

Návod na aktivaci licence bezpečnostního pluginu WordFence Security

Poslední aktualizace 15 listopadu, 2024

[WordFence Security](#) patří mezi špičku mezi bezpečnostními WordPress pluginy. Proto jsme jej vybrali mezi ty pluginy, které na váš [WordPress hosting](#) instalujeme automaticky. Po instalaci je však ještě třeba jej aktivovat a nastavit.

Zde si povíme:

- jak aktivovat bezplatnou licenci WordFence Security
- jak tento WordPress plugin nastavit
- tipy na lepší zabezpečení webových stránek
- něco o pluginu WordFence na závěr

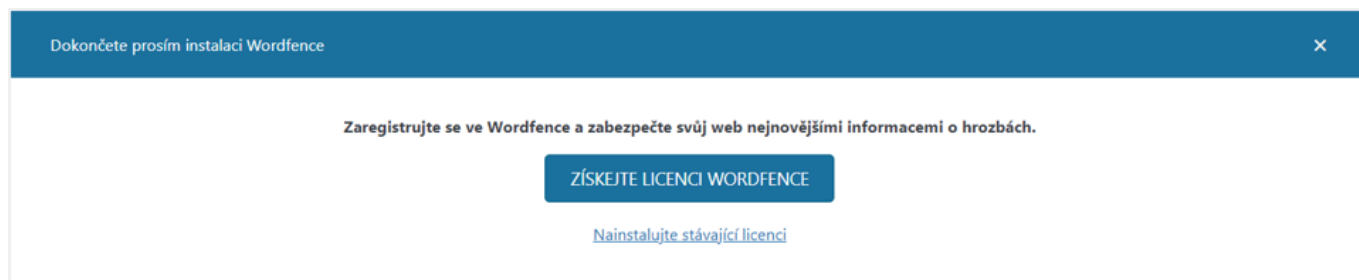
Chcete-li mít **WordFence v češtině** bude možná nutné jej nejprve aktualizovat. Po jeho instalaci si zkontrolujte, zda máte povolenou automatickou aktualizaci.

Aktivace bezplatné licence WordFence

Ve vašem WP adminu na vás po instalaci pluginu bude svítit upozornění, že je třeba instalaci ještě dokončit. WordFence totiž ještě vyžaduje registraci a aktivaci licence na stránkách výrobce.

K využívání pluginu vám ale vystačí bezplatná licence. Pro její získání stačí kliknout na modré tlačítko **Získejte licenci WordFence**.

Následně budete přesměrováni na stránky pluginu.



1. Na webu pluginu pokračujte kliknutím na tlačítko **Get a Free licence**.

Get Your Wordfence License

Wordfence FREE	Wordfence PREMIUM	Wordfence CARE
Free	\$119 per year	\$490 per year
Get a Free License	Buy Now	Buy Now
Join over 4 million secure	Get real-time firewall rules	For business owners who value their time. We install

2. Klikněte na souhlas se 30 denním zpožděním aktualizací databáze pluginu, což je vlastnost verze zdarma.

Are you sure you want delayed protection? ✕

Our firewall rules block exploits targeting WordPress plugins, themes and core. Our malware signatures detect whether your site has been compromised. We release firewall rules and malware signatures in real-time to our Premium customers.

For less than \$10 per month (paid annually) you can get real-time firewall rules and malware signatures as we release them. Are you sure you want the free version of Wordfence which receives firewall rules and malware detection 30 days later than our Premium customers?

[I'd like real-time protection!](#)

[I'm OK waiting 30 days for protection from new threats](#)



3. Zadejte svůj e-mail, na který se naváže FREE licence Wordfence a potvrďte akceptaci s pravidly a klikněte na tlačítko **Register**

Get Wordfence Free ✕

Site URL: <http://mailprome.cz>

Email

This is where you will receive your license key and any future security alerts for your website

Would you like WordPress security and vulnerability alerts sent to you via email?

Yes No

I have read and agree to the [Wordfence License Terms and Conditions](#), the [Services Subscription Agreement](#), and [Terms of Service](#), and have read and acknowledge the [Wordfence Privacy Policy](#).

Register

4. Do vaší e-mailové schránky vám od WordFence přijde potvrzovací e-mail. V e-mailu klikněte na **Install my license automatically**, to vás přenese zpět do Vašeho WordPressu.

Check your email ✕

You're almost done! Your license key has been sent to michalfoist@gmail.com. [Check your email to complete the installation.](#)

If you need additional help, you can visit [our documentation](#) to get help installing your license.

[Can't find the email?](#)



Wordfence <list@wordfence.com>
komu: mně ▾

10:17 (před 1 minutou)



Install Your Wordfence License

Thank you for registering for a Wordfence Free license. Your firewall rules and malware signatures will be delayed by 30 days with Wordfence Free edition.

[If you choose to upgrade to receive real-time firewall rules and malware signatures, you can click here to get Wordfence Premium.](#)

To complete the installation of Wordfence Free, you have two options.

Automatic Installation

Click the button below to automatically install the license key for <http://mailprome.cz>.

Install My License Automatically

5. Zde již jen potvrdíte instalaci licence kliknutím na **Nainstalovat licenci**.

Stránky
Komentáře
Vzhled
Pluginy
Uživatelé
Nástroje
Nastavení
Wordfence
Nástěnka
Firewall
Sken
Nástroje

Nainstalujte aplikaci Wordfence

Nainstalujte si licenci a dokončete aktivaci Wordfence.

E-mail

.....@gmail.com

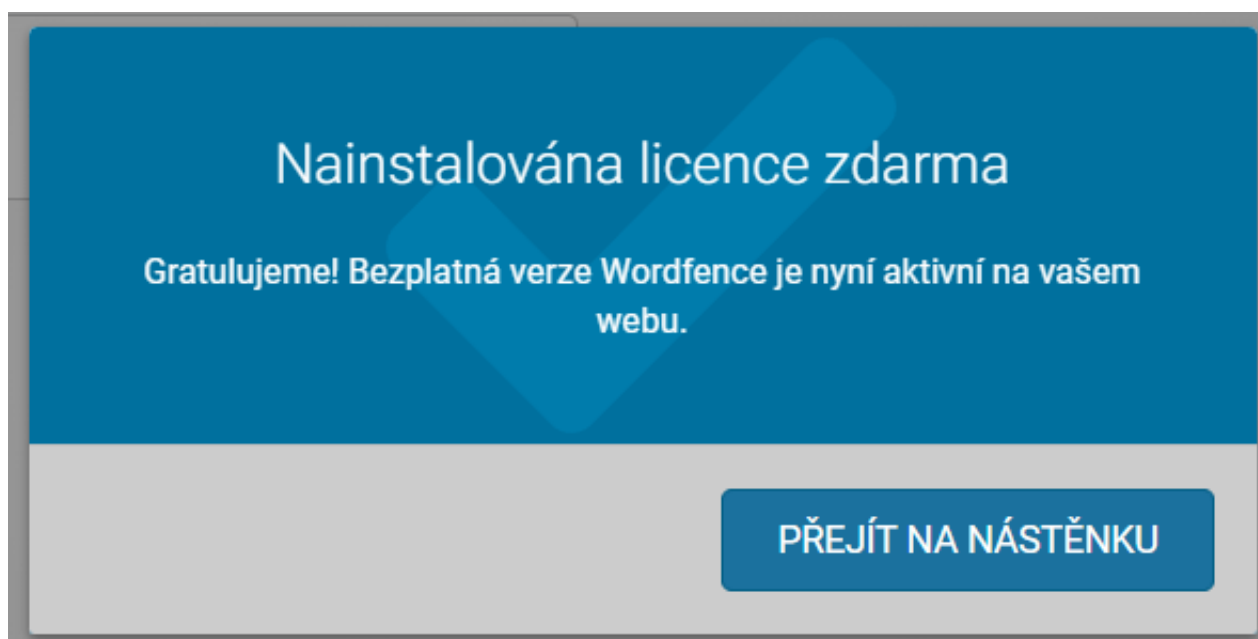
Zde budou zaslány budoucí bezpečnostní výstrahy pro váš web. To lze také změnit v globálních možnostech.

Licenční klíč

119f2bad91f7213ae5fb8d9c2f8720b226d459e8be9b93a3ff5e7b67dfdf4e0294eb813bb49733daca fdee39d416b8

NAINSTALOVAT LICENCI

6. Hotovo, máte nainstalovanou free licenci pluginu Wordfence.



Nyní můžeme přejít k základnímu nastavení pluginu.

Nastavení pluginu WordFence Security

Po nainstalování pluginu Wordfence a jeho aktivaci, která je popsána výše, doporučujeme pouze drobné přenastavení.

V základním nastavení je plugin také funkční, ale s drobnými úpravami dosáhnete lepší bezpečnosti.

Vše zvládnete sami, není to nijak složité.

1. Přejděte v levém menu Wordfence do nastavení **Všechny možnosti**.
2. Zde si můžete nastavit, jak chcete aby vám byly zasílány e-maily o různých aktivitách. Níže zobrazené nastavení je jedna z možností.

Předvolby upozornění e-mailem

Zašlete mi e-mail, když se Wordfence automaticky aktualizuje
Pokud máte povolené automatické aktualizace (viz výše), obdržíte e-mail, když dojde k aktualizaci.

Pokud je Wordfence deaktivován, pošlete mi e-mail

Pošlete mi e-mail, pokud je firewall webové aplikace Wordfence vypnutý

Upozornit na výsledky skenování této úrovně závažnosti nebo vyšší:

Upozornit, když je IP adresa blokována

Upozornit, když je někdo uzamčen pro přihlášení

Upozornit, když je někomu blokováno přihlašování kvůli použití hesla nalezeného při porušení

Upozornit, když se formulář „ztracené heslo“ použije pro platného uživatele

Upozornit, když se přihlásí někdo s přístupem správce

Upozornit, až když se tento administrátor přihlásí z nového zařízení nebo místa

Upozornit, když se přihlásí uživatel bez oprávnění správce

Upozornit, pouze když se uživatel přihlásí z nového zařízení nebo místa

Upozornit, když na mém webu bude zjištěn velký nárůst útoků

Maximální počet e-mailových upozornění odeslaných za hodinu
0 znamená, že budou zasílána neomezená upozornění.

3. Další nastavení je ochrana proti strojovému a robotickému prolamování hesel, tzv. **brute force attack**. Oproti původnímu nastavení lze například zvolit přísnější režim, tedy 3 pokusy a 1 hodinové zablokování.

Ochrana před Brute Force

Aktivujte ochranu brute force

Tato možnost povoluje všechny možnosti „Brute Force Ochrany“, včetně silného vynucování hesla a omezování neplatného přihlášení. Níže můžete upravit jednotlivé možnosti.

OFF ON

Uzamkněte po několika pokusech o neúspěšné přihlášení

3

Uzamkněte po několika pokusech o zapomenuté heslo

20

Počítejte selhání za jaké časové období

4 hodiny

Doba, po kterou je uživatel uzamčen

4 hodiny

4. Další část, kterou doporučujeme upravit je **Rate limit**. Opět se jedná o zvolení přísnějších hodnot, než je výchozí nastavení.

Omezení rychlosti

Povolte omezení rychlosti a pokročilé blokování

POZNÁMKA: Toto zaškrtnuté políčko povoluje VŠECHNY funkce blokování/omezení včetně IP, země a pokročilého blokování a níže uvedená „Pravidla omezení rychlosti“.

OFF ON

Jak bychom měli zacházet s prohlídači Google

Ověřené prohlídače Google nebudou nijak omezeny

Pokud někdo překročí požadavky

480 za minutu

pak

omezit

Pokud zobrazení stránky prohlídače překročí

480 za minutu

pak

omezit

Pokud stránky prohlídače, které nebyly nalezeny (404) překročí

120 za minutu

pak

omezit

Pokud zobrazení stránky člověka překročí

240 za minutu

pak

omezit

Pokud lidské stránky nenalezeny (404) překročí

120 za minutu

pak

omezit

Jak dlouho je IP adresa blokována, když poruší pravidlo

30 minut

Povolené URL adresy stránek 404

Tyto vzory adres URL budou vyloučeny z pravidel omezení používaných k omezení prohlídačů.

/favicon.ico
/apple-touch-icon*.png
/*@2x.png
/browserconfig.xml

5. Nastavení skenování WordFence doporučujeme přepnout na **standardní scan**, ne menší (to je vhodné zejména pro ty, kteří se technicky příliš neorientují v nastavení svého webhostingu a aktuální zátěže webových stránek).

Naplánovat skenování

Naplánujte skenování Wordfence

ZAKÁZÁNO POVOLENO

Nechat Wordfence zvolit, kdy bude Váš web skenován (doporučeno)

Ručně naplánujte skenování **Prémiová funkce**

Základní možnosti typu skenování

Limitovaný scan

Pro základní hostitelské plány. Poskytuje omezené možnosti detekce s velmi nízkým využitím zdrojů.

Standardní scan

Naše doporučení pro všechny webové stránky. Poskytuje nejlepší detekční schopnosti v oboru.

Vysoká citlivost

Pro majitele stránek, kteří si myslí, že mohli být napadeni hackery. Důkladnější, ale může vyvolat falešně pozitivní výsledky.

Vlastní scan

Vybráno automaticky, když byly pro tento web přizpůsobeny Obecné možnosti.

6. Dále upravte **Možnosti výkonu** na zaškrtnou hodnotu Použit skenování s nízkými zdroji, ať si nepřetěžujete svůj webhosting.

Možnosti výkonu

Použit skenování s nízkými zdroji (snižuje zatížení serveru prodloužením doby skenování)

Omezte počet problémů odeslaných v e-mailu s výsledky skenování
0 nebo prázdné znamená, že budou odeslány neomezené problémy

1000

Časový limit, který může skenování spustit během několika sekund
0 nebo prázdné znamená, že bude použito výchozí nastavení 3 hodiny

Kolik paměti by měl Wordfence při skenování vyžadovat
Velikost paměti v megabajtech

256

Maximální doba provedení pro každou fázi skenování
0 jako výchozí. Musí být 8 nebo vyšší a pro většinu serverů se doporučuje 10-20 nebo vyšší

0

Konec s nebezpečnou metodou pokus – omyl

Vyvarujte se nejčastějších chyb, které vám rozbíjí WordPress. Zaregistrujte se ZDARMA do Endora Academy a staňte experty na tvorbu webu.

[Zjistit více](#)

A to je vše!

Po prvních dnech a týdnech se neděste stavu, který uvidíte. Procenta Firewall a Scan zřejmě nebudou 100%, ale to nevádí.

Zjistíte, že na váš web útočí desítky hackerů a robotů týdně (a stovky až tisíce měsíčně). To je na internetu bohužel normální.

WordFence vám tyto útoky jednak reportuje, a jednak chrání váš web, aby útočníci nepronikli do jádra vašich webových stránek.

Drtivou většinu běžných internetových útoků plugin WordFence odvrátí a váš web ubrání.

Wordfence Protection ja aktivován

48%

Firewall

Ochrana před známými a vznikajícími hrozbami
Správa brány firewall

60%

Sken

Detekce bezpečnostních problémů
Spravovat skenování

Prémiová ochrana zakázána

Jako bezplatný uživatel Wordfence aktuálně používáte komunitní verzi kanálu Threat Defense. Uživatelé Premium jsou chráněni dalšími pravidly brány firewall a podpisy malwaru. Upgradujte na Premium ještě dnes a vylepšíte svoji ochranu.

[UPGRADE NA PREMIUM VERZI](#)

[DOZVĚDĚT SE VÍCE](#)

Oznámení 3

Wordfence Terms of Service and UK IDTA

Please review the updated Terms of Service with the new UK IDTA.

[TERMS OF SERVICE](#) [UK IDTA](#)

22 problémů nalezeno v nejnovějším skenování

K dispozici jsou aktualizace proWordPress (v6.2.2), 6 pluginů, a10 šablon

Stav Wordfence Central

Wordfence Central Vám umožňuje spravovat Wordfence na více webech z jednoho místa. Usnadňuje monitorování zabezpečení a konfiguraci Wordfence.

[Připojit tento web](#) [Navštívit Wordfence Central](#)

Nástroje

Živý provoz, vyhledávání Whois, Import/Export a diagnostika

Nápověda

Vyhledejte dokumentaci a nápovědu, kterou potřebujete

Globální možnosti

Spravujte globální možnosti Wordfence, jako jsou výstrahy, stav premium a další

Shrnutí brány firewall: Útoky blokované pro prcada.cz

Typ bloku	Komplex	Hrubou silou	Seznam blokovanych	Celkem
Dnes	36	15	—	51
Týden	55	27	—	82
Měsíc	55	36	—	91

[Premium](#)

[Jak jsou kategorizovány?](#)

Celkový počet blokovanych útoků: Síť Wordfence

24 hodin 30 dní

Celkový počet útoků

Placené verze WordFence vám nabídnou rozšířené možnosti funkcí, nastavení, reportingu i ochrany.

9 / 11

Tipy pro zabezpečení webových stránek obecně

Za prioritní bezpečnostní faktory pro WordPress weby považujeme:

- Pravidelné [aktualizace WordPressu](#).
- Používání ověřených a dobře hodnocených [šablon](#) a [pluginů](#).
- Aktualizace šablony.
- Aktualizace pluginů.
- Používání unikátního [uživatelského jména a hesla](#) pro přihlášení.
- Neukládání hesel kamkoliv do PC ani do internetových prohlížečů (typicky Chrome nabízí uložení). Používejte Password manager (např. [1password.com](#)).
- [Přihlašování do WordPressu](#) z bezpečných WiFi. V kavárnách atp. použijte minimálně [VPN](#).
- Používejte službu [Cloudflare](#) (vyžaduje trochu více technických znalostí při nastavování).
- Nainstalujte, aktivujte a použijte plugin WordFence Security.

A především, pravidelně [své webové stránky zálohujte](#).

Svůj web nikdy neukládejte na bezplatné webhostingy. Vždy používejte spolehlivý a bezpečný [WordPress hosting](#).

K čemu slouží Plugin WordFence Security

WordPress je nejrozšířenější redakční systém, a to je v tomto případě jeho nevýhodou – existuje více útočníků a robotů, kteří jsou zaměřené právě na webové stránky běžící na WordPressu.

Bezpečnostní WordPress plugin WordFence se vám postará o to, aby váš web byl chráněn proti hackerům, robotům a řadě dalších „útočných“ nástrojů.

Slouží jako firewall a malware scanner, jehož úkolem je chránit váš WordPress před napadením.

WordFence je zdarma a při základním nastavení nemá zvýšené nároky na webhosting, takže nemusíte platit ani nic extra za webhostingový tarif.

Má miliony stažení – jedná se o jeden z nejstahovanějších pluginů v celé knihovně WordPress vůbec.

WordFence navíc umí česky.

Nejdůležitější funkce pluginu WordFence

- 2FA: 2 fázová autentifikace
- Ověřování Captcha, ochrana formulářů
- Filtrování dle IP (zamezení přístupu dle IP, z různých zemí, atp.)
- Testování na napadení webu malwarem
- Firewall 24/7