bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > PLUS

Guide de Migration des Équipes et de l'Entreprise

Afficher dans le centre d'aide:
https://bitwarden.com/help/teams-enterprise-migration-guide/

Guide de Migration des Équipes et de l'Entreprise

La migration sécurisée de votre organisation avec Bitwarden est simple et sécurisée. Suivez simplement les étapes de ce guide pour migrer les données et les utilisateurs de votre gestionnaire de mots de passe existant :

1. Exportez vos données .
2. Créez et configurez votre organisation Bitwarden.
3. Importez vos données dans Bitwarden .
4. Intégrez vos utilisateurs .
5. Configurer l'accès aux collections et aux éléments du coffre-fort .

> **Tip**
> If you need assistance during your migration, our Customer Success team is here to help!

Portée

Ce document décrit les meilleures pratiques pour migrer les données sécurisées de votre/vos gestionnaire(s) de mots de passe actuel(s) vers une organisation Bitwarden Équipes ou Entreprise, en construisant une infrastructure de sécurité basée sur des méthodes simples et évolutives.

La gestion des mots de passe est cruciale pour la sécurité organisationnelle et l'efficacité opérationnelle. Fournir des informations sur les meilleures méthodes pour effectuer la migration et la configuration est conçu pour minimiser l'approche d'essai et d'erreur qui est souvent nécessaire lors de l'échange d'outils d'entreprise.

Les étapes dans ce document **sont énumérées dans l'ordre recommandé** pour faciliter l'utilisation et une intégration en douceur pour les utilisateurs.

Étape 1: Exportez vos données

Exporter des données d'un autre gestionnaire de mots de passe sera différent pour chaque solution, et dans certains cas, cela peut être un peu délicat. Utilisez l'un de nos Guides d'Importation & d'Exportation pour obtenir de l'aide, par exemple pour exporter depuis Lastpass ou 1Password.

La collecte d'une exportation complète de vos données peut nécessiter l'attribution de dossiers ou d'éléments partagés à un seul utilisateur pour l'exportation, ou la réalisation de plusieurs exportations entre utilisateurs avec les autorisations appropriées. De plus, les données exportées peuvent inclure des données individuellement possédées ainsi que des données partagées / organisationnelles, alors assurez-vous de supprimer les éléments individuels du fichier d'exportation avant d'importer dans Bitwarden.

> **Note**
>
> We recommend paying special attention to the location of the following types of data during export:
>
> - Secure documents
> - Secure file attachments
> - Secure notes
> - SSH / RSA key files
> - Shared folders
> - Nested shared items
> - Any customized structures within your password management infrastructure

Étape 2 : Configurez votre organisation

Les organisations Bitwarden relient les utilisateurs et les éléments du coffre ensemble pour le partage sécurisé des identifiants, des notes, des cartes de paiement et des identités.

> **Tip**
>
> It's important that you create your organization first and import data to it directly, rather than importing the data to an individual account and then moving items to the organization secondarily.

1. **Créez votre organisation**. Commencez par créer votre organisation. Pour apprendre comment, consultez cet article.

   > **Note**
   >
   > To self-host Bitwarden, create an organization on the Bitwarden cloud, generate a license key, and use the key to unlock organizations on your server.

2. **Intégrer les utilisateurs administratifs** . Avec votre organisation créée, les procédures de configuration supplémentaires peuvent être facilitées en intégrant certains utilisateurs administratifs. Il est important que vous ne commenciez pas à **intégrer les utilisateurs finaux** à ce stade, car il reste quelques étapes pour préparer votre organisation. Apprenez comment inviter des admins ici.

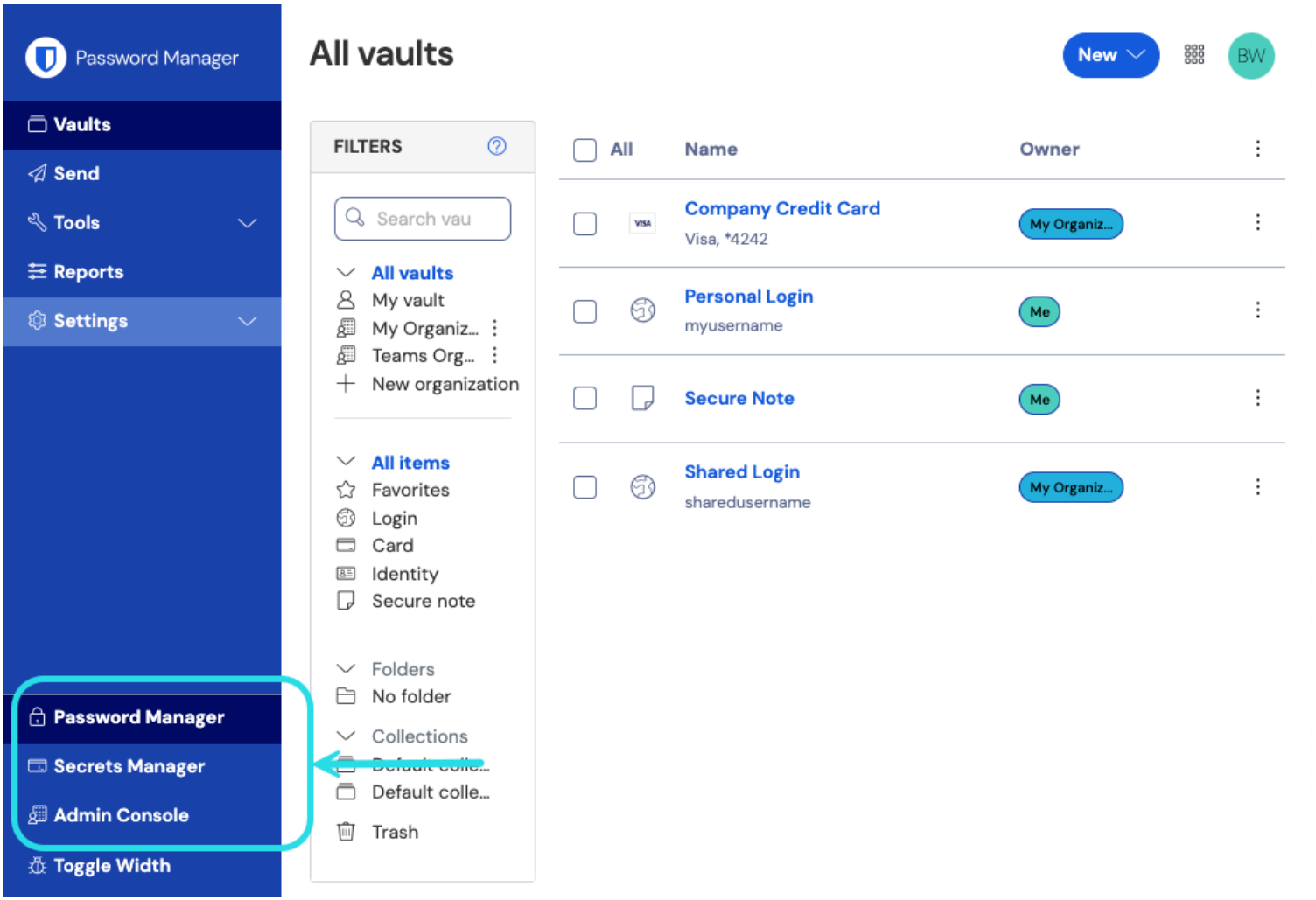
3. **Configurer les services d'identité** . Les organisations d'entreprise prennent en charge la connexion avec l'authentification unique (SSO) en utilisant soit SAML 2.0, soit OpenID Connect (OIDC). Pour configurer SSO, ouvrez l'écran **Paramètres** → **Authentification unique** de la console Admin, accessible par les propriétaires et administrateurs de l'organisation.

4. **Activer les stratégies d'entreprise** . Les politiques de sécurité de l'Entreprise permettent aux organisations de mettre en œuvre des règles pour les utilisateurs, par exemple en exigeant l'utilisation de l'identifiant en deux étapes. Il est fortement recommandé de configurer les politiques de sécurité avant d'intégrer les utilisateurs.

Étape 3 : Importer dans votre organisation

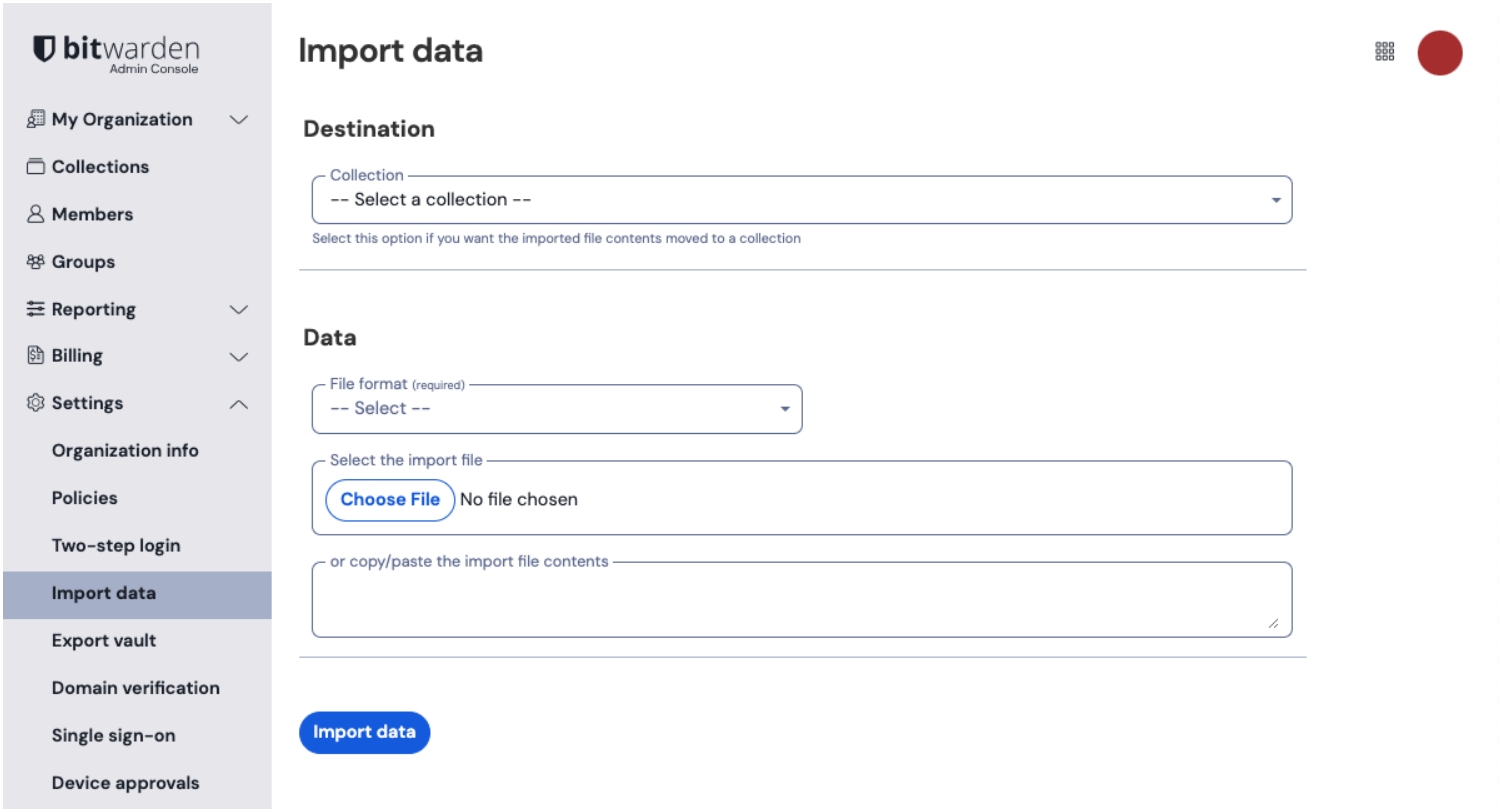
Pour importer des données à votre organisation :

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



commutateur-de-produit

2. Naviguez vers **Paramètres** → **Importer des données**:



Console admin importer

3. Dans le menu déroulant de format, choisissez un **format de fichier** (voir les recommandations d'importation ci-dessous).

4. Sélectionnez le bouton **Choisir un fichier** et ajoutez le fichier à importer.

> **⚠ Warning**
>
> Import to Bitwarden can't check whether items in the file to import are duplicative of items in your vault. This means that **importing multiple files will create duplicative** vault items if an item is already in the vault and in the file to import.

5. Sélectionnez le bouton **Importer les données** pour terminer votre importation.

Actuellement, les fichiers joints ne sont pas inclus dans les opérations d'importation de Bitwarden et devront être téléversés dans votre coffre manuellement. Pour plus d'informations, voir Fichiers joints.

> **Tip**
>
> You should also recommend to employees that they export their individually-owned data from your existing password manager and prepare it for import into Bitwarden. Learn more here.

Importer des recommandations

Lors de l'importation de données dans votre organisation, vous avez deux options :

1. Pour importer le format de fichier par défaut de votre ancien gestionnaire de mots de passe.

2. Pour conditionner un `.CSV` spécifique à Bitwarden pour l'importer.

Nous recommandons de formater votre fichier pour l'importer en tant que Bitwarden `.CSV` pour de meilleurs résultats, ou pour les utilisateurs avancés, en tant que fichier Bitwarden `.JSON`. Pour des instructions sur la façon de créer un fichier d'importation spécifique à Bitwarden, reportez-vous à ce guide d'importation.

Étape 4 : Intégration des utilisateurs

Bitwarden prend en charge l'intégration manuelle via le coffre web et l'intégration automatisée par le biais des intégrations SCIM ou la synchronisation à partir de votre service d'annuaire existant :

Manuel d'intégration

Pour garantir la sécurité de votre organisation, Bitwarden applique un processus en 3 étapes pour l'intégration d'un nouveau membre, inviter → accepter → confirmer. Apprenez comment inviter de nouveaux utilisateurs ici.

Intégration automatisée

L'intégration automatique des utilisateurs est disponible grâce aux intégrations SCIM avec Azure AD, Okta, OneLogin et JumpCloud, ou en utilisant Directory Connector, une application autonome disponible dans une application de bureau et un outil CLI qui synchronisera les utilisateurs et les groupes de votre service d'annuaire existant.

Quelle que soit la méthode que vous utilisez, les utilisateurs sont automatiquement invités à rejoindre l'organisation et peuvent être confirmés manuellement ou automatiquement à l'aide de l'outil Bitwarden CLI.

Étape 5: Configurez l'accès aux collections et aux éléments

Partagez les éléments du coffre avec vos utilisateurs finaux en configurant l'accès via des collections, des groupes et des autorisations au niveau du groupe ou de l'utilisateur:

Collections

Bitwarden permet aux organisations de partager des données sensibles facilement, en toute sécurité et de manière évolutive. Cela est accompli en segmentant les secrets partagés, les éléments, les identifiants, etc. en **collections**.

Les collections peuvent organiser des éléments sécurisés de plusieurs façons, y compris par fonction d'entreprise, attribution de groupe, niveaux d'accès à l'application, ou même protocoles de sécurité. Les collections fonctionnent comme des dossiers partagés, permettant un contrôle d'accès cohérent et un partage parmi les groupes d'utilisateurs.

Les dossiers partagés d'autres gestionnaires de mots de passe peuvent être importés comme collections dans Bitwarden en utilisant le modèle d'importation d'organisation trouvé saisir: lien hypertexte d'actif id: 4DdJLATeuhMYlE581pPErF et en plaçant le nom du dossier partagé dans la colonne `Collection`, par exemple en transformant :

url	username	password	extra	name	grouping	fav
https://azure.microsoft.com/en-us/	AzureUser	5HDXWtuAAK3SX8		Azure Login	Shared-Systems	0
https://github.com/login	GitHubUser	P4JUghjRfhKrDJ		Github	Shared-Systems	0
https://adobe.com	AdobeUser	T6RYSbD5mn78ab		Adobe Login	Shared-Design	0
https://shutterstock.com	ShutterStock	749bs2saWb3bxH		Shutterstock	Shared-Design	0
https://usps.com	USPSUser	6UmtWLkGydBMaZ		USPS Shipping	Shared-Shipping	0
https://ups.com	UPSUser	YBD7ftBZbosS9u		UPS Login	Shared-Shipping	0
https://fedex.com	FedexUser	y44xgs5fiyYZNU		FedExUser	Shared-Shipping	0

Migration Export Example

dans:

collections	type	name	notes	fields	login_uri	login_username	login_password	login_totp
Shared-Systems	login	Azure Login			https://azure.microsoft.com/en-us/	AzureUser	5HDXWtuAAK3SX8	
Shared-Systems	login	Github			https://github.com/login	GitHubUser	P4JUghjRfhKrDJ	
Shared-Design	login	Adobe Login			https://adobe.com	AdobeUser	T6RYSbD5mn78ab	
Shared-Design	login	Shutterstock			https://shutterstock.com	ShutterStock	749bs2saWb3bxH	
Shared-Shipping	login	USPS Shipping			https://usps.com	USPSUser	6UmtWLkGydBMaZ	
Shared-Shipping	login	UPS Login			https://ups.com	UPSUser	YBD7ftBZbosS9u	
Shared-Shipping	login	FedExUser			https://fedex.com	FedexUser	y44xgs5fiyYZNU	

Migration Import Example

Les collections peuvent être partagées avec les groupes et les utilisateurs individuels. Limiter le nombre d'utilisateurs individuels pouvant accéder à une collection rendra la gestion plus efficace pour les administrateurs. Apprenez-en plus ici.

Groupes

L'utilisation de groupes pour le partage est la manière la plus efficace de fournir un accès aux identifiants et aux secrets. Les groupes, comme les utilisateurs, peuvent être synchronisés à votre organisation en utilisant SCIM ou Directory Connector.

Permissions

Les autorisations pour les collections Bitwarden peuvent être attribuées au niveau du groupe ou de l'utilisateur. Cela signifie que chaque groupe ou utilisateur peut être configuré avec des autorisations pour la même collection. Les autorisations de collection comprennent des options pour **Lecture Seule** et **Masquer les Mots de Passe**.

Bitwarden utilise une union d'autorisations pour déterminer les autorisations d'accès finales pour un utilisateur et un élément de collection (en savoir plus). Par exemple:

- L'utilisateur A fait partie du groupe de support de niveau 1, qui a accès à la collection de support, avec une autorisation de lecture seule.
- L'utilisateur A est également un membre du groupe de gestion du support, qui a accès à la collection de support, avec un accès en lecture-écriture.
- Dans ce scénario, l'utilisateur A pourra lire-écrire dans la Collection.

Soutien à la migration

L'équipe de réussite client de Bitwarden est disponible 24/7 avec un support prioritaire pour vos organisations. Si vous avez besoin d'aide ou si vous avez des questions, n'hésitez pas à nous contacter.