SECRETS MANAGER > COMMENCEZ

Connectez-vous à Secrets Manager

Connectez-vous à Secrets Manager

Le compte Bitwarden chiffré de bout en bout avec zéro connaissance que vous utilisez pour vous connecter au gestionnaire de mots de passe sera le même que celui que vous utilisez pour vous connecter à Secrets Manager.

> **Tip**
>
> Cet article concerne la connexion au coffre web de Secrets Manager. Le CLI de Secrets Manager, qui est principalement utilisé pour scripter l'injection de secrets dans vos applications et infrastructures, nécessite de se connecter avec un jeton d'accès.

Mot de passe principal

Votre mot de passe principal est la méthode principale pour accéder à votre compte Bitwarden. Il est important que votre mot de passe principal soit :

- **Mémorable** : les employés et les systèmes de Bitwarden n'ont aucune connaissance, aucun moyen de récupérer ou de réinitialiser votre mot de passe principal. **N'oubliez pas votre mot de passe principal !**
- **Fort** : Un mot de passe principal plus long, plus complexe et moins courant est le meilleur moyen de protéger votre compte. Bitwarden fournit un outil gratuit de test de la force du mot de passe pour tester la force de certains mots de passe mémorables que vous envisagez.

> **Tip**
>
> Inquiet à propos de l'oubli de votre mot de passe principal ? Voici ce qu'il faut faire :
>
> - **Configurez un indice**. Au cas où vous auriez besoin d'un rappel, un courriel d'indice pour le mot de passe principal peut être demandé sur l'écran d'identifiant. Assurez-vous d'utiliser un indice que seul vous comprendrez.
> - **Désignez un** contact d'urgence de confiance. Les utilisateurs avec un accès Premium peuvent accorder l'accès à un compte à un ami ou à un membre de la famille en cas d'urgence.

Apprenez comment changer votre mot de passe principal, ou que faire si vous avez oublié votre mot de passe principal.

Authentification à deux facteurs

L'utilisation de l'identification en deux étapes (également appelée authentification à deux facteurs ou 2FA) pour protéger votre compte Bitwarden empêche un acteur malveillant d'accéder à vos données même s'il découvre votre mot de passe principal en exigeant une authentification à partir d'un appareil secondaire lorsque vous vous connectez.

Il existe de nombreuses méthodes différentes pour l'identifiant en deux étapes, allant des applications d'authentification dédiées aux clés de sécurité matérielles. Quel que soit votre choix, Bitwarden recommande vivement de sécuriser votre coffre en utilisant l'identifiant en deux étapes.

Méthodes gratuites

Bitwarden offre plusieurs méthodes d'identifiant en deux étapes gratuitement, y compris :

Méthode	Instructions de configuration
via une application d'authentification (par exemple, Authy ou Google Authenticator)	Cliquez ici.
via courriel	Cliquez ici.
via un Authentificateur WebAuthn FIDO	Cliquez ici.

Méthodes Premium

Pour les utilisateurs Premium (y compris les membres des organisations payantes), Bitwarden propose plusieurs méthodes avancées d'identifiant en deux étapes :

Méthode	Instructions de configuration
via Duo Security avec Duo Push, SMS, appel téléphonique, et clés de sécurité	Cliquez ici.
via YubiKey (tout appareil de série 4/5 ou YubiKey NEO/NFC)	Cliquez ici.

Se connecter avec l'appareil

Saviez-vous que vous pouvez vous connecter à l'application web Bitwarden en utilisant un appareil secondaire au lieu de votre mot de passe principal? Se connecter avec un appareil est une approche sans mot de passe pour l'authentification, éliminant le besoin d'entrer votre mot de passe principal en envoyant des demandes d'authentification à tout appareil spécifique sur lequel vous êtes actuellement connecté pour approbation. En savoir plus.

Authentification unique

Si votre organisation utilise l'identifiant avec SSO, vous pouvez accéder à votre application web Bitwarden en utilisant vos identifiants fédérés SSO.