SECRETS MANAGER > COMMENCEZ

Gérez votre Organisation

Gérez votre Organisation

> **Note**
> Pour un aperçu complet de l'intégration de Bitwarden, veuillez consulter ce guide pour plus d'informations.

En tant qu'organisation utilisant Secrets Manager, vous partagerez de nombreux outils initialement utilisés par le gestionnaire de mots de passe. Cet article couvre ces domaines communs et fournit des liens pour partager la documentation appropriée.

> **Note**
> Si vous êtes tout nouveau dans les organisations Bitwarden, nous vous recommandons de consulter notre article sur comment commencer en tant qu'administrateur d'organisation.

Partage de mot de passe sécurisé

Les politiques de sécurité permettent aux organisations de l'Entreprise d'imposer des règles de sécurité à leurs membres, par exemple en exigeant l'utilisation de l'identifiant en deux étapes. Bien que certaines politiques de sécurité s'appliquent principalement au gestionnaire de mots de passe, il existe quelques politiques qui sont largement applicables aux utilisateurs de Secrets Manager :

- Exiger une authentification à deux facteurs
- Exigences du mot de passe principal
- Réinitialisation du mot de passe principal
- Organisation Unique
- Authentification par Connexion Unique (Single Sign-On)
- Délai d'expiration du coffre

> **Tip**
> Si vous êtes nouveau sur Bitwarden, nous vous recommandons de définir des politiques de sécurité avant d'intégrer vos utilisateurs.

Gestion des utilisateurs

La gestion des utilisateurs pour les organisations Secrets Manager est similaire aux organisations utilisant le gestionnaire de mots de passe, cependant certains éléments spécifiques à Secrets Manager incluent l'octroi d'accès aux membres de l'organisation à Secrets Manager, les différences de rôle des membres, et la spécification des sièges d'utilisateurs et des comptes de service.

Intégration

Il existe plusieurs méthodes différentes pour intégrer des utilisateurs à votre organisation Bitwarden. Certaines des méthodes couramment utilisées sont mises en évidence ici :

Manuel

Le coffre web Bitwarden offre une interface simple et intuitive pour inviter de nouveaux utilisateurs à rejoindre votre organisation. Cette méthode est la meilleure pour les petites organisations ou celles qui n'utilisent pas des services d'annuaire comme Azure AD ou Okta. Apprenez comment commencer.

SCIM

Les serveurs Bitwarden fournissent un point de terminaison SCIM qui, avec une clé API SCIM valide, acceptera les demandes de votre fournisseur d'identité pour la provision et la déprovision des utilisateurs et du groupe. Cette méthode est la meilleure pour les grandes organisations utilisant un service de répertoire ou un IdP activé par SCIM. Apprenez comment commencer.

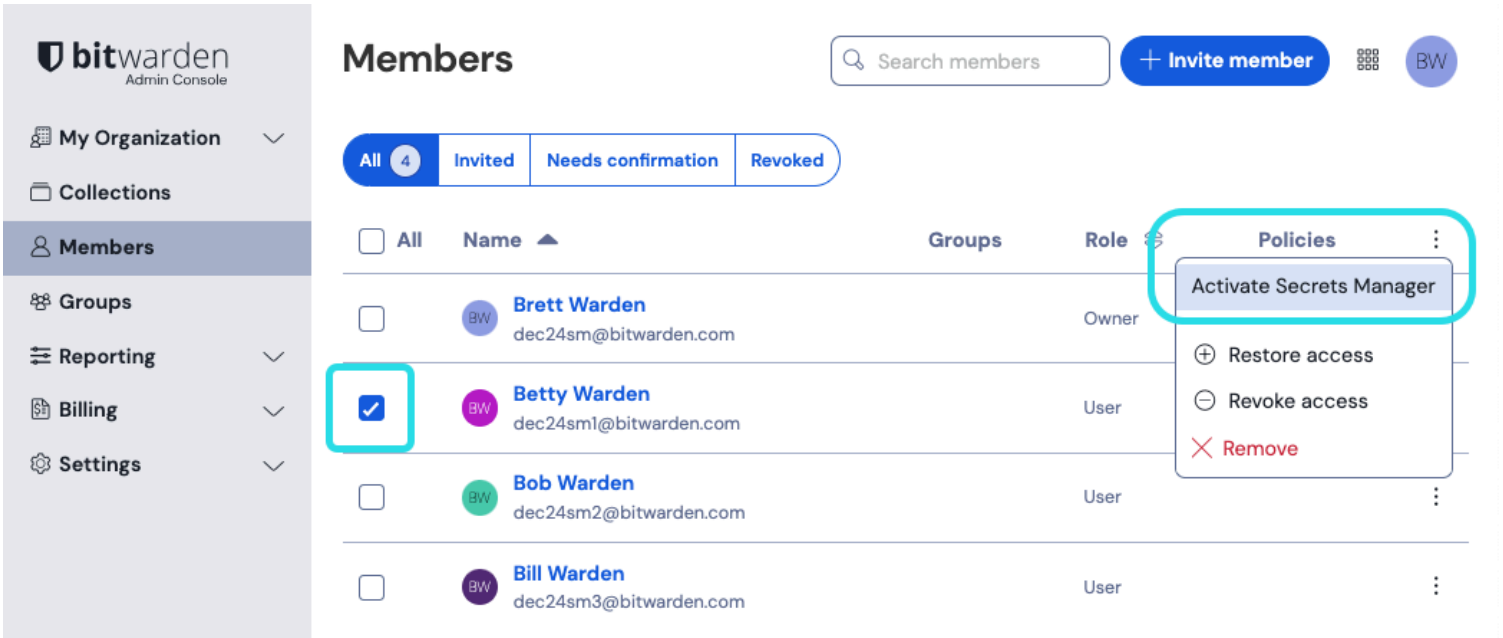
Connecteur de Répertoire

Le Directory Connector provisionne automatiquement les utilisateurs et les groupes dans votre organisation Bitwarden en puisant dans une sélection de services de répertoire source. Cette méthode est la meilleure pour les grandes organisations utilisant des services d'annuaire qui ne prennent pas en charge SCIM. Apprenez comment commencer.

Accès à Secrets Manager

Une fois intégrés, donnez aux membres individuels de votre organisation l'accès à Secrets Manager :

1. Ouvrez la vue **Membres** de votre organisation et sélectionnez les membres auxquels vous souhaitez donner accès à Secrets Manager.
2. En utilisant le menu ⋮, sélectionnez **Activer Secrets Manager** pour accorder l'accès aux membres sélectionnés :



Ajouter des utilisateurs de Secrets Manager

Tip

Donner aux membres l'accès à Secrets Manager ne leur donnera pas automatiquement accès aux projets stockés ou aux secrets. Vous devrez ensuite attribuer l'accès aux projets à des personnes ou des groupes.

Rôles des membres

Le tableau suivant décrit ce que chaque rôle de membre peut faire au sein de Secrets Manager. Pendant la bêta, les utilisateurs ont le même rôle de membre pour Secrets Manager qu'ils ont été assignés pour le gestionnaire de mots de passe :

Rôle du membre	Description
Utilisateur	Les utilisateurs peuvent créer leurs propres secrets, projets, comptes de service et jetons d'accès. Ils peuvent éditer ces objets une fois créés. Les utilisateurs doivent être assignés à des projets ou à des comptes de service afin d'interagir avec les objets existants, et peuvent se voir attribuer un accès **Peut lire** ou **Peut lire, écrire**.
Administrateur	Les admins ont automatiquement accès à **Peut lire, écrire** tous les secrets, projets, comptes de service et jetons d'accès. Les admins peuvent se donner accès à Secrets Manager et attribuer l'accès à Secrets Manager à d'autres membres.
Propriétaire	Les propriétaires ont automatiquement accès à **Peut lire, écrire** à tous les secrets, projets, comptes de service et jetons d'accès. Les propriétaires peuvent s'attribuer eux-mêmes l'accès à Secrets Manager et attribuer l'accès à Secrets Manager à d'autres membres.

Note

Les rôles personnalisés ne sont actuellement pas définis avec des options pour Secrets Manager, cependant ils peuvent toujours être utilisés pour attribuer des capacités spécifiques au gestionnaire de mots de passe ou à une organisation plus large.

Groupes

Les groupes relient ensemble des membres individuels et fournissent une manière évolutive d'accéder à des projets spécifiques et d'obtenir des autorisations pour ceux-ci. Lors de l'ajout de nouveaux membres, ajoutez-les à un groupe pour qu'ils héritent automatiquement des autorisations configurées de ce groupe. En savoir plus.

Une fois que les groupes sont créés dans la console admin, attribuez-les à des projets à partir de l'application web Secrets Manager.

Authentification unique

La connexion avec SSO est la solution de Bitwarden pour l'authentification unique. En utilisant l'identifiant avec SSO, les organisations Entreprise peuvent tirer parti de leur fournisseur d'identité existant pour authentifier les utilisateurs avec Bitwarden en utilisant les protocoles SAML 2.0 ou Open ID Connect (OIDC). Apprenez comment commencer.

Administration de récupération du compte

La récupération de compte permet aux administrateurs désignés de récupérer les comptes utilisateurs de l'organisation de l'entreprise et de restaurer l'accès dans l'événement où un employé oublie son mot de passe principal. La récupération de compte peut être activée pour une organisation en activant la politique d'administration de récupération de compte. Apprenez comment commencer.

Journal des événements

Les journaux d'événements sont des enregistrements horodatés des événements qui se produisent au sein de vos Équipes ou de votre organisation Entreprise. Les événements de Secrets Manager sont disponibles à la fois depuis le **Rapport → Journaux d'événements** de votre coffre d'organisation et depuis la page des journaux d'événements du compte de service.

Les journaux d'événements sont exportables et sont conservés indéfiniment. Bien que de nombreux événements soient applicables à tous les produits Bitwarden et que certains soient spécifiques au gestionnaire de mots de passe, Secrets Manager enregistrera spécifiquement les suivants :

- Secret accédé par un compte de service

Auto-Hébergement

Les organisations d'Entreprise peuvent auto-héberger Bitwarden Secrets Manager en utilisant Docker sur des machines Linux et Windows. Si vous n'avez jamais auto-hébergé Bitwarden auparavant, utilisez ce guide pour vous mettre sur la bonne voie.

Si vous hébergez déjà une organisation Bitwarden Entreprise sur votre propre serveur et souhaitez obtenir un accès à Secrets Manager sur ce serveur :

1. Inscrivez-vous pour un abonnement à Secrets Manager dans votre organisation Bitwarden hébergée dans le cloud.

2. Mettez à jour votre serveur auto-hébergé pour, au minimum, 2023.10.0.

3. Récupérez un nouveau fichier de licence auprès de votre organisation hébergée dans le cloud et téléchargez-le sur votre serveur auto-hébergé .

ⓘ Note

Secrets Manager auto-hébergé n'est pas pris en charge pour l' option de déploiement unifié auto-hébergé Bitwarden. Les Équipes et les organisations d'Entreprise devraient utiliser une installation standard de Linux ou de Windows.