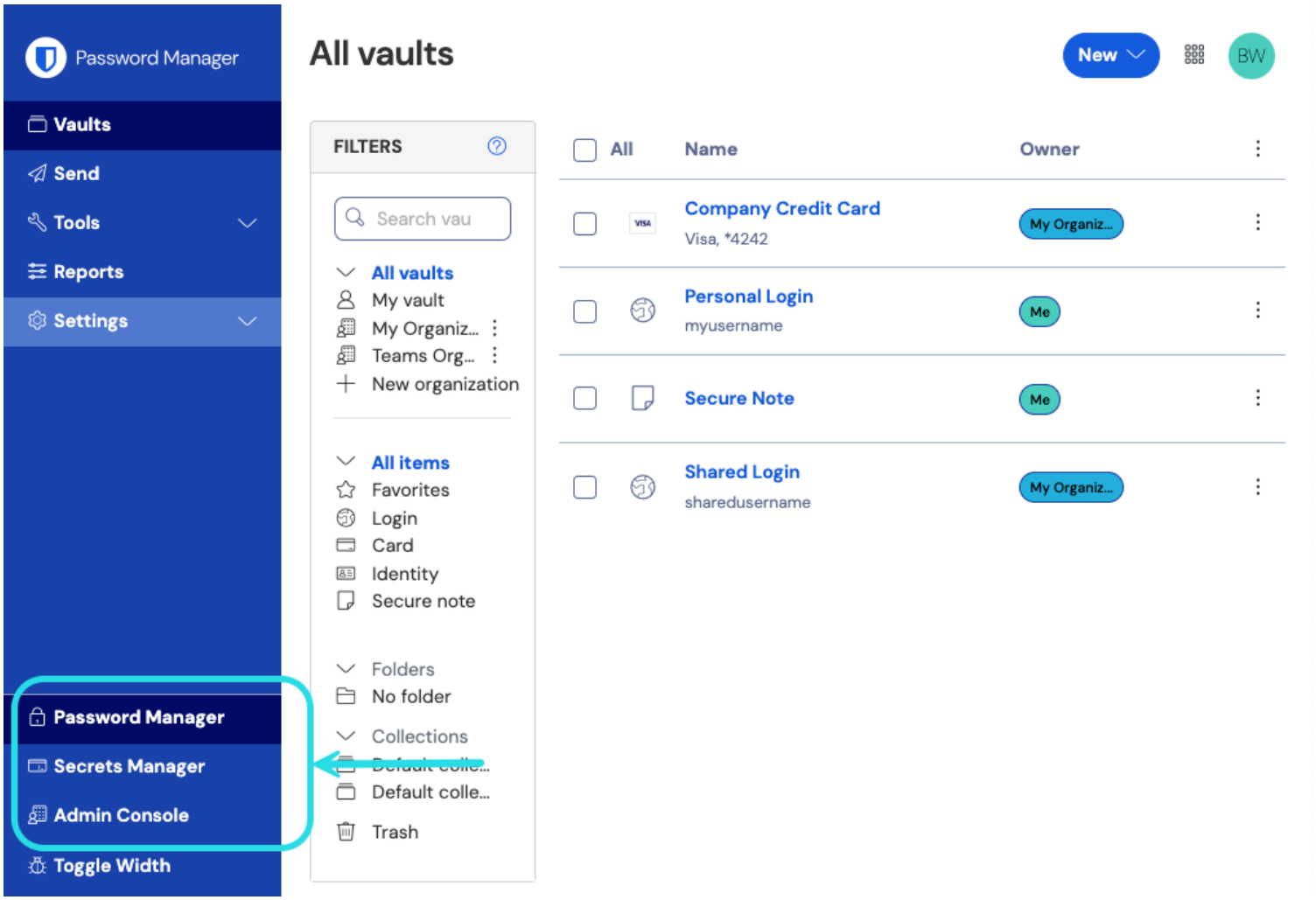
Configurer le SSO avec des appareils de confiance

Configurer le SSO avec des appareils de confiance

Ce document vous guidera à travers l'ajout de SSO avec des appareils de confiance à votre organisation. Vous devez être un propriétaire d'organisation ou un admin pour accomplir ces étapes :

1. Connectez-vous à l'application web Bitwarden et ouvrez la console Admin en utilisant le sélecteur de produit (⊞):



commutateur-de-produit

2. Sélectionnez **Paramètres** → **Politiques de sécurité** dans la navigation.

3. Sur la page des politiques de sécurité, activez les politiques de sécurité suivantes qui sont nécessaires pour l'utilisation des appareils de confiance :

   - La politique de la **seule organisation**.
   - La politique de sécurité **Exiger l'authentification unique**.
   - La politique de l'**administration de récupération de compte**.
   - La politique d'administration de récupération de compte **Exige que les nouveaux membres soient inscrits automatiquement** option.

> **Note**
> Si vous n'activez pas ces politiques de sécurité au préalable, elles seront automatiquement activées lorsque vous activerez l'option de déchiffrement du membre **Appareils de confiance**. Cependant, si certains comptes n'ont pas activé la récupération de compte, ils devront s'inscrire eux-mêmes avant de pouvoir utiliser l'approbation de l'admin pour les appareils de confiance. Les utilisateurs qui activent la récupération de compte doivent se connecter au moins une fois après la récupération du compte pour terminer complètement le processus de récupération de compte.

4. Sélectionnez **Paramètres** > **Connexion unique** dans la navigation. Si vous n'avez pas encore configuré SSO, suivez l'un de nos guides d'aide pour la mise en œuvre de SAML 2.0 ou de OIDC.

5. Sélectionnez l'option **Appareils de confiance** dans la section des options de déchiffrement des membres.

Une fois activé, les utilisateurs peuvent commencer à décrypter leurs coffres avec un appareil de confiance.

Si votre objectif est d'avoir des membres sans mot de passe principal qui peuvent **uniquement** utiliser des appareils de confiance, demandez aux utilisateurs de sélectionner **Se connecter** → **SSO d'Entreprise** à partir de l'invitation de l'organisation pour initier la provision JIT. Les admins/propriétaires devraient toujours utiliser l'option **Créer un compte** afin qu'ils aient des mots de passe principaux pour des raisons de redondance et de basculement.

> **Warning**
> La migration du SSO avec des appareils de confiance vers d'autres options de déchiffrement des membres n'est pas actuellement recommandée :
>
> - Si pour une raison quelconque votre organisation doit revenir à l'option de déchiffrement par mot de passe principal pour ses membres, à partir du chiffrement par appareil de confiance, **vous devez** émettre des mots de passe principaux en utilisant la récupération de compte **à tous les utilisateurs** intégrés sans ceux-ci **pour préserver l'accès à leurs comptes.** Les utilisateurs doivent ensuite se connecter entièrement suite à la récupération du compte du mot de passe principal afin de compléter le flux de travail.
>
> - Passer de SSO avec des appareils de confiance à Key Connector n'est pas pris en charge.

Changement de l'option de déchiffrement des membres de Appareils de confiance à Mot de passe principal

Modifier l'option de déchiffrement des membres de Appareils de confiance à Mot de passe principal sans émettre de mots de passe principaux entraînera le verrouillage du compte utilisateur. Pour effectuer ce changement de politiques de sécurité, vous devez :

1. Émettez des mots de passe principaux à l'aide de la récupération de compte.

2. Les utilisateurs doivent se connecter au moins une fois après la récupération du compte afin de terminer complètement le flux de travail et d'éviter le verrouillage.

Si l'option de déchiffrement du membre a été modifiée sans émettre de mot de passe principal, les trois options suivantes restent pour les utilisateurs :

- Suivez le flux de travail supprimer-récupérer.

- Restaurer le compte à partir d'une sauvegarde de compte/organisation.

- Créez un nouveau compte ou organisation.