

PASSWORD MANAGER > COMMENCEZ

Application Web de Gestionnaire de Mots de Passe

Afficher dans le centre d'aide:

<https://bitwarden.com/help/getting-started-webvault/>

Application Web de Gestionnaire de Mots de Passe

L'application web Bitwarden offre l'expérience Bitwarden la plus riche pour les utilisateurs personnels et les organisations. De nombreuses fonctions importantes telles que la configuration de l'[identifiant en deux étapes](#) ou l'administration d'une [organisation](#) doivent être effectuées à partir du coffre web.

Tip

L'application web est accessible depuis n'importe quel navigateur web moderne à vault.bitwarden.com et vault.bitwarden.eu. Si vous **hébergez vous-même** Bitwarden, l'accès au coffre web sera situé sur votre [domaine configuré](#), par exemple <https://my.bitwarden.server.com>.

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		My Mailing Address Brett Warden	Me	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login username	My Organiz...	⋮

Application web de gestionnaire de mots de passe

Lorsque vous vous connectez pour la première fois à votre application Web, vous arriverez sur la vue **Tous les coffres**. Cet espace listera tous les éléments du coffre, y compris les [identifiants](#), [cartes de paiement](#), [identités](#) et [notes sécurisées](#).

Premiers pas

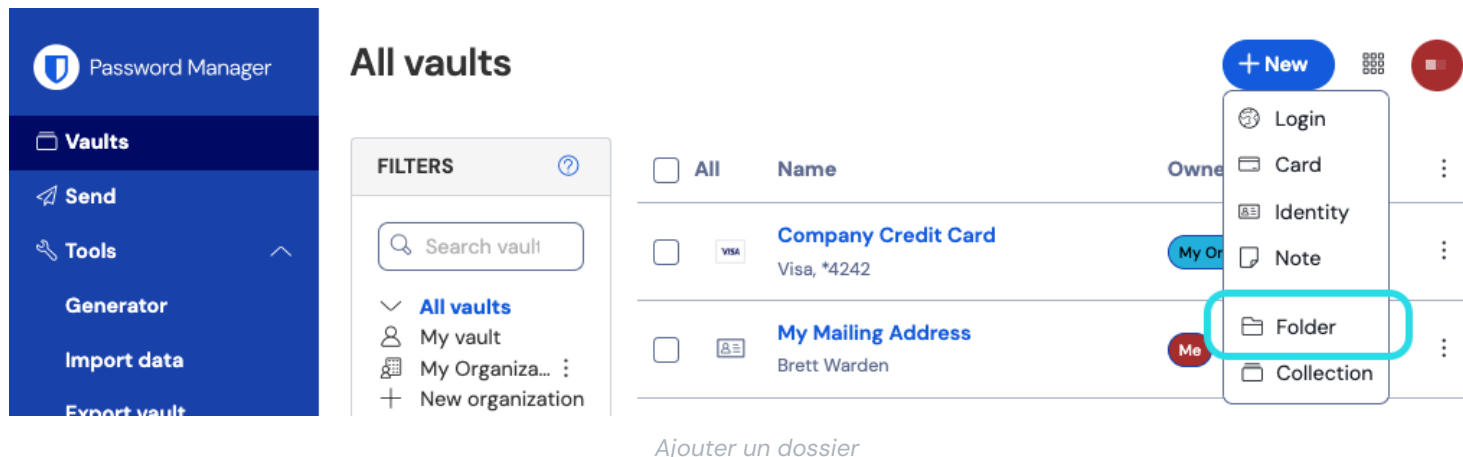
Dans la capture d'écran précédente, la vue **Tous les coffres** affiche **Tous les éléments** dans tous les coffres. Les membres des [organisations](#) auront d'autres coffres répertoriés ici. En utilisant la colonne **Filtres**, vous pouvez organiser votre coffre en **Favorites** et **Dossiers**.

Commençons par configurer un nouveau dossier et ajouter un nouvel identifiant à celui-ci :

Créer un dossier

Pour créer un dossier :

1. Sélectionnez le bouton + **Nouveau** et choisissez **Dossier** dans le menu déroulant:



2. Entrez un nom (par exemple, **Identifiants des réseaux sociaux**) pour votre dossier et sélectionnez **Enregistrer**.

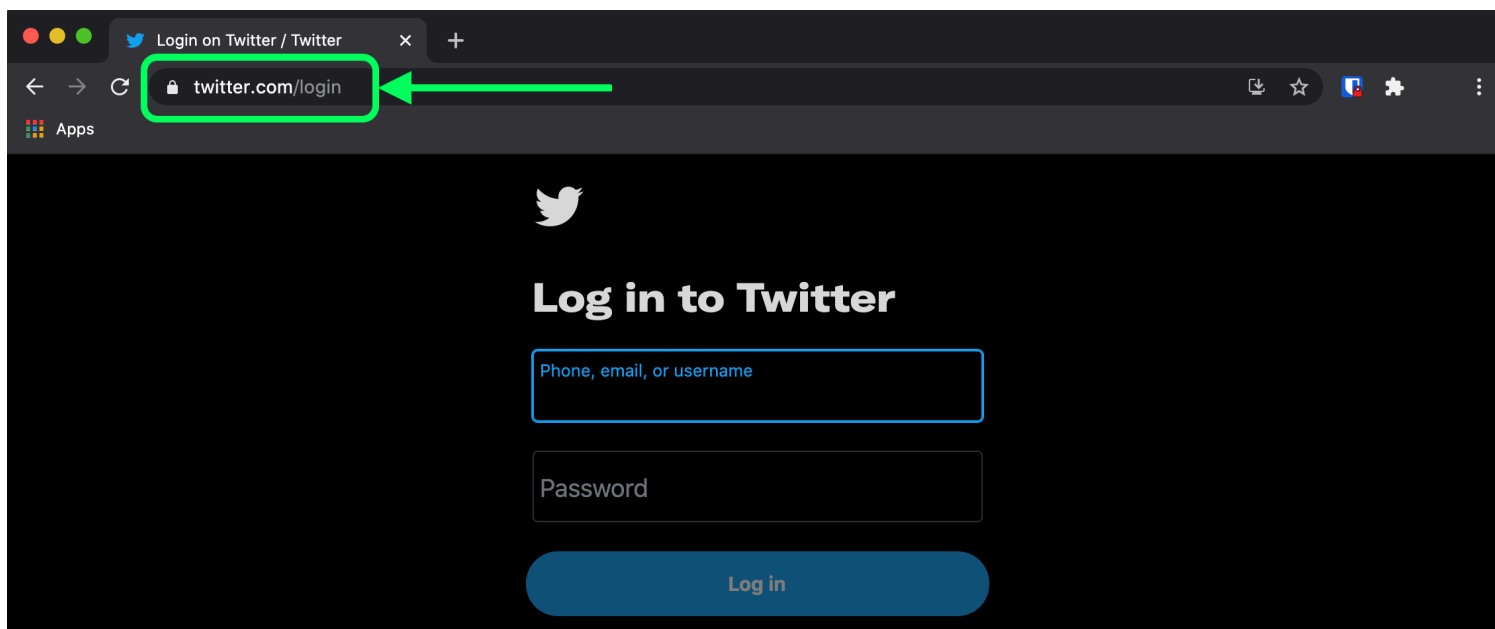
Tip

Pour un coffre plus propre, vous pouvez imbriquer des dossiers à l'intérieur d'autres dossiers.

Ajouter un identifiant

Pour ajouter un nouvel élément d'identifiant :

1. Sélectionnez le bouton + **Nouveau** et choisissez **Élément** dans le menu déroulant.
2. Sélectionnez **Identifiant** dans le menu déroulant (si vous ajoutez une carte de paiement, une identité ou une Note sécurisée à la place, sélectionnez cette option à la place).
3. Entrez un **Nom** pour l'élément. Les noms vous aideront à identifier facilement les éléments dans votre coffre, alors donnez à cet élément un nom reconnaissable (par exemple, **Mon Compte Twitter**).
4. Entrez votre **nom d'utilisateur** et votre **mot de passe**. Pour l'instant, entrez votre mot de passe existant. Nous vous aiderons à le remplacer par un mot de passe plus fort plus tard.
5. Dans le champ **URI 1**, entrez l'URL du site web (par exemple, <https://twitter.com/identifiant>). Si vous ne savez pas quelle URL utiliser, naviguez jusqu'à l'écran d'identifiant du site web et copiez-la depuis votre barre d'adresse.



Trouver une URI

6. Dans le menu déroulant **Dossier**, sélectionnez le nom du dossier dans lequel vous souhaitez ajouter cet élément (par exemple, le dossier **Identifiants des Réseaux Sociaux** que nous avons créé précédemment).

Sélectionnez l'icône ☆ **Favori** pour ajouter cet élément à vos favoris. L'icône se remplira (☆ → ★) lorsqu'il s'agit d'un favori.

7. Bon travail ! Sélectionnez le bouton **Enregistrer** pour terminer l'ajout de cet élément.

Générer un mot de passe fort

Maintenant qu'un nouvel identifiant est enregistré dans votre coffre, améliorez sa sécurité en remplaçant le mot de passe existant par un plus fort :

1. Dans votre coffre, sélectionnez l'élément que vous souhaitez sécuriser.
2. Dans un nouvel onglet ou fenêtre, ouvrez le site Web correspondant et connectez-vous à votre compte avec votre identifiant.

💡 Tip

Si vous avez entré quelque chose dans le champ **URI 1**, cliquez sur l'icône **Lancer** pour l'ouvrir directement depuis votre coffre.

3. Sur ce site web, naviguez vers la zone où vous pouvez **Changer votre mot de passe**.

Typiquement, vous pouvez trouver cela dans une section **Votre Compte**, **Sécurité**, **Paramètres de Connexion**, ou **Paramètres d'Identifiant**.

4. La plupart des sites web vous demandent d'abord d'entrer votre **mot de passe actuel**. Retournez à votre coffre et sélectionnez l'icône **Copier** à côté du champ **Mot de passe**. Ensuite, retournez sur le site web et collez-le dans le champ **Mot de passe actuel**.

Vous avez peut-être mémorisé l'ancien mot de passe, mais il est bon de prendre l'habitude de copier et coller votre mot de passe. Voici comment vous allez vous connecter une fois que votre mot de passe sera remplacé par un plus fort.

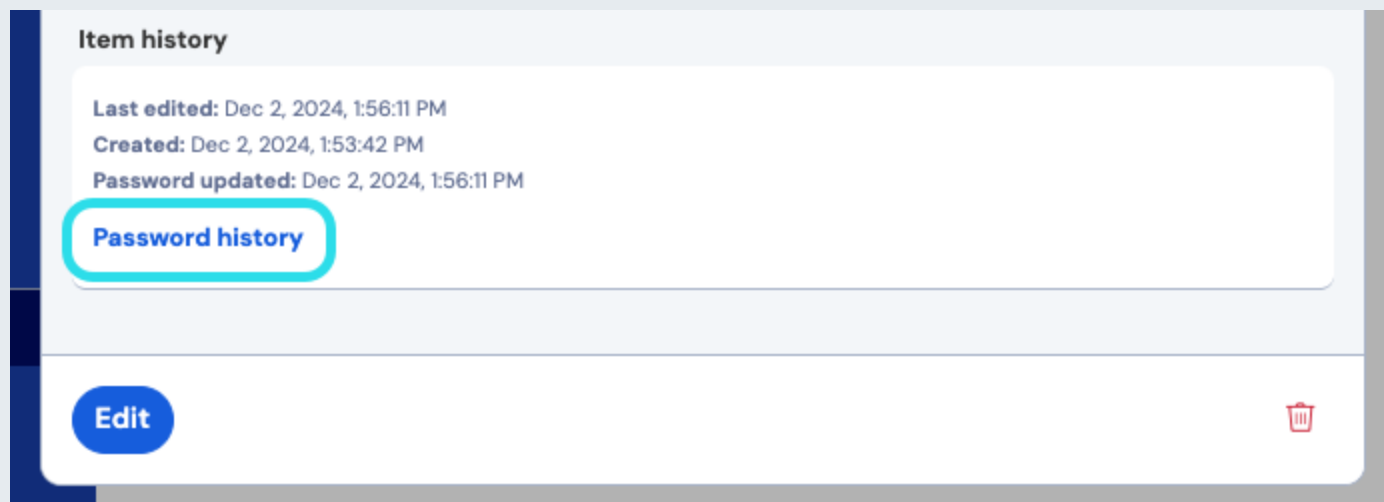
5. Retournez à votre coffre et cliquez sur l'icône **Générer** à côté du champ **Mot de passe**. On vous demandera si vous voulez écraser le mot de passe actuel, alors sélectionnez **Oui** pour continuer.

Cela remplacera votre **mot de passe** par un mot de passe fort généré aléatoirement. Passer d'un mot de passe comme **Fido1234 à X@Ln@x9J@&u@5n##B** peut arrêter un pirate informatique.

6. Copiez votre nouveau mot de passe avec le même icône  **Copier** que vous avez utilisé précédemment, et sélectionnez le bouton **Enregistrer**.

Tip

Ne vous inquiétez pas de réécrire votre mot de passe existant ! Si quelque chose ne va pas, Bitwarden conserve un **Historique des mots de passe** des cinq derniers mots de passe pour chaque identifiant :



Afficher l'historique des mots de passe

7. Retournez sur l'autre site web et collez votre mot de passe fort dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**.

8. Une fois que vous avez **Enregistré** le changement de mot de passe, vous avez terminé !

Importez votre donnée

Bonne nouvelle ! Vous n'avez pas besoin de répéter ce processus pour chaque identifiant si vous avez des noms d'utilisateur et des mots de passe enregistrés dans un navigateur web ou autre gestionnaire de mots de passe. Utilisez l'un de nos guides d'importation spécialisés pour vous aider à transférer vos données depuis :

- [LastPass](#)
- [1Password](#)
- [Dashlane](#)
- [macOS & Safari](#)
- [Google Chrome](#)
- [Firefox](#)

Sécurisez votre coffre

Maintenant que votre coffre est plein de données, prenons quelques mesures pour le protéger en mettant en place un identifiant à deux étapes. La connexion en deux étapes vous oblige à vérifier votre identité lors de la connexion en utilisant un jeton supplémentaire, généralement récupéré à partir d'un autre appareil.

Il existe de nombreuses [méthodes disponibles](#) pour l'identifiant en deux étapes, mais la méthode recommandée pour un compte Bitwarden gratuit est d'utiliser une application d'authentification sur appareil mobile telle que [Authy](#) :






1. Téléchargez Authy sur votre appareil mobile.
2. Dans l'application web Bitwarden, sélectionnez **Paramètres** → **Sécurité** → **Identifiant en deux étapes** à partir de la navigation :

The screenshot shows the Bitwarden web interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, My account, Security (highlighted), Preferences, Domain rules, Emergency access, and Free Bitwarden Famili... At the top right of the main content area, there's a 'Security' header with tabs for 'Master password', 'Two-step login' (selected), and 'Keys'. Below the tabs, the 'Two-step login' section is titled and includes a warning box with a yellow border and a warning icon. The warning text states that setting up two-step login can lock the user out of their account and that a recovery code is essential. A 'View recovery code' button is located below the warning. Underneath, the 'Providers' section lists five options, each with an icon, a description, and a 'Manage' button: Email (envelope icon), Authenticator app (phone and screen icon), Passkey (key icon), Yubico OTP security key (Yubico logo), and Duo (Duo logo).

Authentification à deux facteurs

3. Localisez l'option **Application d'Authentification** et sélectionnez **Gérer** :

Providers

	Email Enter a code sent to your email.	Manage
	Authenticator app Enter a code generated by an authenticator app like Bitwarden Authenticator.	Manage
	Passkey Use your device's biometrics or a FIDO2 compatible security key.	Manage
	Yubico OTP security key Use a YubiKey 4, 5 or NEO device.	Manage
	Duo Enter a code generated by Duo Security.	Manage

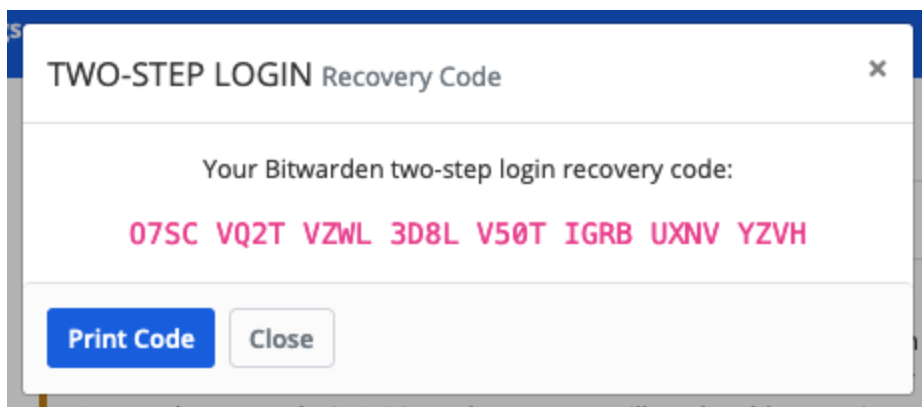
Sélectionnez le bouton Gérer

Vous serez invité à entrer votre mot de passe principal pour continuer.

4. Sur votre appareil mobile, ouvrez Authy et appuyez sur le bouton + **Ajouter un compte**.
5. Scannez le code QR situé dans votre coffre web en utilisant Authy. Une fois scanné, Authy affichera un code de vérification de six chiffres.
6. Entrez le code de vérification à six chiffres dans la boîte de dialogue de votre application Web, et sélectionnez le bouton **Activer**.
7. Sélectionnez le bouton **Fermer** pour revenir à l'écran d'identifiant en deux étapes, et sélectionnez le bouton **Afficher le Code de récupération**.

Votre code de récupération peut être utilisé dans l'éventualité où vous perdez votre appareil mobile. **Il s'agit d'une étape essentielle pour garantir que vous ne serez jamais bloqué hors de votre coffre-fort**, alors ne la sautez pas !

8. Entrez votre mot de passe principal et sélectionnez le bouton **Continuer** pour obtenir votre Code de récupération.



Exemple de Code de récupération

Enregistrez votre code de récupération de la manière qui vous semble la plus logique. Croyez-le ou non, imprimer votre code de récupération et le garder dans un endroit sûr est l'une des meilleures façons de s'assurer que le code n'est pas vulnérable au vol ou à la suppression involontaire.

Prochaines étapes

Félicitations pour avoir maîtrisé les bases de Bitwarden ! Nous voulons que tout le monde soit en sécurité en ligne, donc nous sommes fiers de proposer tout ce que vous avez appris ici gratuitement.

Inscrivez-vous pour le premium

Pour les utilisateurs personnels, nous proposons un abonnement Premium à 10 \$ / an qui déverrouille des capacités avancées, notamment :

- Options avancées d'identification en deux étapes, comme [Duo](#) et [les clés de sécurité YubiKey](#)
- Espace de stockage pour les [fichiers joints cryptés](#)
- Un [Authentificateur de Mot de Passe Unique Temporaire \(TOTP\)](#) intégré
- [Accès d'urgence](#) à votre coffre-fort par des contacts d'urgence de confiance
- [Rapports sur l'état du coffre-fort](#) qui rendent compte de l'hygiène des mots de passe et de la sécurité

Pour commencer un abonnement Premium, sélectionnez le bouton **Go Premium** de votre **affichage des coffres** !

Commencez une organisation

Avez-vous besoin de partager des mots de passe ou d'autres éléments de coffre avec vos amis, votre famille, votre équipe ou toute votre entreprise?

Les organisations Bitwarden vous permettent de faire exactement cela. Nous recommandons d'essayer la fonctionnalité de partage de mot de passe des organisations en [commençant une organisation gratuite pour deux personnes](#).

Une fois que vous avez testé une organisation, consultez notre page [Tarifs Bitwarden](#) pour en savoir plus sur les différents types d'organisation que vous pourriez envisager.