Step 1: install and activate NinjaFirewall

earch Results	Featured Popular Recommended	Favorites	Keyword V ninjafirewall
			4
	NinjaFirewall (WP Edition) – Advanced Security	Active More Details	NinjaScanner – Virus & Activ Malware scan A lightweight, fast and powerful
	A true Web Application Firewall to protect and secure WordPress.		antivirus scanner for WordPress. By The Ninja Technologies Network

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

🚺 NinjaFirewall	PHP backtrace	
Dashboard Firewall Options Firewall Policies	Attach a PHP backtrace to important notifications	Medium verbosity (default)       V         Consult our blog for more info.
Monitoring		
Anti-Malware	Contact email	
Event Notifications	oontaet entan	
Login Protection	Alerts should be sent to	notifications@example.com
Logs		Multiple recipients must be comma-separated (e.g., joe@example.org, alice@example.org ).
Security Rules		

**Step 3:** go to https://magos-securitas.com/downloads/ and download the configuration file **Step 4:** go to NinjaFirewall – Firewall Options

🔊 Appearance	Firewall configuration	
📂 Plugins	Export configuration	Download
👗 Users		File Check configuration will not be exported/imported.
🗲 Tools	Import configuration	Durchsuchen Keine Datei ausnewählt
Settings		Imported configuration must match plugin version 4.x.
🚺 NinjaFirewall		It will override all your current firewall options and rules.
Dashboard	Configuration backup	Available backup files
Firewall Options		To restore NinjaFirewall's configuration to an earlier date, select it in th
Firewall Policies		
Monitoring		
Anti-Malware	Miscellaneous	
Event Notifications		
Login Protection	Dashboard Widget	Show the latest $\begin{bmatrix} 4 \\ 0 \end{bmatrix}$ security news on the dashboard widget.
Logs		Set this value to 0 if you want to disable it.
Security Rules		
WP+ Edition		
🏟 NinjaScanner	Save Firewall Options	

## **Step 5:** import the downloaded configuration

	o Downloads	Q Suchen
Name		Änderungsdatum v Größe Art
nfwp.4.	2.1_20200628.dat	Heute, 20:32 61 KB Dok
🔊 Appearance	Firewall configuration	
🖌 Plugins	Export configuration	Download
<ul> <li>▲ Users</li> <li>✓ Tools</li> <li>☑ Settings</li> <li>☑ NinjaFirewall</li> </ul>	Import configuration	File Check configuration will not be exported/imported.           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.
Dashboard Firewall Options Firewall Policies	Configuration backup	Available backup files           To restore NinjaFirewall's configuration to an earlier date, select it in the list and click 'Save Firewall Option's
Monitoring Anti-Malware Event Notifications	Miscellaneous	
Login Protection Logs	Dashboard Widget	Show the latest <b>4 (b)</b> security news on the dashboard widget. Set this value to 0 if you want to disable it.
WP+ Edition	Save Firewall Options	

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

Tirewall Options		
Your changes have been saved.		
Firewall protection	Enabled	

 ${\bf Step \ 7: \ go \ to \ NinjaFirewall-Event \ Notifications, \ now \ all \ events \ should \ be \ enabled}$ 

🖚 Dashboard	Fvent Natifications	
	WordPress admin dashboard	
<ul><li>Pages</li><li>Comments</li></ul>	Send me an alert whenever	An administrator logs in (default)     Someone - user, admin, editor, etc - logs in     No, thanks (not recommended)
<ul> <li>Appearance</li> <li>Plugins</li> <li>Users</li> </ul>	Plugins	
<ul><li>Tools</li><li>Settings</li></ul>	Send me an alert whenever someone	<ul> <li>✓ Uploads a plugin (default)</li> <li>✓ Installs a plugin (default)</li> </ul>
💮 NinjaFirewall		<ul> <li>✓ Activates a plugin</li> <li>✓ Updates a plugin</li> </ul>
Dashboard Firewall Options		<ul> <li>Ø Deactivates a plugin (default)</li> <li>Ø Deletes a plugin</li> </ul>
Firewall Policies Monitoring Anti-Malware	Themes	
Event Notifications	Send me an alert whenever someone	

Step 8: go to NinjaFirewall – Event Notifications and paste the contact email from step 2, save the form

🚺 NinjaFirewall	PHP backtrace
Dashboard Firewall Options Firewall Policies	Attach a PHP backtrace to important notifications     Medium verbosity (default) ~       Consult our blog for more info.
Monitoring	
Anti-Malware	Contact email
Event Notifications	
Login Protection	Alerts should be sent to notifications@example.com
Logs	Multiple recipients must be comma-separated (e.g., joe@example.org,alice@example.org ).
Security Rules	

Step 9: go to NinjaFirewall – Dashboard

Lusers	Firewall Dashboard	
Tools E Sottings	Firewall	Enabled
Settings	Mode	NinjaFirewall is running in WordPress WAF mode. For better protection, activate its Full WAF
🕡 NinjaFirewall		Activate Full WAF mode
Dashboard		
Firewall Options	Edition	WP Edition ~ Need more security? Explore our supercharged premium version: NinjaFirewall
Firewall Policies	Version	4.3.1 ~ Security rules: 2021-01-27.2
Monitoring		
Anti-Malware	PHP SAPI	FPM-FCGI ~ 7.3.25

Step 10: click on "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	
<ul> <li>Let NinjaFirewall make the necessary changes</li> <li>I want to make the changes myself.</li> </ul>	ges (recommended).	
✓ Enable the sandbox. If there were a problem during the installation, NinjaFirewall would undo those changes automatically for you.		
Finish Installation »		

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. <b>Please wait for 291 seconds</b> befor trying again (you can navigate away from this page and come back in a few minutes).	C) re

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



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

差 Tools	Firewall Dashboard	
II Settings	Firewall	Enabled
🚺 NinjaFirewall 🔹	Mode	NinjaFirewall is running in Full WAF mode.
Dashboard	Edition	WP Edition ~ <u>Need more security? Explore our supercharged premium version: NinjaFirewall (WP+ Edition)</u>
Firewall Options Firewall Policies	Version	4.2.1 ~ Security rules: 2020-06-26.1
Monitoring	PHP SAPI	FPM-FCGI ~ 7.3.15
Anti-Malware		

Step 14: go to NinjaFirewall – Monitoring

🖚 Dashboard	💓 Monitoring	
🖈 Posts		
93 Media	File Check File Guard	
Pages		
Comments	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 butto
🔊 Appearance	Create a snapshot of all files stored in that	/var/www/html/web/wp/
🖌 Plugins	directory	Default: /var/www/html/web/wp
👗 Users	Evolution the following files/folders (entional)	
🔎 Tools	Exclude the following files/folders (optional)	/app/nfwlog/
5 Settings		Full or partial case-sensitive string(s). Multiple values must be comma-separated ( , ).
		✓ Do not follow symbolic links (default)
MinjaFirewall		
Dashboard	Create Snapshot	
Firewall Options		
Firewall Policies		
Monitoring		
Anti-Malware		

## Step 15: create a snapshot

🚺 Monitoring		Help ¥
Snapshot successfully created.		٥
File Check File Guard		
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 Download Snapshot Delete Snapshot	
Last changes	None	

## Step 16: set scan schedule to daily $\mathbf{S}$

Options	
Enable scheduled scans	○ No (default)
	O Hourly
	◯ Twicedaily
	<ul> <li>Daily</li> </ul>
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.	Ø

Step 18: go to File Guard on the same page

Monitoring		
Your changes have been saved.		Ø
File Check File Guard		
Enable File Guard	Disabled	
Save File Guard options		

 ${\bf Step \ 19:}$  enable File Guard and click the save button

Monitoring		Help 🔻
Your changes have been saved.		O
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 colless than $10$ $\odot$ hour(s) ago.	reated
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 ( , )	
Save File Guard options	Full or partial case-sensitive string(s), max. 255 characters. Multiple values must be comma-separated ( , ).	

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

O D localhost:8080/wp-content/index.php?f=%00	☆
Sorry <b>127.0.0.1</b> , 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 ]	

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

<b>9</b> Medien	Firewall Log Live Log
📕 Seiten	Viewing: firewall 2022-02 (181 bytes)
Kommentare	
🔊 Design	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)
🖌 Plugins	
👗 Benutzer	
🖋 Werkzeuge	
🖪 Einstellungen	
NinjaFirewall	
Dashboard	
Firewall Options	
Firewall Policies	
Monitoring	
Anti-Malware	
Event Notifications	
Login Protection	
Logs	

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

<b>W</b> Login Protection	
Enable brute force attack protection	Enabled
Type of protection	Username + Password
	<ul> <li>Captcha image</li> </ul>
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