À propos de SCIM

À propos de SCIM

Le système de gestion d'identité inter-domaine (SCIM) peut être utilisé pour provisionner automatiquement des membres et des groupes dans votre organisation Bitwarden.

Les serveurs Bitwarden fournissent un point de terminaison SCIM qui, avec une clé API SCIM valide, acceptera les demandes de votre fournisseur d'identité (IdP) pour la provision et la déprovision des utilisateurs et du groupe.

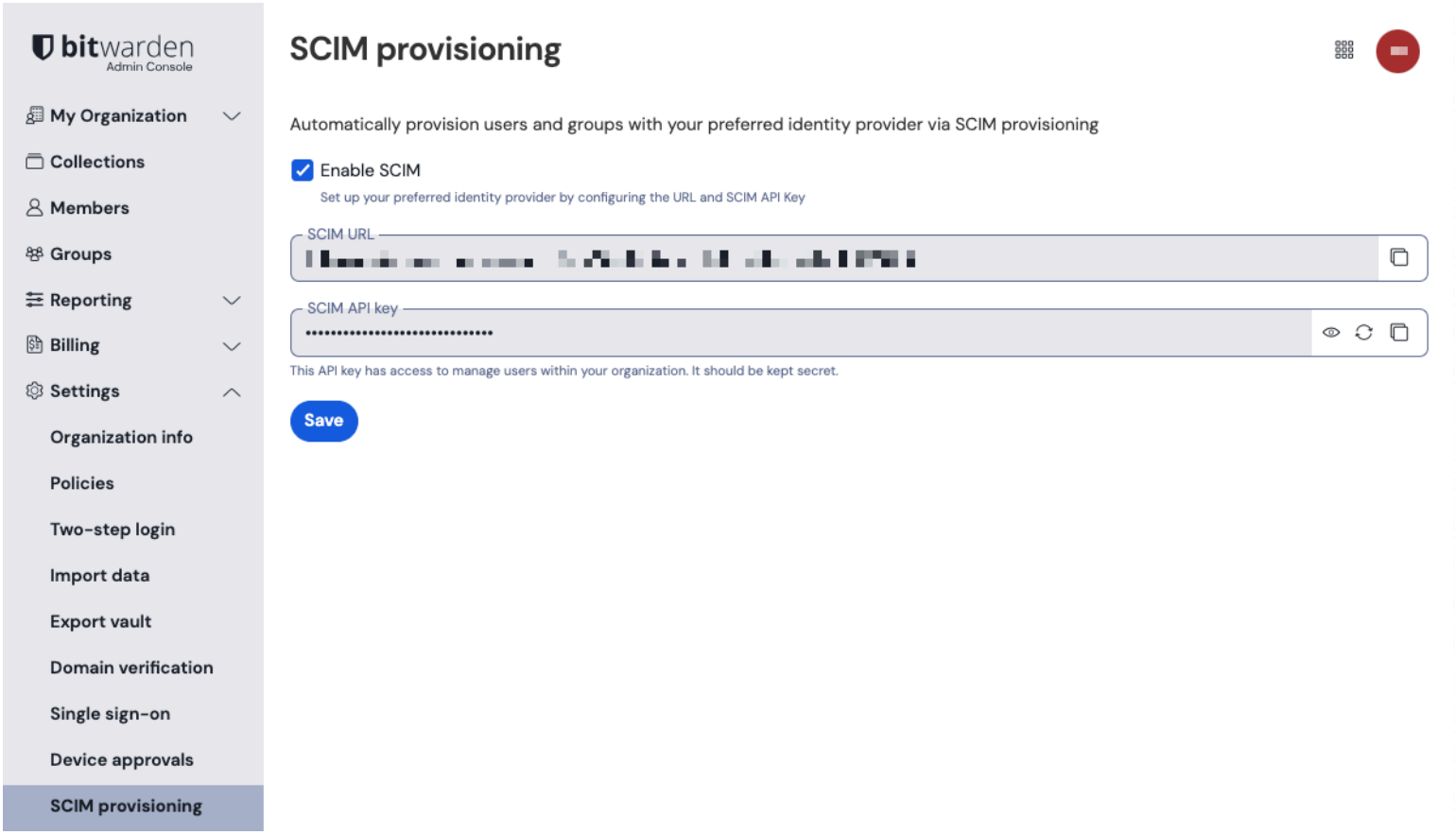
> **Note**
>
> Les intégrations SCIM sont disponibles pour les **organisations d'Entreprise**. Les organisations d'Équipes, ou les clients n'utilisant pas un fournisseur d'identité compatible SCIM, peuvent envisager d'utiliser Directory Connector comme moyen alternatif de provisionnement.

Bitwarden prend en charge SCIM v2 en utilisant des mappages d'attributs standard et propose des intégrations SCIM officielles pour :

- Azure Active Directory
- Okta
- OneLogin
- JumpCloud

Configuration de SCIM

Pour configurer SCIM, votre IdP aura besoin d'une URL SCIM et d'une clé API pour effectuer des demandes autorisées au serveur Bitwarden. Ces valeurs sont disponibles depuis la Console Admin en naviguant vers **Paramètres** → **Provisionnement SCIM**:



Provisionnement SCIM

> **Tip**
>
> Nous recommandons d'utiliser l'un de nos guides dédiés pour configurer une intégration SCIM entre Bitwarden et Azure AD, Okta, OneLogin, ou JumpCloud.

Attributs requis

Bitwarden utilise les noms d'attributs standard SCIM v2, listés ici, cependant chaque IdP peut utiliser des noms alternatifs qui sont mappés à Bitwarden lors de la provision.

Attributs de l'utilisateur

Pour chaque utilisateur, Bitwarden utilisera les attributs suivants :

- Une indication que l'utilisateur est `actif` (**requis**)
- `courriel`[a] ou `nom d'utilisateur` (**requis**)
- `nom d'affichage`
- `identifiant externe`

[a] – Parce que SCIM permet aux utilisateurs d'avoir plusieurs adresses de courriel exprimées sous forme de tableau d'objets, Bitwarden utilisera la `valeur` de l'objet qui contient `"primary": true`.

Attributs de groupe

Pour chaque groupe, Bitwarden utilisera les attributs suivants :

- `nomAffiché` (**requis**)
- `membres` [a]
- `identifiant externe`

[a] – `membres` est un tableau d'objets, chaque objet représentant un utilisateur dans ce groupe.

Révocation et restauration de l'accès

Une fois que les utilisateurs sont provisionnés dans Bitwarden à l'aide de SCIM, vous pouvez temporairement révoquer leur accès à votre organisation et à ses éléments de coffre. Lorsqu'un utilisateur est temporairement suspendu/désactivé dans votre IdP, son accès à votre organisation sera automatiquement révoqué.

> **Tip**
> Seuls les propriétaires peut révoquer et restaurer l'accès aux autres propriétaires.

Les utilisateurs dont l'accès a été révoqué sont répertoriés dans l'**onglet Révoqué** de l'écran **Membres** de l'organisation et feront :

- Ne pas avoir accès à aucun élément de coffre d'organisation, collections.
- Ne pas avoir la capacité d'utiliser SSO pour l'identifiant, ou Duo organisationnel pour l'identifiant en deux étapes.
- Ne pas être soumis aux politiques de sécurité de votre organisation.
- Ne pas occuper un siège de licence.

> **⚠ 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.

En savoir plus sur la révocation et la restauration de l'accès.

Événements SCIM

Votre organisation capturera les journaux d'événements pour les actions effectuées par les intégrations SCIM, y compris inviter des utilisateurs et supprimer des utilisateurs, ainsi que créer ou supprimer des groupes. Les événements dérivés de SCIM enregistreront `SCIM` dans la colonne **Membre**.

Utilisateurs et groupes préexistants

Les organisations avec des utilisateurs et des groupes qui ont été intégrés avant l'activation de SCIM, soit manuellement soit en utilisant le connecteur de répertoire, devraient noter ce qui suit :

	...qui existe dans l'IdP.	...qui n'existe pas dans l'IdP.
Utilisateur préexistant	•Ne sera pas dupliqué •Ne sera pas forcé de rejoindre à nouveau l'organisation •Ne sera pas retiré des groupes dont ils sont déjà membre	•Ne sera pas retiré de l'organisation •N'aura pas d'adhésions de groupe ajoutées ou supprimées
Groupe préexistant	•Ne sera pas dupliqué •Aura des membres ajoutés selon l'IdP •Ne supprimera pas les membres préexistants	•Ne sera pas retiré de l'organisation •Ne verra pas de membres ajoutés ou supprimés

Note

If you are using Directory Connector, make sure to turn syncing off before activating SCIM.