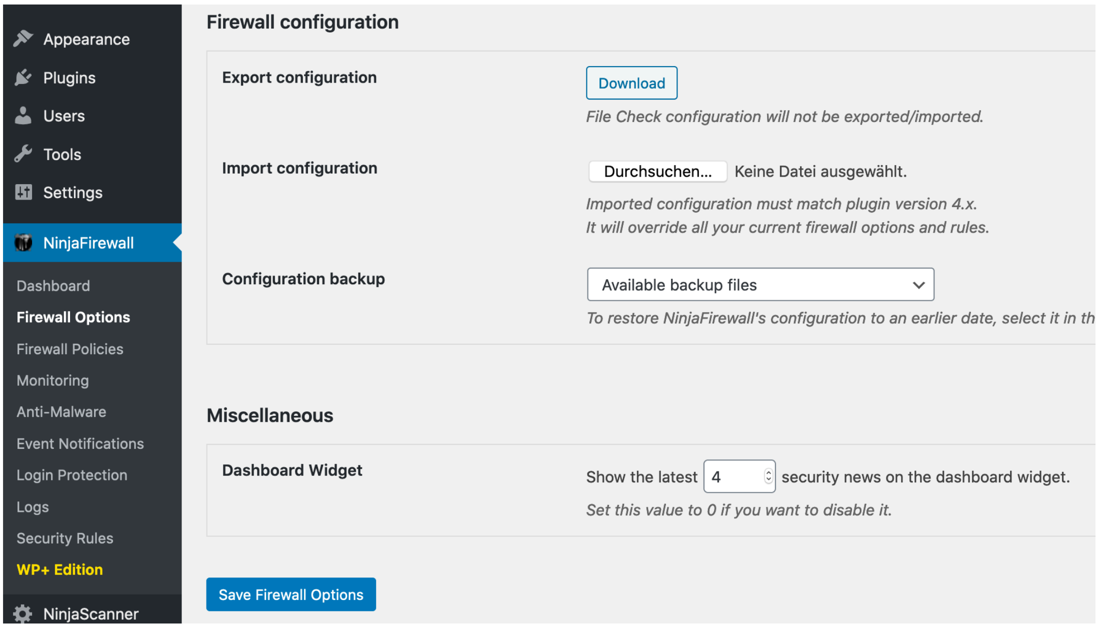
PHP backtrace

Attach a PHP backtrace to important notifications: Medium verbosity (default)
Consult our blog for more info.

Contact email

Alerts should be sent to: notifications@example.com
Multiple recipients must be comma-separated (e.g., `joe@example.org,alice@example.org`).

Schritt 3: gehe zu https://magos-securitas.com/downloads/ und lade die Konfigurations-Datei herunter
Schritt 4: gehe zu NinjaFirewall – Firewall Options



Firewall configuration

Export configuration: Download
File Check configuration will not be exported/imported.

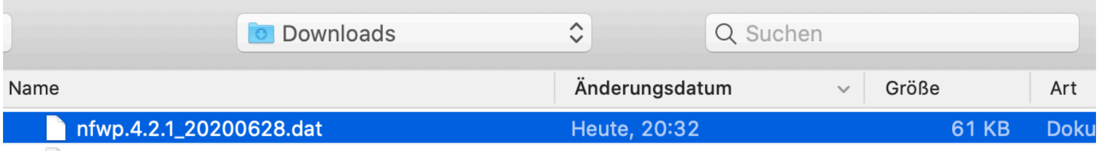
Import configuration: Durchsuchen... Keine Datei ausgewählt.
Imported configuration must match plugin version 4.x.
It will override all your current firewall options and rules.

Configuration backup: Available backup files
To restore NinjaFirewall's configuration to an earlier date, select it in th

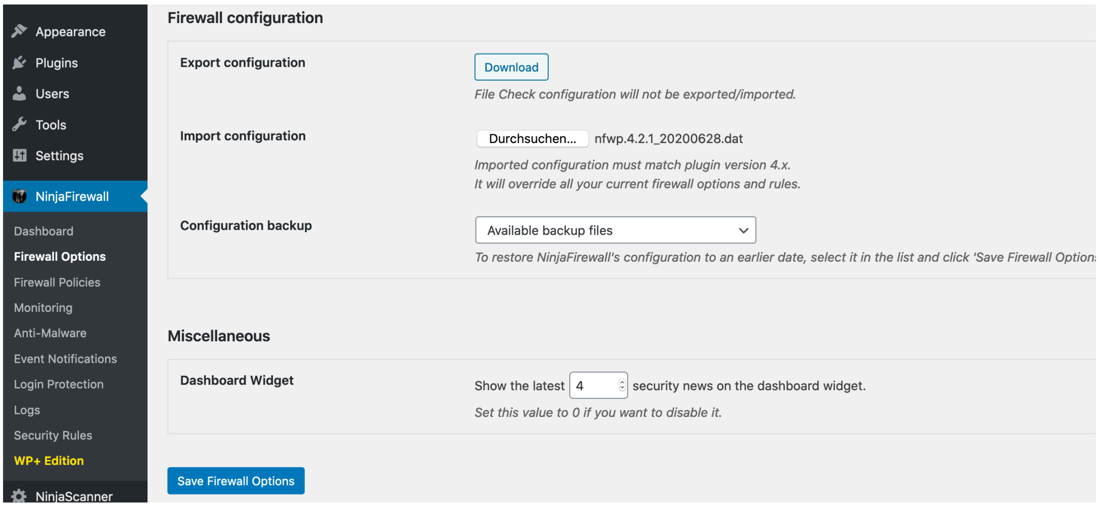
Miscellaneous

Dashboard Widget: Show the latest 4 security news on the dashboard widget.
Set this value to 0 if you want to disable it.

Schritt 5: importiere die heruntergeladene Konfigurations-Datei



Name	Änderungsdatum	Größe	Art
nfwp.4.2.1_20200628.dat	Heute, 20:32	61 KB	Doku



Firewall configuration

Export configuration: Download
File Check configuration will not be exported/imported.

Import configuration: Durchsuchen... nfwp.4.2.1_20200628.dat
Imported configuration must match plugin version 4.x.
It will override all your current firewall options and rules.

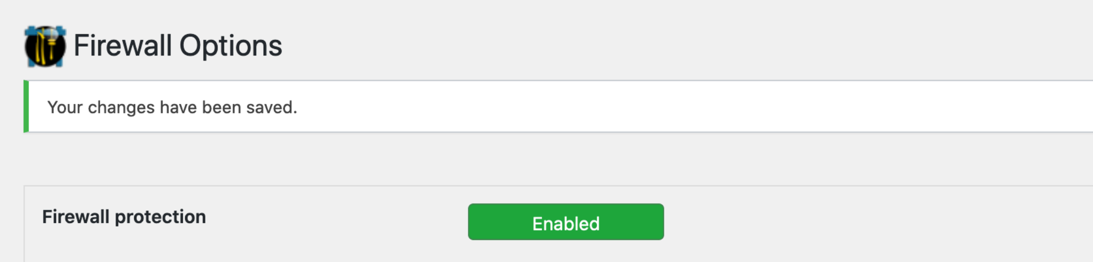
Configuration backup: Available backup files
To restore NinjaFirewall's configuration to an earlier date, select it in the list and click 'Save Firewall Option

Miscellaneous

Dashboard Widget: Show the latest 4 security news on the dashboard widget.
Set this value to 0 if you want to disable it.

Save Firewall Options

Schritt 6: speicher das Formular (in manchen Fällen müssen Schritt 6 und 7 wiederholt werden)

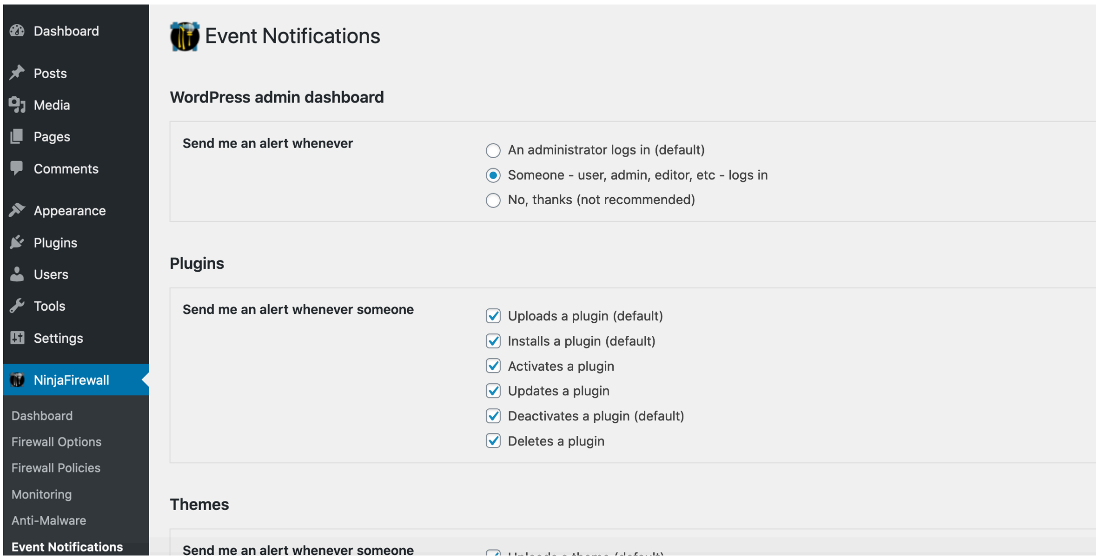


Firewall Options

Your changes have been saved.

Firewall protection: Enabled

Schritt 7: gehe zu NinjaFirewall – Event Notifications, alle Events sollten angehakt sein



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)

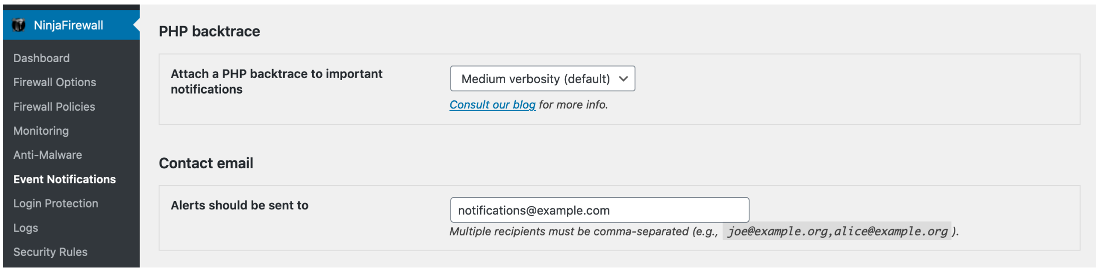
Plugins

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
☑ Uploads a theme (default)

Schritt 8: gehe zu NinjaFirewall – Event Notifications und füge die Kontakt-Emailadresse von Schritt 2 ein, speicher das Formular



PHP backtrace

Attach a PHP backtrace to important notifications: Medium verbosity (default)

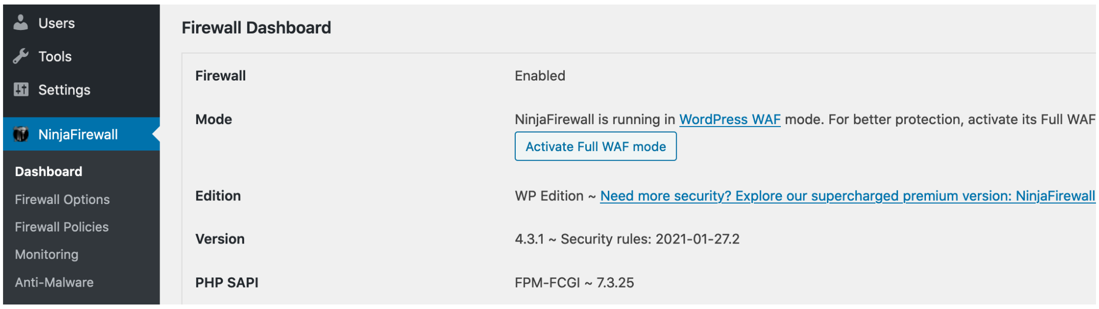
Consult our blog for more info.

Contact email

Alerts should be sent to: notifications@example.com

Multiple recipients must be comma-separated (e.g., `joe@example.org,alice@example.org`).

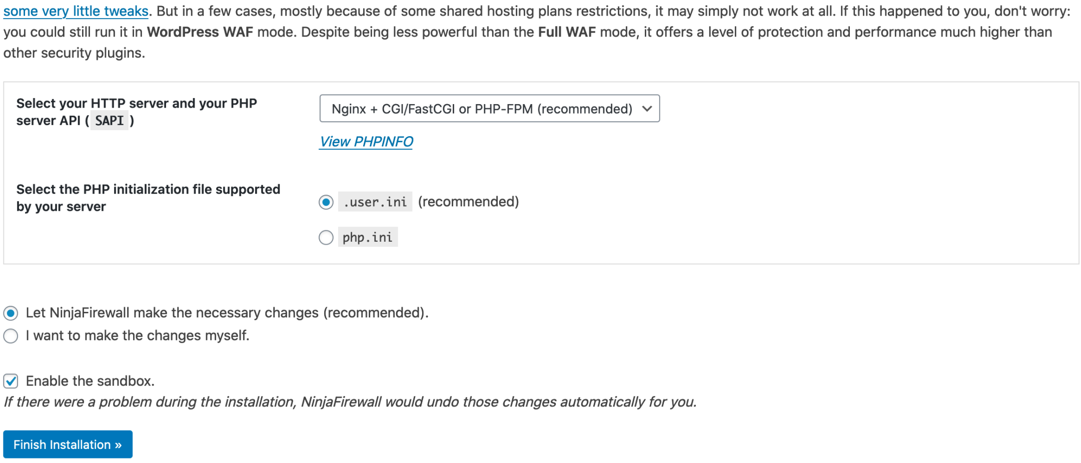
Schritt 9: gehe zu NinjaFirewall – Dashboard



Firewall Dashboard

Firewall	Enabled
Mode	NinjaFirewall is running in WordPress WAF mode. For better protection, activate its Full WAF
Edition	WP Edition ~ Need more security? Explore our supercharged premium version: NinjaFirewall
Version	4.3.1 ~ Security rules: 2021-01-27.2
PHP SAPI	FPM-FCGI ~ 7.3.25

Schritt 10: klick auf „activate Full WAF mode“



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`): Nginx + CGI/FastCGI or PHP-FPM (recommended)

View PHPINFO

Select the PHP initialization file supported by your server:

● `.user.ini` (recommended)

○ `php.ini`

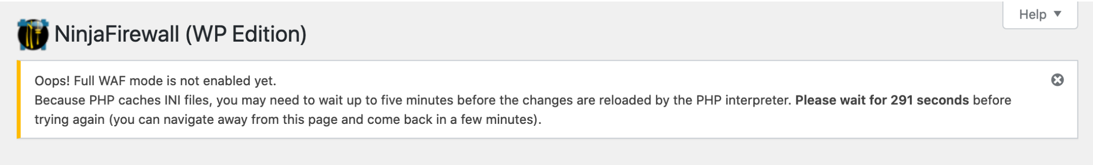
● Let NinjaFirewall make the necessary changes (recommended).

○ I want to make the changes myself.

☑ Enable the sandbox.

If there were a problem during the installation, NinjaFirewall would undo those changes automatically for you.

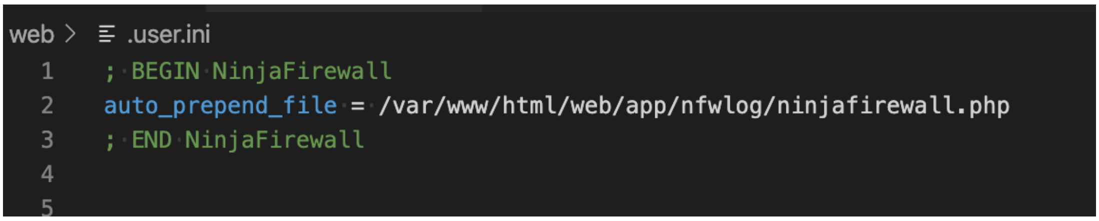
Schritt 11: speicher das Formular (runterscrollen um den Button zu sehen, die ausgewählten Einstellungen sollten ok sein)



NinjaFirewall (WP Edition)

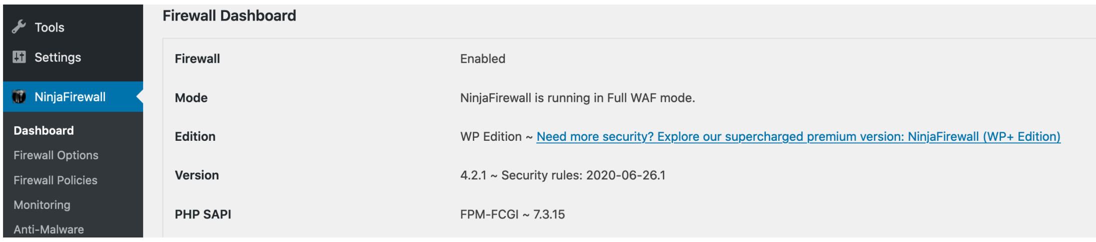
Oops! Full WAF mode is not enabled yet.
Because PHP caches INI files, you may need to wait up to five minutes before the changes are reloaded by the PHP interpreter. **Please wait for 291 seconds** before trying again (you can navigate away from this page and come back in a few minutes).

Schritt 12: NinjaFirewall wird eine .user.ini Datei auf der Ebene von wp-config.php erstellen



```
; BEGIN NinjaFirewall
auto_prepend_file = /var/www/html/web/app/nfwlog/ninjafirewall.php
; END NinjaFirewall
```

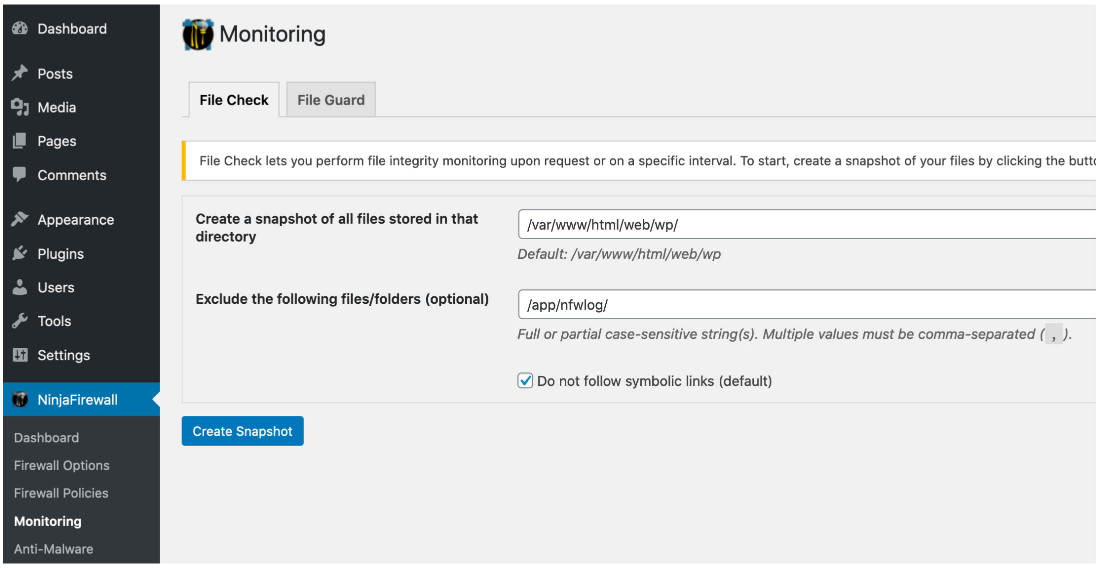
Schritt 13: nach ein paar Minuten sollte der Status aktualisiert sein (Seite neuladen)



Firewall Dashboard

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

Schritt 14: gehe zu NinjaFirewall – Monitoring



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 butt

Create a snapshot of all files stored in that directory: /var/www/html/web/wp/

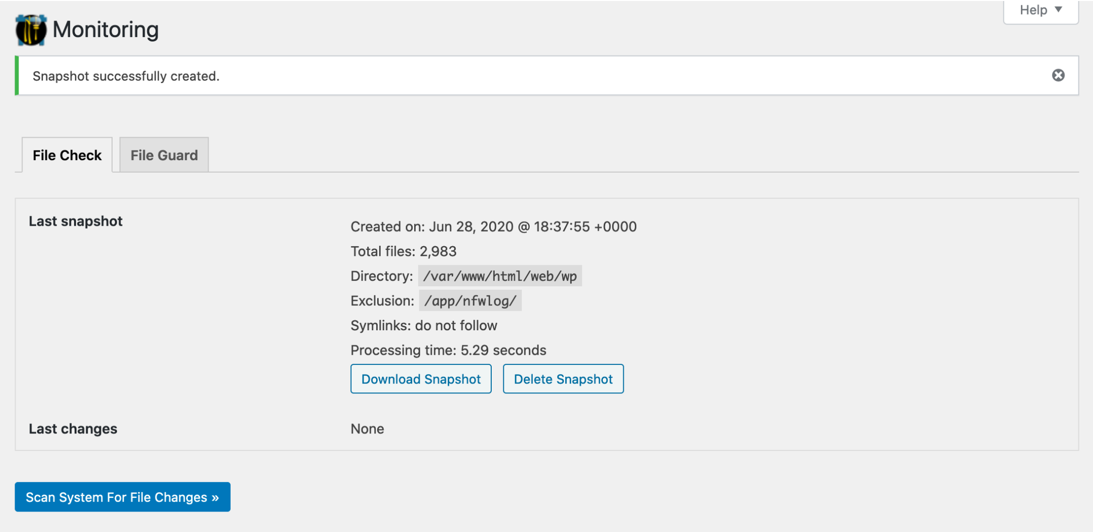
Default: /var/www/html/web/wp

Exclude the following files/folders (optional): /app/nfwlog/

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

☑ Do not follow symbolic links (default)

Schritt 15: erstell einen Snapshot



Monitoring

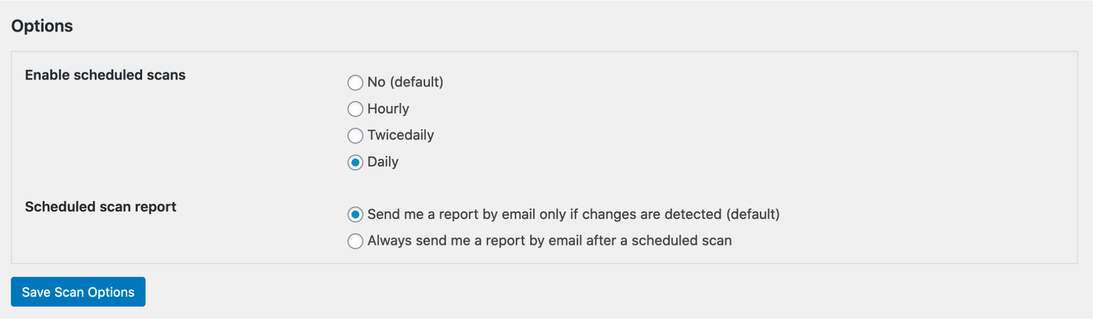
Snapshot successfully created.

Last snapshot

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

Last changes: None

Schritt 16: setz das Scan-Intervall auf täglich



Options

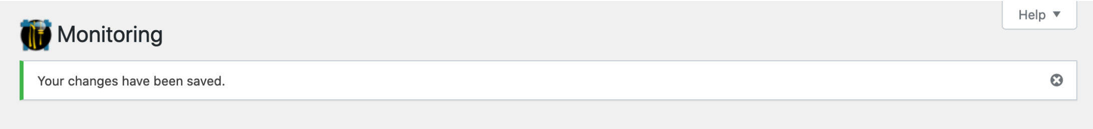
Enable scheduled scans

○ 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

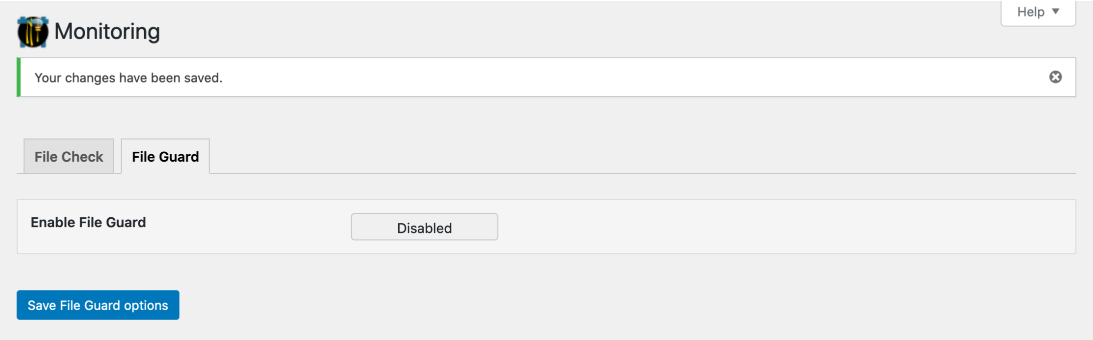
Schritt 17: klick den Speichern-Button



Monitoring

Your changes have been saved.

Schritt 18: gehe zu File Guard auf der gleichen Seite

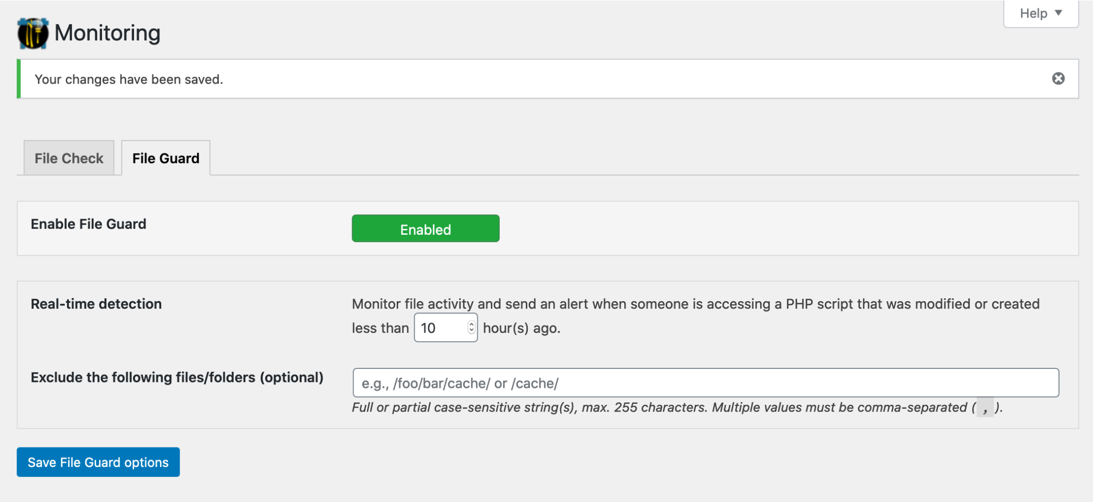


Monitoring

Your changes have been saved.

Enable File Guard: Disabled

Schritt 19: aktivier File Guard und klick den Speichern-Button



Monitoring

Your changes have been saved.

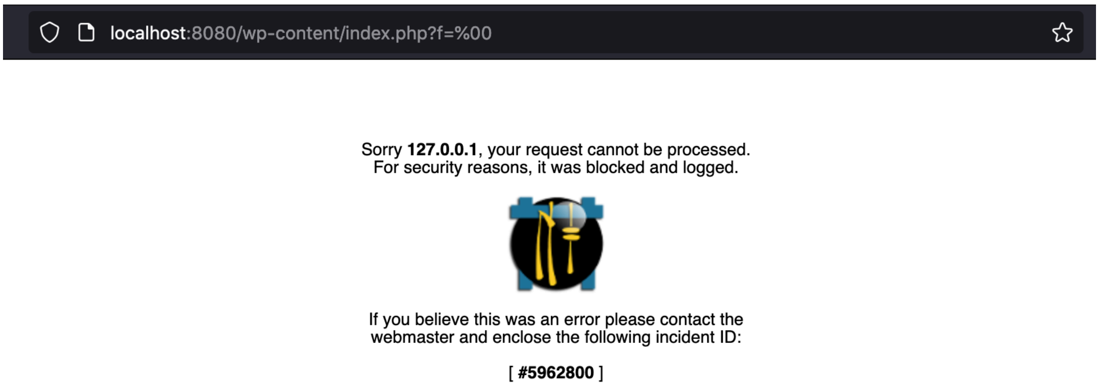
Enable File Guard: Enabled

Real-time detection: Monitor file activity and send an alert when someone is accessing a PHP script that was modified or created less than 10 hour(s) ago.

Exclude the following files/folders (optional): e.g., /foo/bar/cache/ or /cache/

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

Schritt 20: öffne ein neues Inkognito-Fenster im Browser und öffne deine-domain/wp-content/index.php?f=%00, die Anfrage sollte blockiert werden und dort sollte die folgende Information von NinjaFirewall zu sehen sein, die unten auch die Event-ID enthält



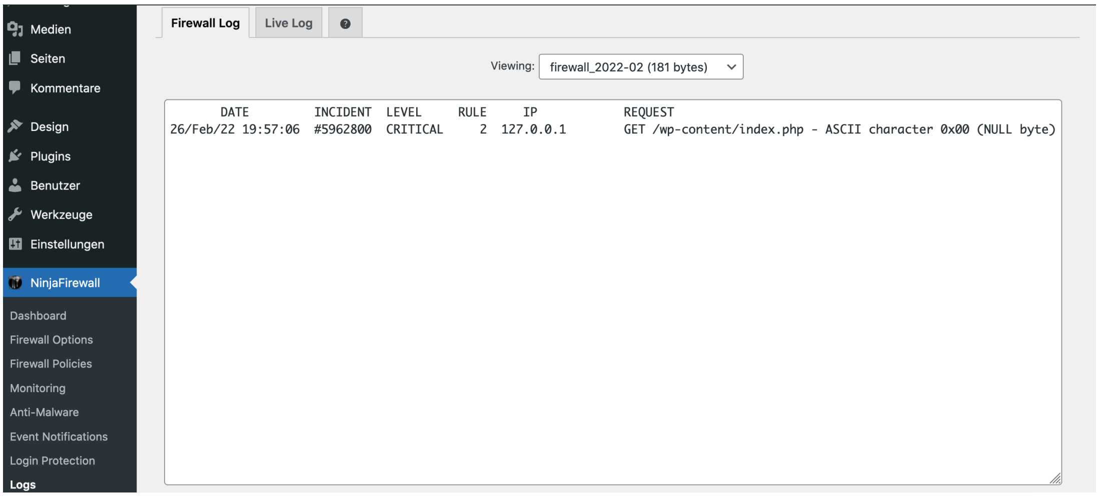
localhost:8080/wp-content/index.php?f=%00

Sorry **127.0.0.1**, 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:

[**#5962800**]

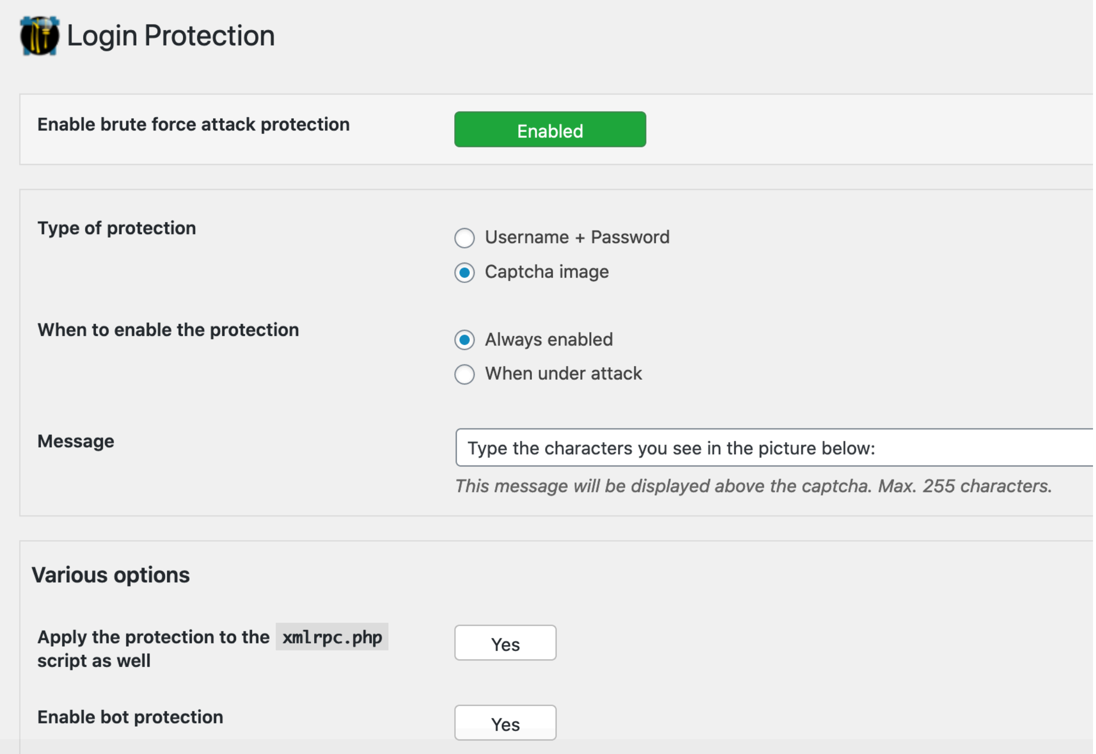
Schritt 21: gehe zu NinjaFirewall – Logs, die blockierte Anfrage sollte jetzt dort auftauchen



Viewing: firewall_2022-02 (181 bytes)

```
       DATE          INCIDENT  LEVEL     RULE     IP             REQUEST
26/Feb/22 19:57:06  #5962800  CRITICAL     2  127.0.0.1        GET /wp-content/index.php - ASCII character 0x00 (NULL byte)
```

Schritt 22 (optional): gehe zu NinjaFirewall – Login Protection und verwende die folgenden Optionen



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