

- Tableau de bord
- WP Jobsearch
- JobSearch Options
- Articles
- Médias
- Pages
- Commentaires
- FAQs
- MailPoet
- Apparence
- Extensions 1
- Comptes
- Outils
- Éditeur de page
- Réglages
- GPL Downloads
- WP Mail SMTP
- LayerSlider
- Membres
- Agent IA
- Speed Optimizer
- Security Optimizer
- Tableau de bord
- Sécurité du site
- Sécurité de connexion
- Journal d'activité
- Actions post-piratage
- Theme Options
- Loco Translate
- Replier le menu

Security Optimizer – Sécurité de connexion



La sécurité de la connexion est primordiale pour assurer la sécurité de votre site et de vos données. Utilisez les outils que nous avons réunis pour protéger votre WordPress wp-admin contre les visiteurs ou visiteuses non autorisés, les robots et autres attaques humaines ou automatisées.

Réglages de connexion

URL de connexion personnalisée

Les attaquants tentent souvent des exploits sur /wp-admin qui est l'URL de connexion par défaut de WordPress. Modifiez-la pour éviter ces attaques et disposer d'une URL de connexion facilement mémorisable.

CONFIGURER

Accès à la connexion

Par défaut, toutes les adresses IP peuvent accéder à votre compte WordPress. Vous pouvez utiliser cette fonctionnalité pour autoriser la connexion uniquement pour certaines IP ou à une série d'IP afin d'empêcher les attaques par force brute ou les tentatives de connexion malveillantes.

CONFIGURER

Authentification à deux facteurs pour les administrateurs/administratrices et les éditeurs/éditrices

L'authentification à deux facteurs oblige les administrateurs ou administratrices à se connecter uniquement après avoir fourni un jeton, généré à partir d'une application Authenticator. Si l'un de vos utilisateurs ou utilisatrices n'a plus accès à son application Authenticator et ne peut pas se connecter pour obtenir ses codes de sauvegarde, [cliquez ici](#) pour réinitialiser son authentification à deux facteurs.

Désactiver les identifiants courants

L'utilisation d'identifiants courants tels que « admin » constitue une menace pour la sécurité et entraîne souvent un accès non autorisé. En activant cette option, nous désactiverons la création d'identifiants courants et si vous avez déjà un ou plusieurs utilisateurs ou utilisatrices avec un identifiant faible, nous vous demanderons d'en créer un ou plusieurs nouveaux.

Limiter les tentatives de connexion

Limite le nombre de fois qu'un utilisateur ou utilisatrice peut tenter de se connecter à wp-admin avec des infos de connexions incorrectes. Lorsque la limite de tentatives de connexion est atteinte, l'IP d'où proviennent les tentatives est d'abord bloquée pendant une heure. Si les tentatives se poursuivent après la première heure, la limite sera alors fixée à 24 heures, puis à 7 jours.

5

