Politiques de sécurité de l'Entreprise

Afficher dans le centre d'aide https://bitwarden.com/help/policies/

Politiques de sécurité de l'Entreprise

Quelles sont les politiques de sécurité de l'Entreprise ?

Les politiques de l'Entreprise permettent aux organisations de l'Entreprise d'appliquer des règles de sécurité pour tous les utilisateurs, par exemple en imposant l'utilisation de l'identifiant en deux étapes.

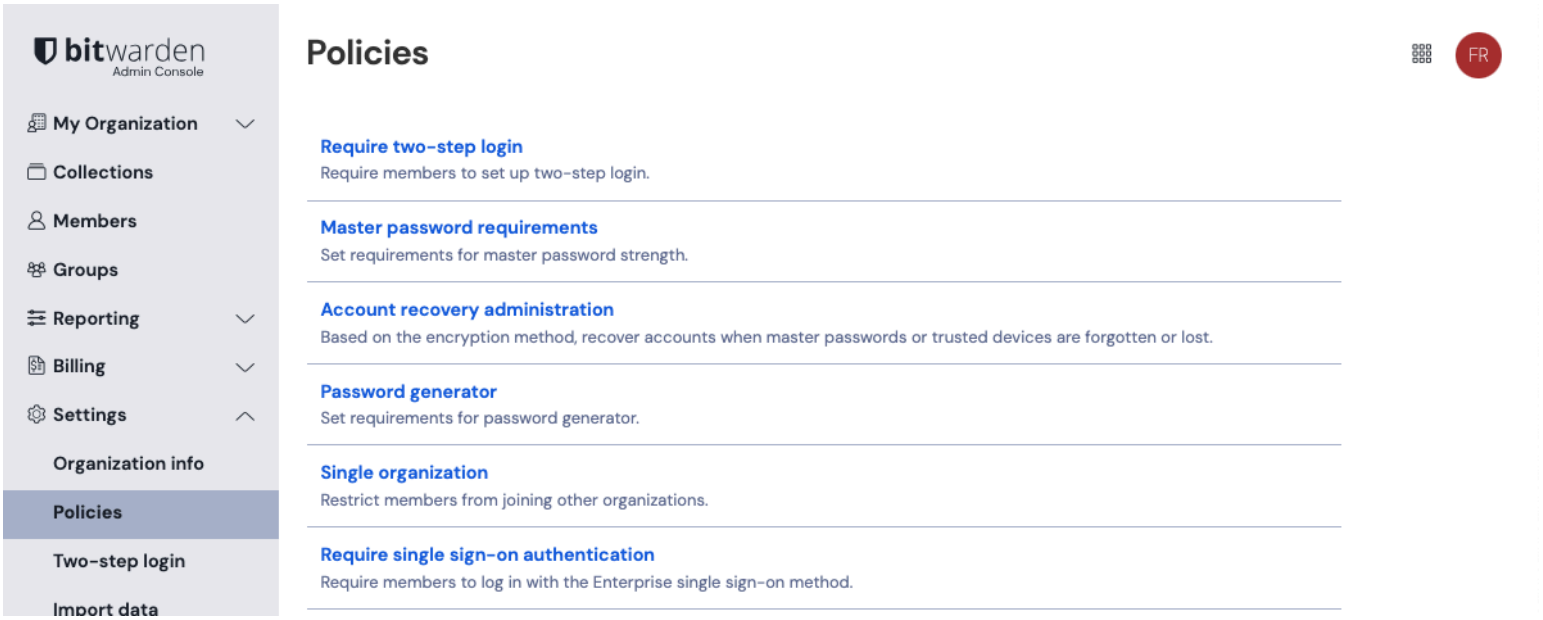
Les politiques de sécurité de l'Entreprise peuvent être définies par les admins ou les propriétaires de l'organisation.

Warning

Nous recommandons de définir les politiques de sécurité de l'entreprise avant d'inviter des utilisateurs à votre organisation. Certaines politiques de sécurité supprimeront les utilisateurs non conformes lorsqu'elles sont activées, et certaines ne sont pas rétroactivement applicables.

Définir les politiques de sécurité de l'Entreprise

Les politiques de sécurité peuvent être définies à partir de la console Admin en naviguant vers **Paramètres → Politiques de sécurité**:



Définir les politiques de sécurité

Politiques de sécurité disponibles

Exiger une authentification à deux facteurs

Activer la politique **Exiger une connexion en deux étapes** obligera les membres à utiliser une méthode de connexion en deux étapes pour accéder à leurs coffres. Si vous utilisez la fonctionnalité 2FA d'un fournisseur d'identité ou d'un SSO, vous n'avez pas besoin d'activer cette politique de sécurité. Cette politique est appliquée même pour les utilisateurs qui n'ont que accepté l'invitation à votre organisation.

Warning

Les membres de l'organisation qui ne sont ni propriétaires ni admins et qui n'ont pas configuré l'identifiant en deux étapes pour leur compte seront retirés de l'organisation lorsque vous activerez cette politique de sécurité. Les utilisateurs qui sont supprimés à la suite de cette politique seront informés par courriel et devront être à nouveau invités à rejoindre l'organisation. Informations supplémentaires:

- L'utilisateur existant ne pourra pas accepter l'invitation, y compris une invitation à être propriétaire ou admin, jusqu'à ce que la connexion en deux étapes soit activée pour leur coffre.
- Les nouveaux utilisateurs seront automatiquement configurés avec un identifiant en deux étapes basé sur le courriel, mais peuvent changer cela à tout moment.

Exigences du mot de passe principal

Activer la politique de **exigences du mot de passe principal** imposera un ensemble configurable de conditions minimales pour la force du mot de passe principal des utilisateurs. Les organisations peuvent appliquer :

- Complexité minimale du mot de passe principal
- Longueur minimale du mot de passe principal
- Types de caractères requis

La complexité du mot de passe est calculée sur une échelle de 0 (faible) à 4 (fort). Bitwarden calcule la complexité du mot de passe en utilisant la bibliothèque zxcvbn.

Utilisez l'option **Exiger que les membres existants changent leurs mots de passe** pour exiger des membres existants non conformes de l'organisation, quel que soit leur rôle, de mettre à jour leur mot de passe principal lors de leur prochain identifiant. Les utilisateurs qui créent un nouveau compte à partir de l'invitation de l'organisation seront invités à créer un mot de passe principal qui répond à vos exigences.

Administration de récupération du compte

Activer la politique de **Administration de la récupération de compte** permettra aux propriétaires et aux admins d'utiliser la réinitialisation du mot de passe pour réinitialiser le mot de passe principal des utilisateurs inscrits. Par défaut, les utilisateurs devront se inscrire eux-

mêmes à la réinitialisation du mot de passe, cependant l'option d'inscription automatique peut être utilisée pour forcer l'inscription automatique des utilisateurs invités.

La politique d'administration de récupération de compte est nécessaire pour que votre organisation utilise SSO avec des appareils de confiance.

> **Note**
>
> La politique de la **seule organisation** doit être activée avant d'activer cette politique.
>
> En conséquence, vous devez désactiver la politique de **gestion de récupération de compte** avant de pouvoir désactiver la politique de **organisation unique**.

Inscription automatique

Activer l'option **inscription automatique** inscrira automatiquement tous les nouveaux membres, quel que soit leur rôle, à la réinitialisation du mot de passe lorsque leur invitation à rejoindre l'organisation est acceptée et les empêchera de se retirer.

> **Note**
>
> Les utilisateurs déjà dans l'organisation ne seront pas inscrits rétroactivement à la réinitialisation du mot de passe, et devront s'inscrire eux-mêmes.

Générateur de mot de passe

Activer la politique du **générateur de mot de passe** imposera un ensemble configurable de exigences minimales pour tous les mots de passe générés par l'utilisateur pour tous les membres, quel que soit leur rôle. Les organisations peuvent appliquer :

- Mot de passe, phrase secrète, ou préférence utilisateur

Pour les mots de passe:

- Longueur minimale du mot de passe
- Nombre minimum (0-9) décompte
- Nombre minimum de caractères spéciaux (!@#$%^&*)

- Types de caractères requis

Pour les phrases secrètes :

- Nombre minimum de mots
- Que ce soit pour mettre en majuscule
- Que ce soit pour inclure des nombres

Warning

Les mots de passe existants non conformes **ne seront pas** modifiés lorsque cette politique de sécurité est activée, ni les éléments ne seront retirés de l'organisation. Lors de la modification ou de la génération d'un mot de passe après l'activation de cette politique, les règles de politique configurées seront appliquées.

Une bannière est affichée aux utilisateurs sur l'écran du générateur de mot de passe pour indiquer qu'une politique de sécurité affecte leurs paramètres de générateur.

Organisation Unique

L'activation de la politique de la **Organisation unique** empêchera les membres non-propriétaires/non-admin de votre organisation de pouvoir rejoindre d'autres organisations, ou de créer d'autres organisations. Cette politique est appliquée même pour les utilisateurs qui ont seulement accepté l'invitation à votre organisation, cependant cette politique n'est pas appliquée pour les propriétaires et les admins.

Warning

Les utilisateurs dans l'organisation qui sont membres de plusieurs organisations seront retirés de votre organisation lorsque vous activez cette politique de sécurité.

Les utilisateurs qui sont supprimés en raison de cette politique seront informés par courriel et devront être à nouveau invités à rejoindre l'organisation. Les utilisateurs ne pourront pas accepter l'invitation à l'organisation tant qu'ils ne se seront pas retirés de toutes les autres organisations.

Authentification par Connexion Unique (Single Sign-On)

Activer la politique **"Exiger l'authentification unique"** obligera les utilisateurs non-propriétaires/non-admin à se connecter avec SSO. Si vous êtes auto-hébergé, vous pouvez appliquer cette politique de sécurité pour les propriétaires et les admins en utilisant une variable d'environnement. Pour plus d'informations, voir Utilisation de l'identifiant avec SSO. Cette politique de sécurité n'est pas appliquée pour les propriétaires et les admins.

Les membres des organisations utilisant cette politique ne pourront pas se connecter avec des clés de passe.

> **Note**
>
> La politique de la **seule organisation** doit être activée avant d'activer cette politique.
>
> En conséquence, vous devez désactiver la politique **Exiger une authentification unique** avant de pouvoir désactiver la politique **Organisation unique**.

Supprimer le coffre individuel

L'activation de la politique **Supprimer le coffre individuel** obligera les utilisateurs non-propriétaires/non-admin à enregistrer les éléments du coffre dans une organisation en empêchant la propriété des éléments du coffre pour les membres de l'organisation.

Une bannière est affichée aux utilisateurs sur l'écran **Ajouter un élément** indiquant qu'une politique de sécurité affecte leurs options de propriété.

Cette politique est appliquée même pour les utilisateurs qui ont seulement accepté l'invitation à votre organisation, cependant cette politique n'est pas appliquée pour les propriétaires et les admins.

> **Note**
>
> Les éléments du coffre qui ont été créés avant la mise en œuvre de cette politique de sécurité ou avant de rejoindre l'organisation resteront dans le coffre individuel de l'utilisateur.

Supprimer le Send

Activer la politique **Supprimer Send** empêchera les membres non-propriétaires/non-admin de créer ou d'éditer un Send en utilisant Bitwarden Send. Les membres soumis à cette politique pourront toujours supprimer les Sends existants qui n'ont pas encore atteint leur date de suppression. Cette politique de sécurité n'est pas appliquée pour les propriétaires et les admins.

Une bannière est affichée aux utilisateurs dans la vue **Send** et lors de l'ouverture de tout Send existant pour indiquer qu'une politique les limite à supprimer uniquement les Sends.

Options Send

Activer la politique des **options d'envoi** permettra aux propriétaires et aux admins de spécifier des options pour créer et éditer des envois. Cette politique de sécurité n'est pas appliquée pour les propriétaires et les admins. Les options comprennent :

Option	Description
Ne permettez pas aux utilisateurs de cacher leur adresse de courriel.	Activer cette option supprime l'option masquer le courriel, ce qui signifie que tous les Sends reçus indiqueront de qui ils sont envoyés.

Délai d'expiration du coffre

Définir la politique de **délai d'expiration du coffre** vous permettra de :

- Mettez en œuvre une durée maximale de délai d'expiration du coffre pour tous les membres de votre organisation **à l'exception des propriétaires**. Cette option applique la restriction de délai d'expiration à toutes les applications client (mobile, bureau, extension de navigateur, et plus encore).
- Définissez une action de délai d'expiration du coffre pour tous les membres de votre organisation **à l'exception des propriétaires**. Cette option peut être réglée sur **Préférence de l'utilisateur**, **Verrouiller** ou **Déconnexion** lorsqu'un délai d'expiration du coffre se produit.

  L'option **Déconnexion** peut être utilisée, par exemple, pour inciter les utilisateurs à utiliser le 2FA chaque fois qu'ils accèdent à leurs coffres et pour empêcher l'utilisation hors ligne en effaçant régulièrement les données locales des machines des utilisateurs.

Une bannière est affichée aux utilisateurs lors de la configuration du délai d'expiration du coffre, indiquant qu'une politique de sécurité affecte leurs options. Certaines options de délai d'expiration du coffre, comme **Au redémarrage du navigateur** ou **Jamais** ne seront pas disponibles pour les utilisateurs lorsque cette politique de sécurité est activée. Cette politique de sécurité n'est pas appliquée pour les propriétaires et les admins.

Note

La politique de la **seule organisation** doit être activée avant d'activer cette politique.

En conséquence, vous devez désactiver la politique de **délai d'expiration du coffre** avant de pouvoir désactiver la politique de **organisation unique**.

Supprimer l'exportation individuelle du coffre

Activer la politique **Supprimer l'exportation individuelle de coffre** interdira aux membres non-propriétaires/non-admin de votre organisation d'exporter les données de leur coffre individuel. Cette politique de sécurité n'est pas appliquée pour les propriétaires et les admins.

Dans le coffre Web et le CLI, un message est affiché aux utilisateurs indiquant qu'une politique de sécurité affecte leurs options. Dans d'autres clients, l'option sera simplement désactivée.

Activer la saisie automatique

Activer la politique de **Activation de la saisie automatique** activera automatiquement la fonctionnalité de saisie automatique lors du chargement de la page sur l'extension du navigateur pour tous les membres existants et nouveaux de l'organisation. Les membres pourront toujours désactiver ou modifier le comportement de la saisie automatique lors du chargement de la page pour leur extension de navigateur s'ils le souhaitent.