bitwarden | Article du Centre d'Aide

PASSWORD MANAGER > ADMINISTRATION DES CHAMBRES FORTES

Rapports sur la santé des chambres fortes

Afficher dans le centre d'aide:
https://bitwarden.com/help/reports/

Rapports sur la santé des chambres fortes

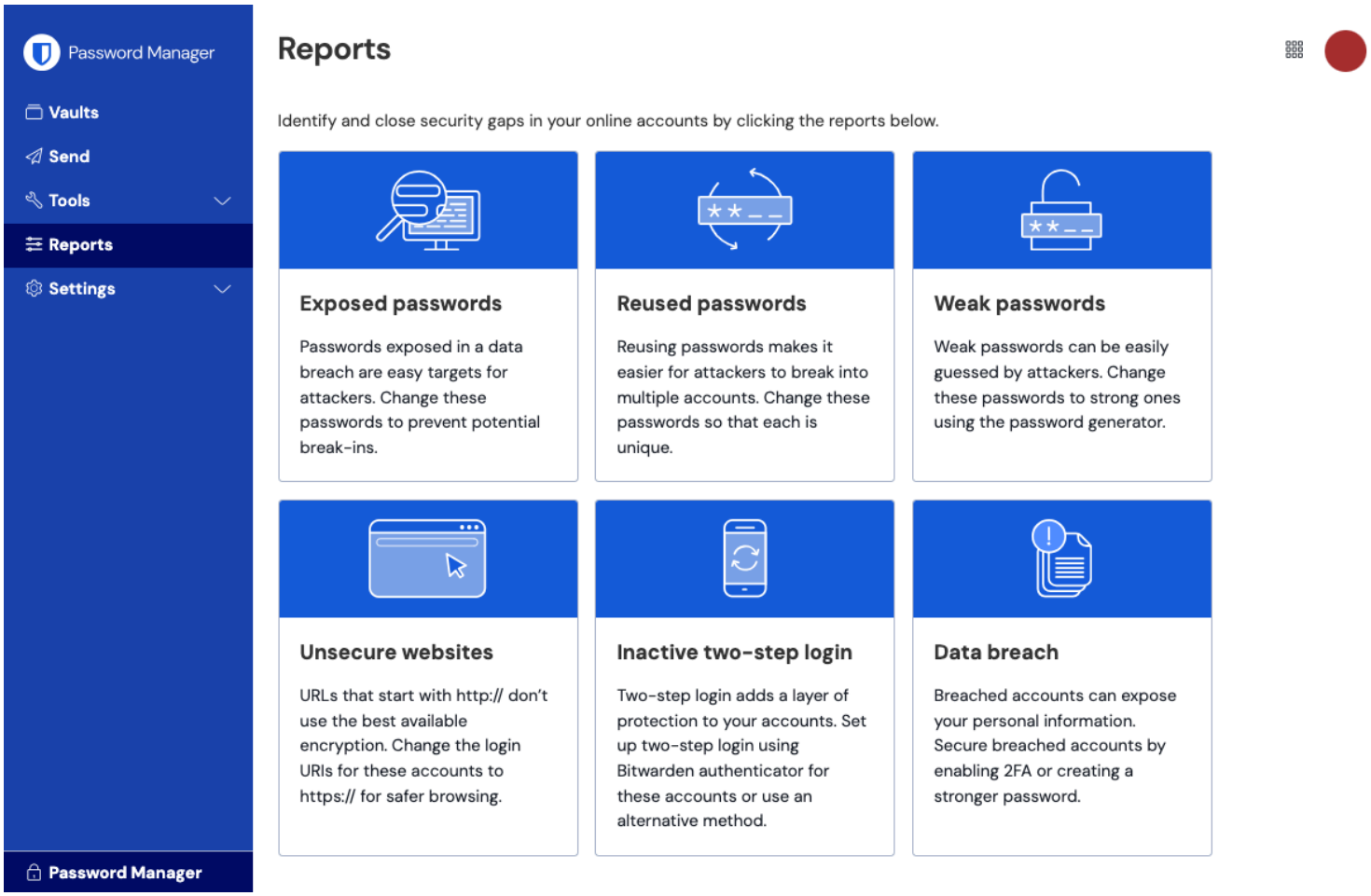
Les rapports de santé du coffre peuvent être utilisés pour évaluer la sécurité de votre coffre individuel ou d'organisation Bitwarden. Les rapports, par exemple le rapport sur les mots de passe réutilisés et les mots de passe faibles, sont exécutés localement sur votre client. Cela permet d'identifier les éléments offensants, sans que Bitwarden n'ait jamais accès à des versions non cryptées de ces données.

> **Note**
>
> La plupart des rapports de santé du coffre ne sont disponibles que pour les utilisateurs Premium, y compris les membres des organisations payantes (Familles, Équipes ou Entreprise), mais le rapport de brèche de données est gratuit pour tous les utilisateurs.

Afficher un rapport

Pour exécuter tout rapport de santé de coffre pour votre **coffre individuel** :

1. Connectez-vous à l'application Web et sélectionnez **Rapports** de la navigation:



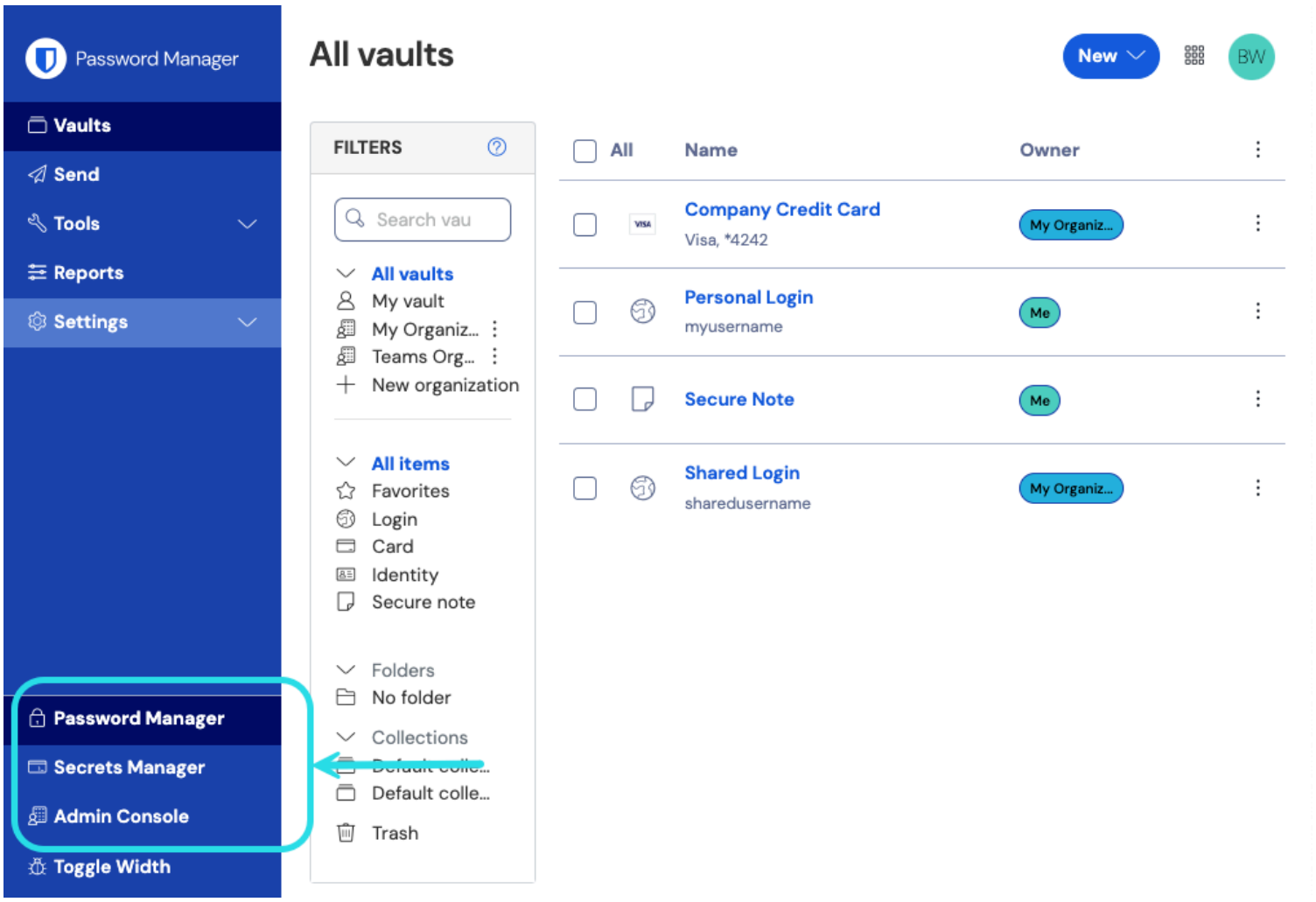
Page de rapport

2. Choisissez un rapport à exécuter.

Pour exécuter tout rapport de santé de coffre pour votre **coffre d'organisation** :

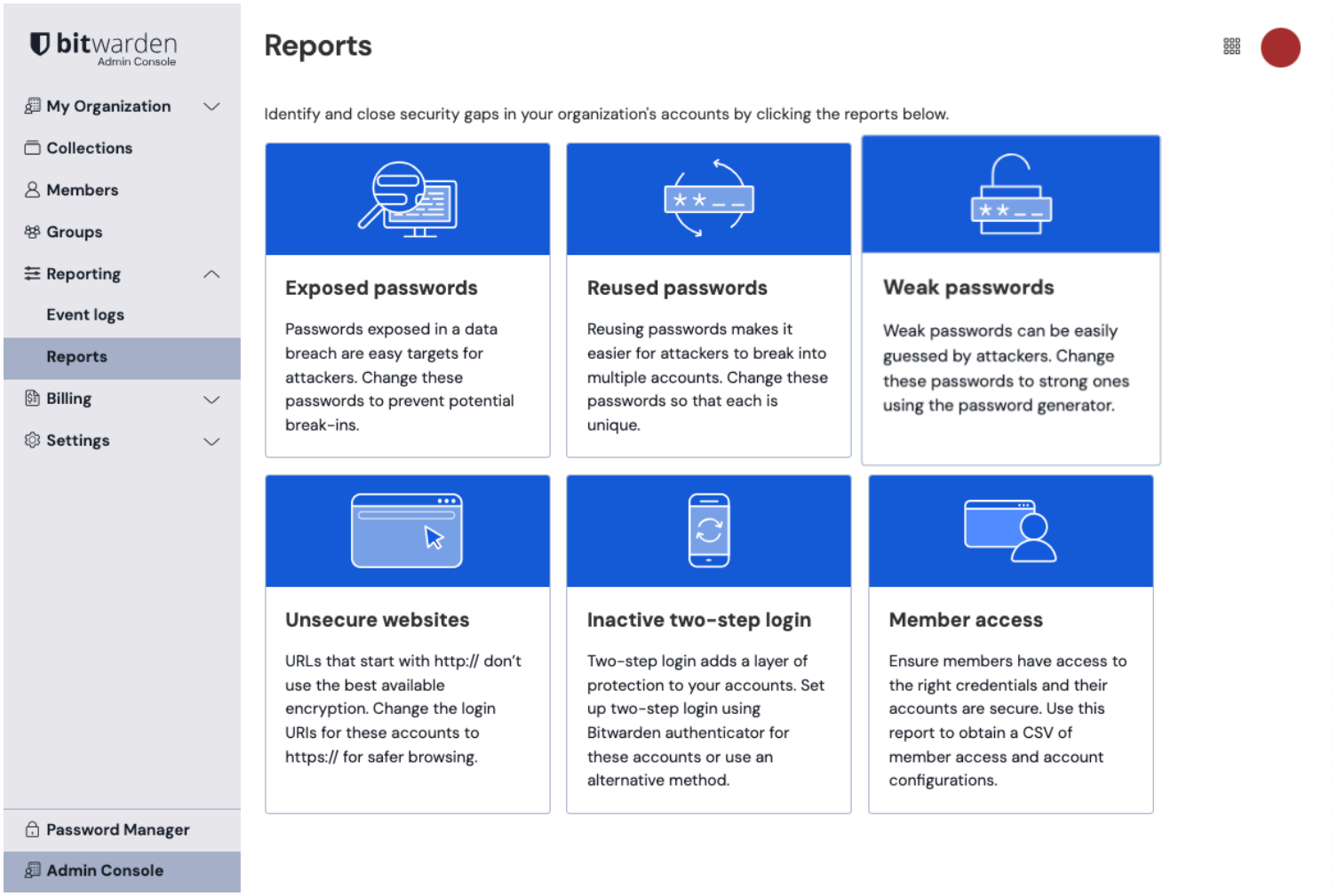
1. Connectez-vous à l'application web Bitwarden.

2. Ouvrez la console Admin en utilisant le sélecteur de produit (⊞):



commutateur-de-produit

3. Dans votre organisation, sélectionnez **Rapport** → **Rapports** dans la navigation



Rapports d'organisation

4. Choisissez un rapport à exécuter.

Rapports disponibles

Rapport sur les mots de passe exposés

Le rapport sur les mots de passe exposés identifie les mots de passe qui ont été découverts dans des brèches de données connues qui ont été rendues publiques ou vendues sur le dark web par des pirates.

Ce rapport utilise un service web de confiance pour rechercher les cinq premiers chiffres du hachage de tous vos mots de passe dans une base de données de mots de passe connus pour avoir été divulgués. La liste correspondante de hachages renvoyée est ensuite comparée localement avec le hachage complet de vos mots de passe. Cette comparaison est uniquement effectuée localement pour préserver votre k-anonymat.

Une fois identifié, vous devriez créer un nouveau mot de passe pour les comptes ou services offensants.

> **Tip**
>
> Pourquoi utiliser les cinq premiers chiffres des hachages de mot de passe ?
>
> Si le rapport est effectué avec vos mots de passe réels, peu importe qu'ils aient été exposés ou non, vous les divulgueriez volontairement au service. Le résultat de ce rapport ne signifie pas nécessairement que votre compte a été compromis, mais plutôt que vous utilisez un mot de passe qui a été trouvé dans ces bases de données de mots de passe exposés, mais vous devriez éviter d'utiliser des fuites et des mots de passe non uniques.

Rapport sur les mots de passe réutilisés

Le rapport sur les mots de passe réutilisés identifie les mots de passe non uniques dans votre coffre. La réutilisation du même mot de passe pour plusieurs services peut permettre aux pirates d'accéder facilement à plus de vos comptes en ligne lorsque un service est violé.

Une fois identifié, vous devriez créer un mot de passe unique pour les comptes ou services offensants.

Rapport sur les mots de passe faibles

Le rapport sur les mots de passe faibles identifie les mots de passe faibles qui peuvent facilement être devinés par les pirates et les outils automatisés utilisés pour craquer les mots de passe, classés par gravité de la faiblesse. Ce rapport utilise zxcvbn pour l'analyse de la force du mot de passe.

Une fois identifié, vous devriez utiliser le générateur de mot de passe Bitwarden pour générer un mot de passe fort pour les comptes ou services offensants.

Rapport sur les sites Web non sécurisés

Le rapport sur les sites Web non sécurisés identifie les éléments d'identifiant qui utilisent des schémas non sécurisés (`http://`) dans les URI. Il est beaucoup plus sûr d'utiliser `https://` pour crypter les communications avec TLS/SSL. Pour en savoir plus, consultez l'utilisation des URI.

Une fois identifiés, vous devriez changer les URI offensants de `http://` à `https://`.

Rapport 2FA inactif

Le rapport Inactif 2FA identifie les éléments d'identifiant où :

- L'authentification à deux facteurs (2FA) via TOTP est disponible depuis le service
- Vous n'avez pas stocké une clé d'authentificateur TOTP

L'authentification à deux facteurs (2FA) est une étape de sécurité importante qui aide à sécuriser vos comptes. Si un site web le propose, vous devriez toujours activer le 2FA. Les éléments offensants sont identifiés en croisant les données URI avec les données de https://2fa.directory/.

Une fois identifié, configurez le 2FA en utilisant l'hyperlien `Instructions` pour chaque élément offensant :

Instructions du rapport

Rapport de brèche de données (coffres individuels uniquement)

Le rapport de brèche de données identifie les données compromises (adresses de courriel, mots de passe, cartes de paiement, date de naissance, et plus) dans les brèches connues, en utilisant un service appelé Have I Been Pwned (HIBP).

Lorsque vous créez un compte Bitwarden, vous aurez l'option d'exécuter ce rapport sur votre mot de passe principal avant de décider de l'utiliser. Pour exécuter ce rapport, un hachage de votre mot de passe principal est envoyé à HIBP et comparé aux hachages exposés stockés. Votre mot de passe principal n'est jamais exposé par Bitwarden.

Une "violation" est définie par HIBP comme "un incident où les données sont involontairement exposées dans un système vulnérable, généralement en raison de contrôles d'accès insuffisants ou de faiblesses de sécurité dans le logiciel". Pour plus d'informations, référez-vous à la documentation FAQ de HIBP.

Note

Si vous auto-hébergez Bitwarden, afin d'exécuter le rapport de brèche de données sur votre instance, vous devrez acheter une clé d'abonnement HIBP qui vous autorisera à faire des appels à l'API, obtenue ici.

Une fois que vous avez la clé, ouvrez votre `./bwdata/env/global.override.env` et REMPLACEZ la valeur des espaces réservés pour `globalSettings__hibpApiKey` avec votre clé API achetée :

```
Bash

globalSettings__hibpApiKey=REPLACE
```

Pour plus d'informations, voir configurer les variables d'environnement.