CONSOLE ADMIN > GESTION DES UTILISATEURS

Aperçu de l'intégration et de la succession

Aperçu de l'intégration et de la succession

> **Tip**
> Lisez l'intégralité du document ci-dessous ou téléchargez le PDF.

Gestion de mots de passe adaptée à votre entreprise

Faire monter rapidement en compétence les nouveaux employés stimule la productivité. De même, dire au revoir correctement renforce la confiance dans la sécurité des systèmes et des comptes de votre entreprise. Que votre entreprise penche vers la consolidation et la centralisation, ou préfère un environnement flexible et dynamique, Bitwarden répond à vos besoins.

Ce guide couvre l'approche de Bitwarden pour l'intégration et la planification de la succession pour les membres de votre organisation, en commençant par notre approche de la relation entre les membres et les organisations, puis en couvrant les cas d'utilisation les plus simples pour l'intégration et la succession, et enfin en passant aux leviers et options à votre disposition pour adapter Bitwarden à vos besoins.

L'approche Bitwarden

La vision de Bitwarden est d'imaginer un monde où personne ne se fait pirater. Nous poursuivons cela dans notre mission d'aider les individus et les entreprises à gérer leurs informations sensibles facilement et en toute sécurité. Bitwarden croit que :

- La gestion de base des mots de passe pour les individus peut et devrait être **Gratuite**. Nous fournissons exactement cela, un compte de base gratuit pour les individus.
- Les individus et les familles devraient jouer un rôle actif dans leur sécurité en utilisant les TOTP, l'accès d'urgence et d'autres fonctionnalités de sécurité.
- Les organisations peuvent grandement améliorer leur profil de sécurité grâce à la gestion organisationnelle des mots de passe et au partage sécurisé.

> **Tip**
> Pour Bitwarden, différents plans et options sont connectés et complémentaires, tous provenant de notre vision d'un monde sans piratage. Donner à chacun au travail **et** à la maison la capacité de gérer les mots de passe nous rapproche d'un pas de cet objectif.

Un aspect clé de Bitwarden est que, contrairement à de nombreuses applications logicielles, tout dans chaque coffre est crypté de bout en bout. Pour maintenir ce modèle de sécurité, chaque personne utilisant Bitwarden doit avoir un compte unique avec un mot de passe principal unique. Les mots de passe principaux doivent être **solides** et **mémorables**.

Chaque utilisateur est responsable de son mot de passe principal. Bitwarden est une solution de chiffrement à connaissance zéro, ce qui signifie que l'équipe de Bitwarden, ainsi que les systèmes Bitwarden eux-mêmes, n'ont aucune connaissance de, aucun moyen de récupérer, ou aucun moyen de réinitialiser un quelconque mot de passe principal.

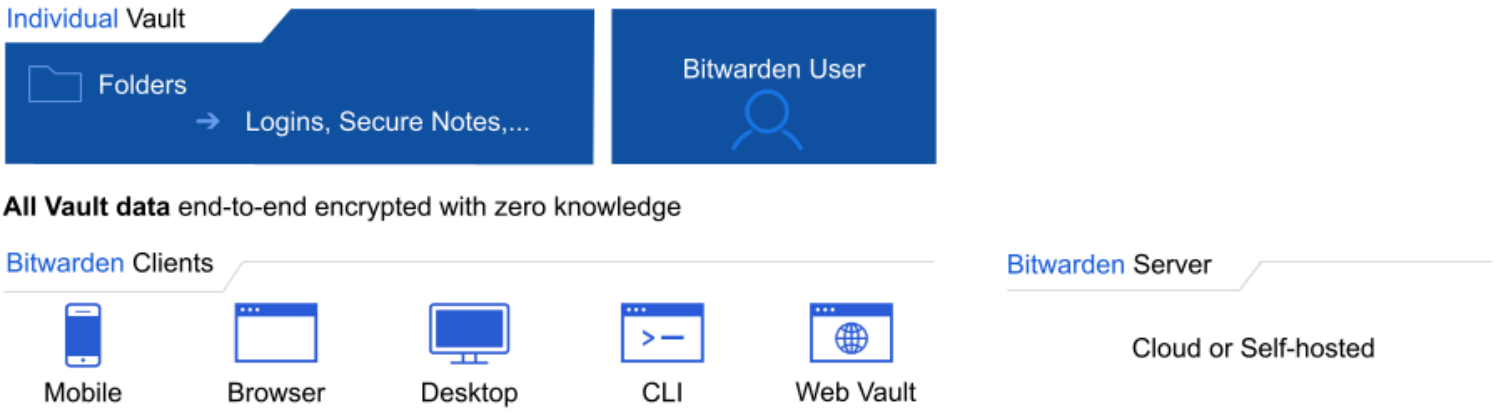
Utilisez Bitwarden partout

La sécurité partout signifie la sécurité n'importe où, donc les meilleurs gestionnaires de mots de passe fournissent un accès sur tous vos appareils. Bitwarden prend en charge une gamme d'applications client, chacune pouvant être connectée à nos serveurs hébergés dans le cloud ou à un serveur auto-hébergé de votre choix :

Clients/Serveurs Bitwarden

Coffres individuels des utilisateurs

Toute personne qui crée un compte Bitwarden aura son propre coffre individuel. Accessible depuis n'importe quelle application client, les coffres individuels sont uniques à chaque utilisateur et seul cet utilisateur détient la clé pour y accéder, en utilisant une combinaison de son adresse de courriel et de son mot de passe principal. Les comptes personnels, et les éléments de coffre individuellement possédés stockés à l'intérieur, sont la responsabilité du propriétaire du compte. Les propriétaires, admins et gestionnaires de l'organisation ne peuvent pas voir le coffre individuel de tout autre utilisateur par conception, garantissant que les données du coffre individuel de quelqu'un restent les siennes.



Coffres personnels

Les organisations Familles, Équipes et Entreprise fournissent automatiquement aux membres individuellement des fonctionnalités Premium, comme l'accès d'urgence et le stockage crypté des pièces jointes, qu'ils peuvent choisir d'utiliser. Les données dans un coffre individuel appartiennent à l'utilisateur. Les coffres individuels ne permettent pas le partage, les organisations le font.

Tip

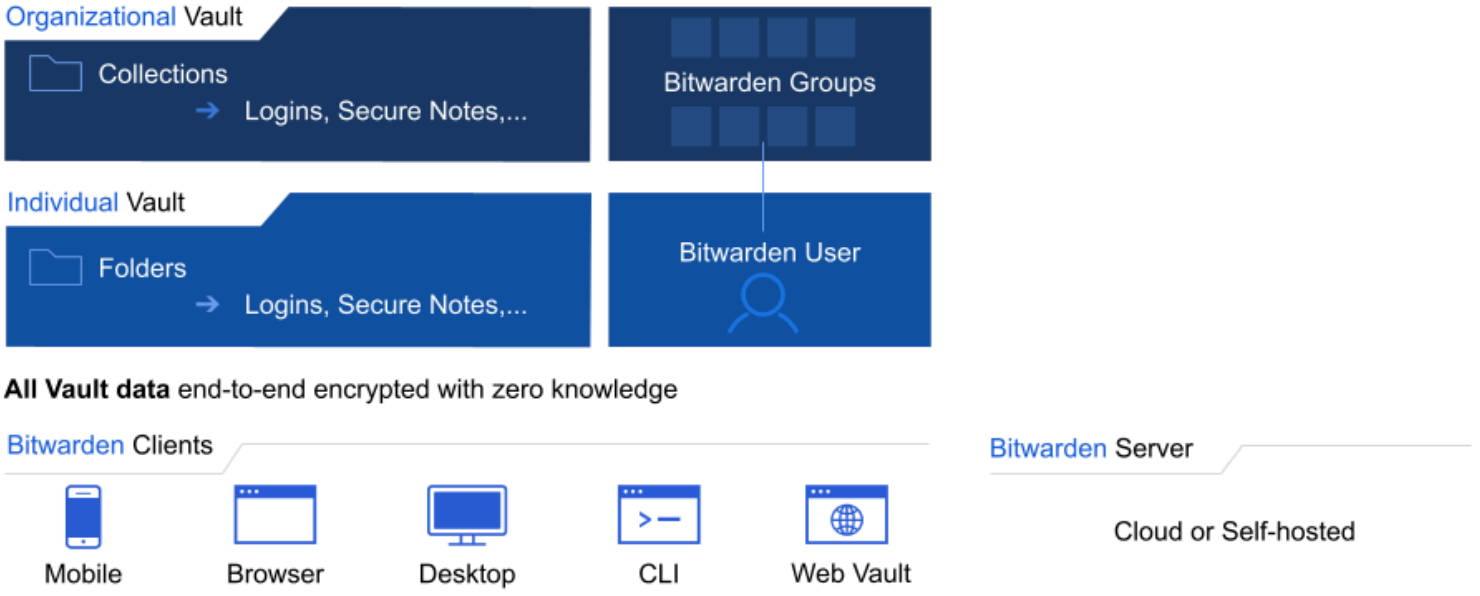
Pourquoi fournir des coffres individuels par défaut ?

Les coffres individuels sont un élément essentiel de l'approche Bitwarden. Les employés utilisent une gamme de références chaque jour, personnellement et professionnellement, et **les habitudes formées dans un domaine deviennent généralement des habitudes dans l'autre**. Selon notre point de vue, les employés qui utilisent des pratiques de sécurité appropriées dans leur vie personnelle transposeront ce bon comportement dans leur vie professionnelle, **protégeant votre entreprise** dans le processus.

Utiliser le même outil dans les deux domaines aide à former l'habitude plus rapidement et plus facilement. Les organisations de l'Entreprise ont la possibilité de configurer les politiques de sécurité, y compris pour désactiver les coffres individuels.

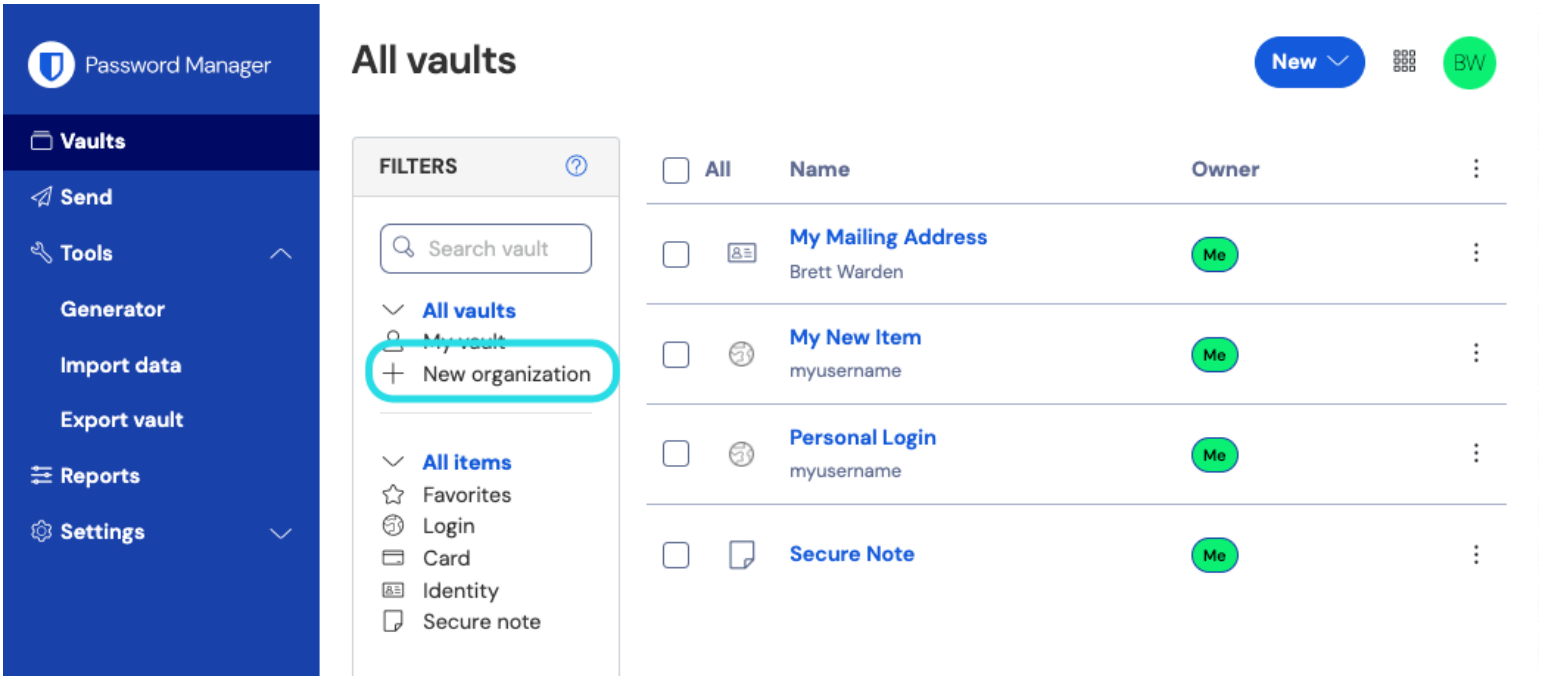
Organisations Bitwarden

Les **organisations Bitwarden** ajoutent une couche de collaboration et de partage à la gestion des mots de passe pour votre équipe ou entreprise, vous permettant de partager en toute sécurité des informations communes comme les mots de passe wifi de bureau, les identifiants en ligne, ou les cartes de paiement d'entreprise partagées. Le partage sécurisé à travers les organisations est sûr et facile.



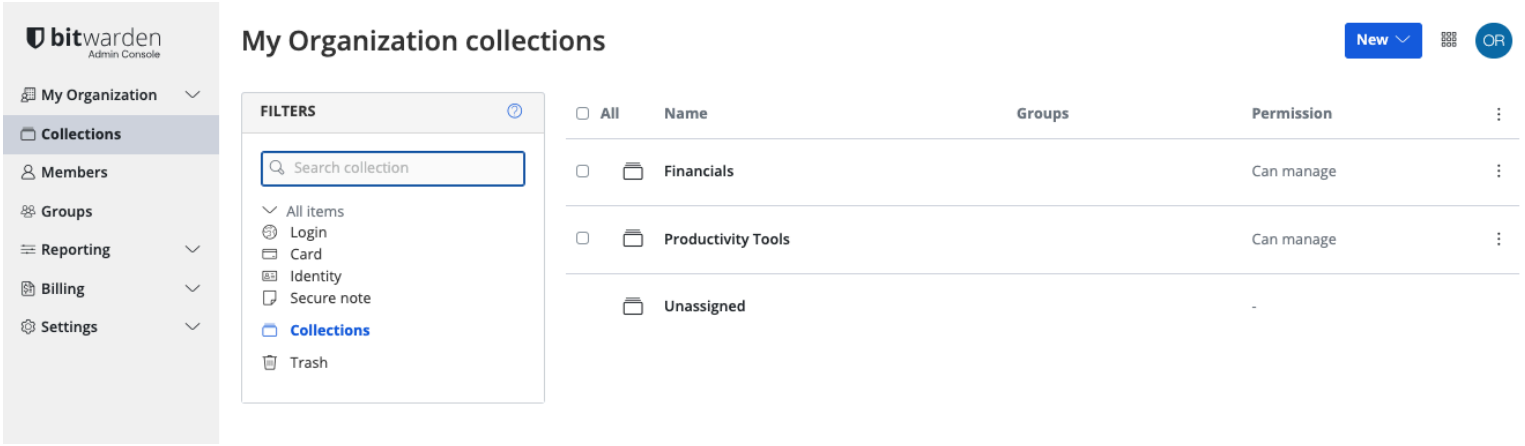
Coffre de l'Organisation

N'importe qui peut démarrer une organisation directement depuis l'application web :



Nouvelle organisation

Une fois créé, vous arriverez dans la Console Admin, qui est le centre névralgique pour tout ce qui concerne le partage et l'administration de l'organisation. Celui qui lance l'organisation sera le propriétaire, lui donnant le plein contrôle pour superviser le coffre, pour gérer les éléments, les membres, les collections et les groupes, pour exécuter le rapport, et configurer des paramètres comme les politiques de sécurité :



Console Admin

Collections

Les organisations Bitwarden gèrent les membres et les données de manière évolutive et sécurisée. Gérer les membres et les données sur une base individuelle est inefficace pour les grandes entreprises et peut laisser place à l'erreur. Pour résoudre ce problème, les organisations proposent des collections et des groupes .

Les collections rassemblent ensemble des identifiants, des notes, des cartes de paiement et des identités pour un partage sécurisé au sein d'une organisation:

Utilisation des collections

Intégration des membres

Une fois que votre organisation est établie et que les collections sont configurées pour stocker vos données, les propriétaires et les administrateurs devraient inviter de nouveaux membres. Pour garantir la sécurité de votre organisation, Bitwarden applique un processus en 3 étapes pour l'intégration de nouveaux membres, Inviter → Accepter → Confirmer.

Les membres peuvent être intégrés directement à partir du coffre web, en utilisant l'application Directory Connector pour synchroniser les utilisateurs individuels et les groupes, ou par le biais de la provision Just in Time (JIT) en utilisant l'identifiant avec SSO.

Ajout de membres

Dans les cas les plus simples, les utilisateurs peuvent être ajoutés à votre organisation directement depuis l'application web. Lors de l'ajout d'utilisateurs, vous pouvez désigner à quelles collections leur donner accès, quel rôle leur attribuer, et plus encore.

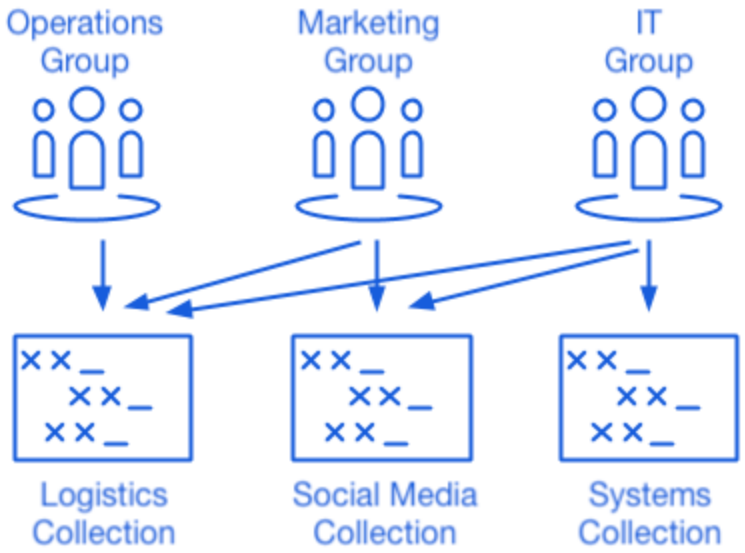
Découvrez étape par étape comment ajouter des utilisateurs à votre organisation .

Une fois que les utilisateurs sont entièrement intégrés à votre organisation, vous pouvez leur attribuer l'accès aux données du coffre de votre organisation en les affectant à des collections. Les Équipes et les organisations d'Entreprise peuvent assigner des utilisateurs à des groupes pour une attribution d'autorisations scalable, et construire des associations de groupe-collection au lieu d'attribuer l'accès au niveau individuel.

> **Tip**
>
> Pour les grandes organisations, SCIM et Directory Connector sont les meilleures méthodes pour intégrer et désintégrer les utilisateurs à grande échelle.

Groupes

Les groupes relient ensemble des utilisateurs individuels et fournissent une manière évolutive d'attribuer des autorisations, y compris l'accès aux collections et autres contrôles d'accès. Lors de l'intégration de nouveaux utilisateurs, ajoutez-les à un groupe pour qu'ils héritent automatiquement des autorisations configurées de ce groupe :



Utilisation de Collections avec des Groupes

Contrôles d'accès complets basés sur le rôle

Bitwarden adopte une approche favorable à l'entreprise pour partager à grande échelle. Les membres peuvent être ajoutés à l'organisation avec un nombre de rôles différents, appartenir à différents groupes, et avoir ces groupes assignés à diverses collections pour réguler l'accès. Parmi les rôles disponibles se trouve un rôle personnalisé pour une configuration granulaire des autorisations administratives.

Désactivation des utilisateurs

Chez Bitwarden, nous considérons le partage des identifiants comme un aspect essentiel pour accomplir le travail de manière efficace et sécurisée. Nous reconnaissons également qu'une fois qu'une accréditation est partagée, il est techniquement possible pour le destinataire de la conserver. Pour cette raison, l'intégration sécurisée en utilisant des contrôles d'accès basés sur le rôle appropriés et en mettant en œuvre des politiques de sécurité joue un rôle important dans la facilitation d'une succession sécurisée.

Il existe une variété d'outils fournis par Bitwarden pour personnaliser votre flux de travail et exercer un contrôle plus important sur la succession. Les sections suivantes décriront un flux de travail de succession de base, qui n'utilise aucun de ces outils, et certaines tactiques de succession avancées fréquemment utilisées par les organisations :

Désapprovisionnement de base

La suppression des utilisateurs de Bitwarden implique de retirer les utilisateurs de votre organisation, et comme pour l'intégration, cela peut être fait directement à partir du coffre web ou de manière automatisée en utilisant SCIM ou Directory Connector.

Alice est une **Utilisatrice** dans votre organisation, qui est hébergée sur le cloud Bitwarden et utilise des adresses de courriel d'entreprise (par exemple, `premier-dernier@entreprise.com`). Actuellement, voici comment Alice utilise Bitwarden:

Zone de produit	Description
Applications client	Utilise Bitwarden sur mobile et une extension de navigateur personnellement et professionnellement, et le coffre web pour un travail occasionnel lié à l'organisation.
Courriel & mot de passe principal	Se connecte à Bitwarden en utilisant `alice@company.com` et `p@ssw0rD`.
Articles personnels	Stocke divers éléments personnels, y compris les identifiants et les cartes de paiement, dans son coffre personnel.
Authentification à deux facteurs	Utilise Duo 2FA à l'échelle de l'organisation.
Collections	Alice a l'autorisation de gérer pour la collection "Marketing Credentials", ce qui lui donne la capacité de gérer de nombreux aspects de cette collection.
Éléments partagés	A créé et partagé plusieurs éléments de coffre qui sont possédés par l'organisation et résident dans la collection de son Équipe.

Une fois qu'Alice est retirée de votre organisation :

Zone de produit	Description
Applications client	Peut continuer à utiliser n'importe quelle application Bitwarden pour accéder à son coffre individuel, cependant **tous perdront immédiatement l'accès** au coffre de l'organisation, à toutes les collections et à tous les éléments partagés.

Zone de produit	Description
Courriel & mot de passe principal	Elle peut continuer à se connecter en utilisant `alice@company.com` et `p@ssw0rD`, cependant, comme elle n'aura pas accès à sa boîte de réception `@company.com` , elle devrait être conseillée de changer le courriel associé à son compte Bitwarden.
Éléments individuels	Elle pourra toujours utiliser son coffre individuel et accéder aux éléments stockés à l'intérieur.
Autorisations dans l'organisation	Perdra **immédiatement toutes les autorisations et l'accès à** tout ce qui est lié à l'organisation.
Authentification à deux facteurs	Elle ne pourra pas utiliser Duo 2FA de l'organisation pour accéder à son coffre, mais peut configurer l'une de nos options d'identifiant en deux étapes gratuites ou mettre à niveau vers Premium pour plus.
Collections créées	La "collection d'équipe de marketing" d'Alice sera conservée par les propriétaires et les admins de l'organisation, qui peuvent attribuer à un nouvel utilisateur l'autorisation de gérer.
Éléments partagés	La propriété des collections et des éléments partagés **appartient à l'organisation**, donc Alice perdra l'accès à tous ces éléments malgré le fait qu'elle les ait créés.

Tip

Les appareils hors ligne mettent en cache une copie en lecture seule des données du coffre, y compris les données du coffre organisationnel. Si vous prévoyez une exploitation malveillante de cela, les identifiants auxquels le membre avait accès devraient être mis à jour lorsque vous le retirez de l'organisation.

Déprovisionnement avancé

Warning

Pour ces comptes qui n'ont pas de mot de passe principal à la suite de SSO avec des appareils de confiance, les retirer de votre organisation ou révoquer leur accès coupera tout accès à leur compte Bitwarden à moins que :

1. Vous leur attribuez un mot de passe principal en utilisant la récupération de compte au préalable.
2. L'utilisateur se connecte au moins une fois après la récupération du compte afin de terminer complètement le processus de récupération du compte.

Prise de contrôle administrative

En utilisant la politique de réinitialisation du mot de passe principal, les propriétaires et les admins de votre organisation peuvent réinitialiser le mot de passe principal d'un utilisateur lors de la succession.

La réinitialisation du mot de passe principal d'un utilisateur déconnecte l'utilisateur de toutes les sessions Bitwarden actives et réinitialise ses identifiants aux valeurs spécifiées par l'administrateur, ce qui signifie que cet administrateur (et uniquement cet administrateur) aura les clés des données du coffre de l'utilisateur, y compris les éléments dans le coffre individuel. Cette tactique de prise de contrôle du coffre est couramment utilisée par les organisations pour s'assurer que les employés ne conservent pas l'accès à des éléments individuels du coffre qui peuvent être liés au travail et peuvent être utilisés pour faciliter les audits de chaque identifiant qu'un employé aurait pu utiliser.

> **Note**
>
> **La réinitialisation du mot de passe admin ne contourne pas l'identifiant en deux étapes**. Dans de nombreux cas, nous recommandons d'utiliser SSO car certains IdPs vous permettront de configurer la 2FA et les politiques de sécurité pour contourner la 2FA pour vos utilisateurs.

Enlèvement du coffre individuel

Si votre organisation nécessite un contrôle en temps réel de tous les éléments du coffre, vous pouvez utiliser la politique de suppression individuelle du coffre pour exiger que les utilisateurs enregistrent tous les éléments du coffre dans l'organisation. Cela permettra d'éviter la nécessité de prendre le contrôle et d'auditer un compte d'utilisateur lors de la succession, car il sera complètement vide de données une fois retiré de l'organisation.

Suppression de compte sans identifiant

Comme mentionné précédemment, supprimer un utilisateur de votre organisation ne supprime pas automatiquement leur compte Bitwarden. Dans le flux de travail de succession de base, lorsqu'un utilisateur est supprimé, il ne peut plus accéder à l'organisation ou à tout élément et collection partagés, cependant, il pourra toujours se connecter à Bitwarden en utilisant son mot de passe principal existant et accéder à tout élément individuel du coffre.

Les organisations souhaitant supprimer complètement le compte, y compris tous les éléments individuels du coffre, pourraient être en mesure d'utiliser l'une des méthodes suivantes pour le faire lors de la succession :

1. Si vous auto-hébergez Bitwarden, un admin autorisé peut supprimer le compte depuis le Portail de l'Administrateur Système.

2. Si le compte a une adresse courriel @yourcompany.com que votre entreprise contrôle, vous pouvez utiliser le processus supprimer sans se connecter et confirmer la suppression dans la boîte de réception @yourcompany.com.

Concevoir votre organisation pour votre entreprise

Chez Bitwarden, nous disons souvent que la gestion des mots de passe est une gestion des personnes, et nous pouvons adapter les flux de travail à votre organisation. En offrant une large gamme d'options, partagées via notre approche open source, les clients peuvent être assurés qu'ils peuvent répondre à leurs propres besoins individuels.

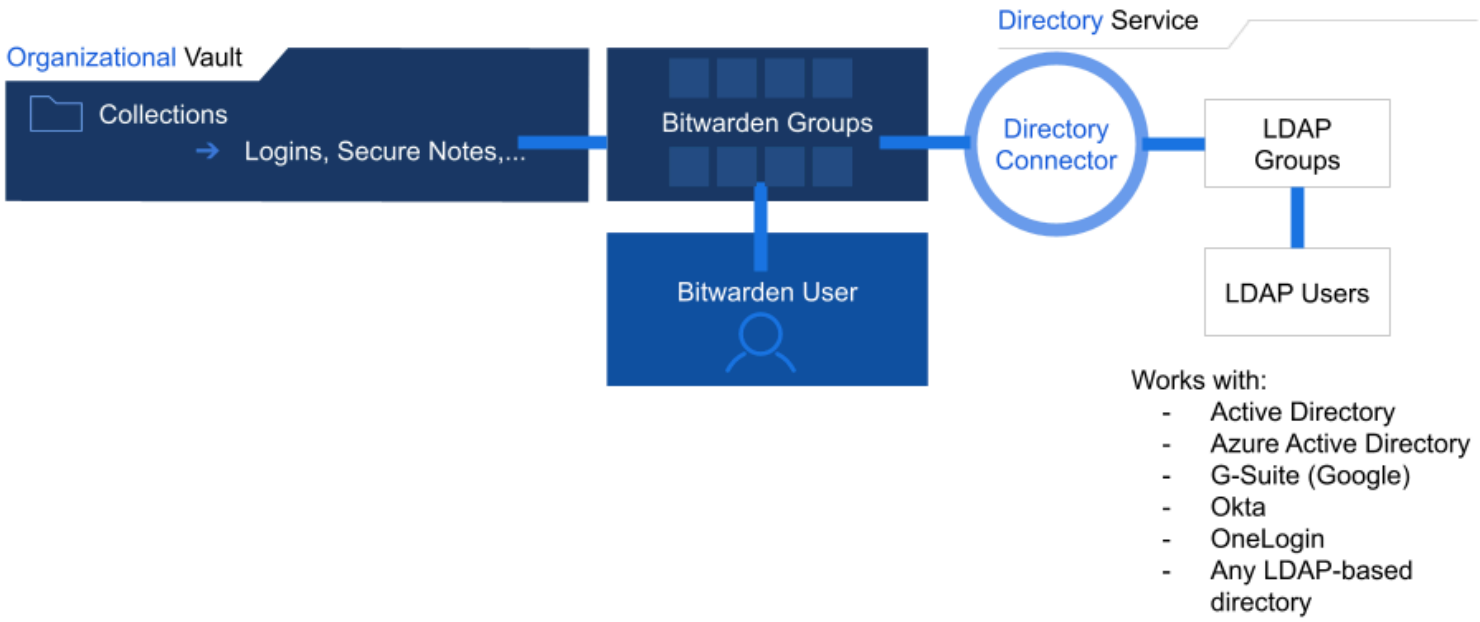
Commencez dès aujourd'hui avec un essai gratuit Enterprise ou Teams.

SCIM

Pour les organisations Entreprise avec de grandes bases d'utilisateurs qui fonctionnent en utilisant une identité prise en charge (actuellement, Azure AD, Okta, OneLogin et JumpCloud), les intégrations SCIM peuvent être utilisées pour provisionner automatiquement des membres et des groupes dans votre organisation Bitwarden. En savoir plus.

Connecteur de Répertoire

Pour les entreprises avec de grandes bases d'utilisateurs qui fonctionnent à l'aide de services d'annuaire (LDAP, AD, Okta, et autres), Directory Connector peut synchroniser les utilisateurs et les groupes de l'annuaire vers l'organisation Bitwarden. Directory Connector est une application autonome qui peut être exécutée n'importe où avec accès à vos répertoires et à Bitwarden.



Connecteur de Répertoire

De nombreuses équipes Bitwarden et organisations d'entreprise concentrent leurs efforts d'intégration sur le Directory Connector et utilisent les zones d'administration du coffre de l'organisation pour gérer les relations entre le groupe et la collection.

Le connecteur de répertoire fera :

- Synchroniser les groupes de répertoires basés sur LDAP avec les groupes Bitwarden
- Synchroniser les utilisateurs au sein de chaque groupe
- Inviter de nouveaux utilisateurs à rejoindre l'organisation
- Supprimez les utilisateurs supprimés de l'organisation

Identifiez-vous avec SSO

Les organisations Entreprise Bitwarden peuvent s'intégrer à votre fournisseur d'identité existant (IdP) en utilisant SAML 2.0 ou OIDC pour permettre aux membres de votre organisation de se connecter à Bitwarden en utilisant SSO. La connexion avec SSO sépare l'authentification de l'utilisateur du déchiffrement du coffre :

L'**authentification** est effectuée via votre IdP choisi et conserve tous les processus d'authentification à deux facteurs liés à cet IdP. **Le déchiffrement** des données du coffre-fort nécessite la clé individuelle de l'utilisateur, qui dérive en partie du mot de passe principal. Il y a deux options de déchiffrement, les deux obligeront les utilisateurs à s'authentifier en utilisant leurs identifiants SSO habituels.

- **Mot de passe principal** : une fois authentifiés, les membres de l'organisation déchiffreront les données du coffre-fort à l'aide de leurs mots de passe principaux .

- **Chiffrement géré par le client**: Connectez l'identifiant avec SSO à votre serveur de clé de déchiffrement auto-hébergé. En utilisant cette option, les membres de l'organisation n'auront pas besoin d'utiliser leur mot de passe principal pour décrypter les données du coffre. Au lieu de cela, Key Connector récupérera une clé de déchiffrement stockée en toute sécurité dans une base de données que vous possédez et gérez.
  - Exploitez votre fournisseur d'identité existant.
  - Protégez le chiffrement de bout en bout de vos données.
  - Fournir des utilisateurs automatiquement.
  - Configurez l'accès avec ou sans SSO.
  - Déchiffrez les données du coffre selon les besoins de sécurité de votre entreprise.

Partage de mot de passe sécurisé

Les organisations de l'Entreprise peuvent mettre en œuvre une variété de politiques de sécurité conçues pour établir une base sécurisée pour toute entreprise. Les politiques de sécurité comprennent :

- **Exiger une connexion en deux étapes :** Exiger des utilisateurs qu'ils mettent en place une connexion en deux étapes sur leurs comptes personnels.
- **Exigences du mot de passe principal :** définissez les exigences minimales concernant la force du mot de passe principal.
- **Générateur de mot de passe:** Définissez les exigences minimales pour la configuration du générateur de mot de passe.
- **Organisation unique :** empêchez les utilisateurs de rejoindre d'autres organisations.
- **Supprimer le coffre individuel :** Obligez les utilisateurs à enregistrer les éléments du coffre dans une organisation en supprimant l'option de propriété personnelle.

> **Tip**
>
> La politique de **Suppression de coffre individuel**, par exemple, s'inscrit dans la discussion précédente concernant l'interaction entre les coffres individuels et les coffres de l'organisation. Certaines entreprises peuvent désirer l'assurance d'avoir toutes les accréditations conservées dans le coffre de l'organisation. Une mise en œuvre possible pourrait impliquer de permettre à chaque utilisateur individuel d'avoir sa propre collection, qui contrairement aux coffres individuels pourrait être supervisée par les propriétaires et les admins de l'organisation.

Journal des événements

Les organisations Bitwarden incluent l'accès aux journaux d'événements, qui peuvent être affichés directement à partir du coffre web ou exportés pour être analysés dans les systèmes de gestion des informations et des événements de sécurité (SIEM) comme Splunk. Les journaux d'événements incluent des informations sur :

- Interactions utilisateur-élément
- Modifications apportées aux éléments du coffre
- Événements d'intégration
- Changements de configuration de l'organisation

- Beaucoup, beaucoup plus

> **Tip**
> En plus de ces avantages, les clients apprécient la possibilité d'intégrer étroitement Bitwarden dans leurs systèmes existants. Bitwarden propose une API publique robuste et une interface de ligne de commande (CLI) complète pour une intégration plus poussée dans les flux de travail de l'organisation existante.

Auto-Hébergement

Conformément à l'approche de Bitwarden pour offrir la gestion des mots de passe partout et en tout lieu, Bitwarden propose une option d'auto-hébergement pour répondre à une gamme encore plus large de cas d'utilisation pour les Entreprises. Il y a de nombreuses raisons pour une entreprise de choisir d'être auto-hébergée. Spécifiquement en ce qui concerne l'intégration, la succession et les fonctionnalités améliorées, voici quelques-unes des raisons pour lesquelles les entreprises choisissent de le faire :

- **Suppression immédiate des comptes d'utilisateurs :** Parce que vous contrôlez le serveur, les utilisateurs peuvent être entièrement supprimés (y compris leur coffre individuel).
- **Contrôle d'accès réseau** : Les propriétaires d'organisation peuvent déterminer quel accès réseau les employés doivent utiliser pour accéder à leur serveur Bitwarden.
- **Paramètres de proxy avancés :** Les administrateurs peuvent choisir d'activer ou de désactiver certains types d'appareils pour accéder au serveur Bitwarden.
- **Utilisez un cluster de base de données existant :** Connectez-vous à une base de données Microsoft SQL Server existante. Des bases de données supplémentaires seront prises en charge à l'avenir.
- **Augmentez le stockage pour les fichiers joints et Bitwarden Send:** Les fichiers joints pour les éléments Bitwarden ou Bitwarden Send sont conservés sur le stockage fourni par l'utilisateur.

Assemblez les pièces

Le connecteur de répertoire, l'identifiant avec SSO, les politiques de sécurité de l'Entreprise et votre coffre fonctionnent bien individuellement ou en harmonie pour optimiser votre expérience de gestion de l'intégration, de la succession et de l'organisation. Le tableau suivant détaille comment cela pourrait ressembler à assembler ces pièces en un processus fluide :

Étape	Description
Synchroniser	Utilisez Directory Connector pour synchroniser les groupes et les utilisateurs vers Bitwarden à partir de votre service de répertoire existant.
Inviter	Le connecteur de répertoire émettra automatiquement des invitations aux utilisateurs synchronisés.
Authentifiez	Associez votre identifiant à la mise en œuvre du SSO avec la politique de sécurité du SSO pour obliger les utilisateurs à s'inscrire avec le SSO lorsqu'ils acceptent leurs invitations.

Étape	Description
Administrer	Utilisez le coffre web pour promouvoir certains utilisateurs à différents rôles et pour garantir que les relations groupe-collection sont configurées pour accorder le bon accès aux bons utilisateurs.
Re-synchroniser	Exécutez périodiquement Directory Connector pour supprimer de Bitwarden les utilisateurs qui ne sont plus actifs dans votre service d'annuaire et pour commencer l'intégration des nouvelles recrues.

FAQ

Q: Si un employé a déjà un compte Bitwarden, pouvons-nous l'attacher à l'organisation afin qu'il n'ait pas besoin d'un autre compte Bitwarden ?

A: Oui! Tu peux. Certains clients recommandent qu'avant d'associer des utilisateurs à l'organisation, ces utilisateurs aient un coffre Bitwarden associé à leur courriel d'entreprise. Ce choix est spécifique à l'entreprise et les deux approches fonctionnent.

Q: Lorsqu'un employé quitte, pouvons-nous détacher leur compte de l'organisation afin qu'ils n'aient plus accès aux identifiants de l'entreprise et qu'ils ne perdent pas leurs identifiants individuellement possédés ?

A: Oui! C'est exactement ce que la déprovisionnement implique.

Q: Peut-on empêcher les employés de dupliquer les identifiants de l'organisation de l'entreprise dans leur coffre individuel ?

A: Oui! En utilisant notre suite complète de contrôles d'accès basés sur le rôle, vous pouvez rendre les identifiants **en lecture seule** pour éviter la duplication.