

Procédure - Mise en place du gestionnaire de mots de passe

[Dépôt GitHub](#)



Informations générales

- **Date de création** : 23/01/2026
- **Dernière modification** : 23/01/2026
- **Auteur** : MEDO Louis

Sommaire

- A. Présentation des gestionnaires de mot de passe.
- B. Mise en place de Bitwarden.

A. Présentation des gestionnaires de mot de passe

1. Pourquoi cela existe ?

Le cerveau humain n'est pas conçu pour mémoriser des dizaines de mots de passe complexes et uniques qui ne contiennent pas de mots du dictionnaire.

Cependant, pour s'en souvenir, les utilisateurs ont tendance à utiliser des mots de passe simples (pass123, admin...) ou à réutiliser le même partout.

Ce qui génère un risque : si un site est piraté et que les mots de passe n'ont pas été correctement hachés, tous vos comptes sont compromis.

Pour répondre à ce risque, nous avons créé le gestionnaire de mot de passe qui va agir comme un coffre-fort numérique. Vous ne retenez qu'une seule clé (le mot de passe maître), et le logiciel génère et retient les autres pour vous.

2. Les différents types d'architectures des gestionnaires de mots de passe.

Client-serveur (exemple : BitWarden, Passbolt)

- **Fonctionnement** : les mots de passe sont chiffrés sur votre appareil puis envoyés sur un serveur distant (cloud).
- **Avantage** : synchronisation automatique entre les différents supports (PC, smartphone...)

Standalone / Local (exemple : Keepass)

- **Fonctionnement** : la base de données est un fichier chiffré stocké uniquement sur votre disque dur ou clé USB.
- **Avantage** : contrôle total des données, pas d'exposition sur Internet. Cependant, pas de synchronisation native.

Pour cette solution, il faut faire attention à maintenir une sauvegarde de sa base de données en utilisant la règle du 3-2-1.

3. Notions de sécurité

Le gestionnaire de mots de passe utilise un mot de passe appelé **Maître**, c'est la clé qui permet d'ouvrir votre coffre-fort. En conséquence, il doit être long (16 caractères), avoir des caractères spéciaux, des majuscules, des chiffres et vous ne devez pas le réutiliser ailleurs.

Il faut également faire attention à ne pas le perdre : s'il est perdu, les données sont irrécupérables, les gestionnaires de mots de passe fonctionnent avec une architecture "zéro connaissance". Cependant, certains gestionnaires de mots de passe proposent de générer des clés de récupération que vous pouvez stocker sur une clé USB chiffrée par exemple.

Ne pas mettre tous ses œufs dans le même panier.

Certains gestionnaires de mots de passe proposent de stocker vos codes de double authentification A2F dans Bitwarden. Cependant, je déconseille d'utiliser ces fonctionnalités qui

peuvent paraître très pratiques au quotidien, mais qui constituent en fait un risque en cas de compromission de votre coffre-fort. Si un attaquant accède à votre gestionnaire de mot de passe, il pourra être en capacité d'accéder à l'entièreté de vos comptes même avec une double authentification. Pour remédier à ce risque, je conseille d'utiliser une application dédiée comme FreeOTP ou Aegis.

B. Mise en place de Bitwarden dans votre groupe.

Nous allons mettre en place la solution Bitwarden dans les groupes d'AP. Cette solution nous permet d'avoir un espace entreprise qui va contenir les mots de passe de vos projets tout en ayant chacun vos identifiants de connexion (principe de non-répudiation).

Prérequis

- Une adresse email valide par étudiant.

1. Création du compte Bitwarden (Binômes)

1.1 Inscription au service. Se rendre sur <https://vault.bitwarden.com/#/register>. Remplir l'adresse email et le nom.

1.2 Définition de la Phrase de Passe Maître. Au lieu d'un mot de passe complexe court (ex: Tr0uB4douR&3), nous utiliserons une **phrase de passe** (4 à 5 mots aléatoires).

Exemple valide : `cheval-corRect-batterie7-agRafe3`

1.3 Vérification. Une fois le compte créé, connectez-vous. Un bandeau vous demande de vérifier votre email. Cliquez sur le lien reçu par courriel pour débloquer l'accès complet.

2. Durcissement du compte (Binômes)

2.1 Activation de la Double Authentification (A2F). Dans le coffre Web, aller dans **Paramètres du compte > Sécurité > Identification en deux étapes**.

- Cliquez sur "Gérer" pour **Authenticator App**.
- Scannez le QR Code avec votre smartphone.
- Saisissez le code à 6 chiffres pour valider.

2.2 Sauvegarde du code de récupération. Une fois l'A2F activée, Bitwarden affiche un **Code de récupération**.

- **Action :** Imprimez ce code ou écrivez-le sur papier et stockez-le en lieu sûr (physique).

2.3 Vérification. Déconnectez-vous totalement. Tentez de vous reconnecter : le site doit vous demander votre mot de passe maître **PUIS** le code à 6 chiffres de votre téléphone.

3. Configuration de l'Organisation (Partage)

3.1 Initialisation de l'Organisation. Dans le menu, cliquez sur "**New Organization**" (ou "Share your passwords").

- **Nom** : AP-[NomProjet]
- **Email de facturation** : Votre email.
- **Plan** : Choisir "Free" (Gratuit).

3.1 Création des Collections. Allez dans l'onglet **Gérer > Collections**. Créez une collection pour partager vos mots de passe :

- AP (pour tous vos identifiants utilisés durant les différentes situations professionnelles)

Une **Collection** est un conteneur administré par l'organisation qui permet de regrouper des identifiants partagés et d'y appliquer des permissions d'accès spécifiques (lecture, écriture) pour chaque utilisateur.

3.3 Ajouter votre binôme. Invitez votre binôme via **Personnes > Inviter**, sélectionnez `Admin` comme rôle pour qu'il puisse créer et modifier les mots de passe également. Ensuite, dans **Collections** ajoutez le à la collection **AP** avec les droits d'édition. Enfin, cliquez sur les **trois petits points > confirmer** dans l'interface de gestion des membres

Notes

- **Principe de moindre privilège** : Ne donnez les droits "Admin" à votre collègue que si c'est strictement nécessaire. Sinon, le droit "Utilisateur" suffit.