bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > PLUS

Guide de Migration de LastPass Entreprise

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

Guide de Migration de LastPass Entreprise

La migration sécurisée de votre organisation avec Bitwarden est simple et sécurisée. Suivez les étapes de ce guide pour migrer les données et les utilisateurs de LastPass :

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

> **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 en toute sécurité de Lastpass à 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 vise à 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 une utilisation facile et une intégration en douceur pour les utilisateurs.

Étape 1: 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 l'intégration des 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 **Single Sign-On** dans les **paramètres** de l'organisation dans 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 exiger l'utilisation de l'identifiant en deux étapes. Il est fortement recommandé de configurer les politiques de sécurité avant d'intégrer les utilisateurs.

Étape 2 : Importer les données

Exporter de LastPass

Créez une exportation complète de toutes vos données partagées à partir du coffre web LastPass sous forme de fichier `.csv` (apprenez comment). La collecte d'une exportation complète peut nécessiter l'attribution de tous les dossiers partagés à l'utilisateur exportateur avant de créer l'exportation.

De plus, toute exportation créée dans LastPass contiendra des données à la fois de votre coffre personnel et des dossiers partagés qui vous sont attribués. À ce stade, nous recommandons d'auditer l'exportation que vous avez créée pour vous assurer qu'elle contient toutes vos données partagées et aucune donnée personnelle.

Importer vers Bitwarden

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**:

3. Complétez les champs suivants à partir des menus déroulants :

   - **Collection :** Sélectionnez si vous souhaitez que le contenu importé soit déplacé vers une collection existante. Dans la plupart des cas, vous n'aurez pas créé de collections dans Bitwarden car l'importation le fera pour vous, alors laissez cette option vide.
   - Format de fichier : sélectionnez **Lastpass (csv)** .

4. Sélectionnez Choisir un fichier et ajoutez le fichier à importer ou copier+coller le contenu de votre fichier dans la boîte de saisie.

   > ⚠ **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 **Importer des données** pour déclencher l'importation.

Les fichiers joints devront être téléversés manuellement dans votre coffre. Notez que les dossiers partagés qui sont imbriqués dans LastPass seront recréés en tant que collections imbriquées dans votre organisation Bitwarden, cependant, s'il n'y a pas de donnée dans la collection "parent", vous devrez créer manuellement la collection parent avec un nom correspondant.

> **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.

Étape 3 : 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 intégrer un nouveau membre, inviter → accepter → confirmer. Apprenez comment inviter de nouveaux utilisateurs ici.

> **Tip**
> Once users are onboarded, instruct them to import their personal data to Bitwarden using an exported file or, if their LastPass accounts are still active, using the **Direct import** method described here.

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.

> **Tip**
> Once users are onboarded, instruct them to import their personal data to Bitwarden using an exported file or, if their LastPass accounts are still active, using the **Direct import** method described here.

Étape 4 : 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 permettre à une organisation de sécuriser des éléments de nombreuses manières, y compris par fonction commerciale, affectation 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 de LastPass peuvent être importés comme des 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 `collections`.

Les collections peuvent être partagées avec des groupes et des utilisateurs individuels. Limiter le nombre d'utilisateurs individuels pouvant accéder à une collection rendra la gestion plus efficace pour les admins. En savoir plus ici.

> **Note**
> Nested collections do not inherit the permissions of the top level collection. See using groups to designate permissions.

Groupes

Utiliser des groupes pour partager est la manière la plus efficace de fournir un accès aux identifiants et aux secrets. Les groupes, comme les utilisateurs, peuvent être synchronisés avec 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 différentes autorisations pour la même collection. Les options d'autorisation de collection comprennent les options :

- Peut voir
- Peut voir, sauf les mots de passe
- Peut modifier
- Peut modifier, sauf les mots de passe
- Accordez l'accès à toutes les collections actuelles et futures

En savoir plus sur les autorisations ici. Bitwarden utilise une union d'autorisations pour déterminer les autorisations d'accès finales pour un utilisateur et une collection. Par exemple:

- L'utilisateur A fait partie du groupe de support de niveau 1, qui a accès à la collection de support, avec l'autorisation d'afficher.
- L'utilisateur A est également un membre du groupe de gestion du support, qui a accès à la collection de support, avec un accès pouvant éditer.
- Dans ce scénario, l'utilisateur A pourra éditer 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.