# Le gestionnaire de mots de passe auto-hébergé de Bitwarden

Gérez en toute sécurité vos identifiants professionnels et vos politiques de sécurité personnalisées sur votre propre serveur en hébergeant vous-même le gestionnaire de mots de passe Bitwarden.

Obtenez la vue interactive complète à https://bitwarden.com/fr-fr/self-hosted-password-manager-on-premises/

bitwarden

### Appliquer son propre modèle de sécurité

Placez votre installation Bitwarden derrière un proxy, un pare-feu et d'autres protections pour une plus grande sécurité des données.

### Contrôler les sauvegardes et la disponibilité

Les solutions basées sur les conteneurs de Docker ou de Kubernetes s'intègrent dans votre stratégie de haute disponibilité et de récupération existante, et dans le cadre de vos procédures établies.

### Personnaliser pour répondre à vos besoins

Répondez à vos exigences de conformité spécifiques et à vos politiques internes de résidence des données grâce à des variables d'environnement flexibles pour répondre à des besoins évolutifs.

## Le gestionnaire de mots de passe de confiance à la maison, au travail et en déplacement

### Accessibilité multiplateforme & appareils illimités

Accédez aux données critiques dans votre coffre depuis n'importe quel emplacement, navigateur et via un nombre illimité d'appareils

### Intégrer Bitwarden en toute transparence

Bitwarden s'intègre en toute transparence dans votre pile technologique existante grâce à des options d'intégration flexibles telles que les fournisseurs d'identité à authentification unique (SSO) et les services d'annuaire, y compris SCIM.

### Audit de sécurité & conformité

Open source, audité par une tierce partie, et conforme aux réglementations GDPR, Privacy Shield, HIPAA, et CCPA

### Synchronisation de répertoire

Utilisez le support SCIM ou le connecteur de répertoire pour rationaliser la provision et la synchronisation des utilisateurs et du groupe avec votre service de répertoire

### Rapports de santé du coffre

Accédez à des rapports perspicaces pour révéler des mots de passe faibles, réutilisés et d'autres mesures de sécurité utiles

### Support toujours actif

Les agents du service client sont disponibles pour vous aider à toute heure.

## Les avantages des gestionnaires de mots de passe auto-hébergés

### Une véritable souveraineté des données

Que les inquiétudes viennent du conseil d'administration ou de vos clients, avec l'auto-hébergement, la véritable souveraineté des données est une réalité.

### Conformité réglementaire

Si votre secteur d'activité, votre service ou votre produit a des exigences strictes en matière de conformité des données, le gestionnaire de mots de passe Bitwarden auto-hébergé coche une case importante en matière de conformité.

### Sécurité personnalisable

Ajustez les paramètres de sécurité en fonction de vos besoins. Adaptez chaque aspect de la sécurité de votre organisation, des variables d'environnement de l'auto-hébergement aux politiques du produit.

### Intégration transparente

La prise en charge des installations pour Windows, Linux, Docker ou Kubernetes, s'intègre à votre infrastructure informatique existante. Le serveur Bitwarden auto-hébergé est compatible avec tous les clients finaux, y compris les applications mobiles et de bureau et les extensions de navigateur. In-produit, intégration avec votre fournisseur d'identité, vos services d'annuaire, etc.

### Prêt pour l'audit et la conformité

Des journaux d'événements détaillés peuvent être ingérés par des outils SIEM par le biais d'intégrations ou d'API afin de suivre l'activité des utilisateurs et de garantir la conformité avec vos politiques internes et les réglementations externes. Les résultats des audits effectués par des tiers, les rapports SOC 2 et d'autres informations relatives à la conformité de l'application sont publiés et mis à jour chaque année.

---

## Bénéficiez d'une sécurité de pointe et d'un contrôle total de vos données.

Rendez votre expérience en ligne plus sûre, plus rapide et plus agréable en hébergeant vous-même le gestionnaire de mots de passe Bitwarden.

---

## FAQ

Plus de FAQ sur l'auto-hébergement ici

- Quels sont les avantages de l'utilisation d'un gestionnaire de mots de passe auto-hébergé ?

1. **Une véritable souveraineté des données**: L'auto-hébergement d'un gestionnaire de mots de passe vous donne un contrôle total sur vos données. Vous gérez votre propre serveur, en veillant à ce que les mots de passe et les informations d'identification sensibles soient stockés sur l'infrastructure que vous contrôlez.

2. **Sécurité renforcée**: Avec une solution auto-hébergée, vous pouvez appliquer votre propre modèle de sécurité. Placez votre installation de gestion des mots de passe derrière des proxys et des pare-feux pour une protection supplémentaire.

3. **Personnalisation**: Les gestionnaires de mots de passe auto-hébergés offrent souvent des variables d'environnement flexibles, ce qui vous permet de personnaliser la configuration pour répondre à vos besoins spécifiques et aux exigences de conformité.

4. **Avantages de l'open source**: La confiance et la transparence sont essentielles lorsqu'il s'agit de choisir un gestionnaire de mots de passe à auto-héberger. Bitwarden étant un gestionnaire de mots de passe open source, les mesures de sécurité sont auto-vérifiables et chaque ligne de code est régulièrement inspectée par des milliers d'experts et de passionnés de sécurité dans le monde entier.

5. **Conformité réglementaire**: L'auto-hébergement peut aider à répondre aux exigences strictes en matière de conformité des données dans divers secteurs, car vous avez un contrôle total sur la résidence et l'accès aux données.

6. **Intégration avec les systèmes existants**: Les solutions auto-hébergées permettent souvent une intégration transparente avec votre infrastructure informatique actuelle, y compris les services d'annuaire et les fournisseurs d'identité.

7. **Préparation à l'audit**: Accédez à des journaux d'événements détaillés pour suivre l'activité des utilisateurs, ce qui peut s'avérer crucial pour les audits internes et le maintien de la conformité.

- **Quelles sont les plateformes sur lesquelles je peux héberger ?**

  Les clients Bitwarden sont multiplateformes, et le serveur peut être déployé dans des conteneurs Docker sur Windows, Linux, ou dans Kubernetes avec l'utilisation d'une carte Helm.

  Docker Desktop sur Windows peut nécessiter une licence selon que votre entreprise répond ou non aux exigences de Docker en matière de licences, mais Docker sur Linux est gratuit.

  Pour en savoir plus sur Docker et les technologies de conteneurs, consultez le site web de Docker.

- **Comment déployer Bitwarden sur AWS, Azure, GCP ou VMware vCenter ?**

  Bitwarden dispose de guides approfondis pour le déploiement d'installations Docker dans la documentation d'aide. Des instructions pour l'installation sur AWS EKS, OpenShift et Azure AKS à l'aide de Helm sont également disponibles. Vous trouverez ci-dessous des ressources recommandées pour vous aider à démarrer :

  - Guides de déploiement Docker
  - Guides de déploiement de Helm
  - Comment héberger soi-même une organisation Bitwarden

- Comment installer un gestionnaire de mots de passe open source sur mon propre serveur ?

  La mise en place d'un gestionnaire de mots de passe open source sur votre propre serveur implique généralement les étapes suivantes

  1. **Préparez votre serveur**: Assurez-vous que vous disposez d'un serveur ou d'une machine virtuelle. Il peut s'agir d'un matériel sur site ou d'un serveur en nuage.
  2. **Sélectionnez la méthode de déploiement**: De nombreux gestionnaires de mots de passe auto-hébergés proposent plusieurs options d'installation. Les plus courantes sont les suivantes :
     - Conteneurs Docker
     - Déploiements Kubernetes
  3. **Installation**: Explorez la documentation détaillée de l'auto-hébergement Bitwarden pour différents types de déploiement.
  4. **Configuration**: Définir des variables d'environnement et ajuster les paramètres en fonction des exigences de sécurité et des besoins de l'organisation.
  5. **Gestion des utilisateurs**: Créer des comptes d'administrateur et configurer les droits d'accès des utilisateurs.
  6. **Configuration du client**: Installez des extensions de navigateur, des applications de bureau et des applications mobiles pour vos utilisateurs, en veillant à ce qu'elles soient configurées pour se connecter à votre serveur auto-hébergé.
  7. **Test**: Testez minutieusement l'installation, y compris les fonctions telles que le générateur de mot de passe, le partage sécurisé et l'authentification multifactorielle.
  8. **Plan de maintenance**: Établissez des procédures de sauvegardes régulières, de mises à jour et d'audits de sécurité pour que votre gestionnaire de mots de passe auto-hébergé reste sûr et à jour.

  **N'oubliez pas que si l'auto-hébergement offre de nombreux avantages, il nécessite également une maintenance permanente et une vigilance en matière de sécurité.** Assurez-vous que vous disposez des ressources et de l'expertise nécessaires pour gérer efficacement une solution auto-hébergée.