bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > GESTION DES UTILISATEURS >

Intégration Okta SCIM

Afficher dans le centre d'aide:
https://bitwarden.com/help/okta-scim-integration/

Intégration Okta SCIM

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

> **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.

Cet article vous aidera à configurer une intégration SCIM avec Okta. La configuration implique de travailler simultanément avec le coffre web Bitwarden et le portail admin Okta. Au fur et à mesure que vous avancez, nous vous recommandons d'avoir les deux facilement disponibles et de compléter les étapes dans l'ordre où elles sont documentées.

Fonctionnalités prises en charge

Les fonctionnalités de provisionnement suivantes sont prises en charge par cette intégration :

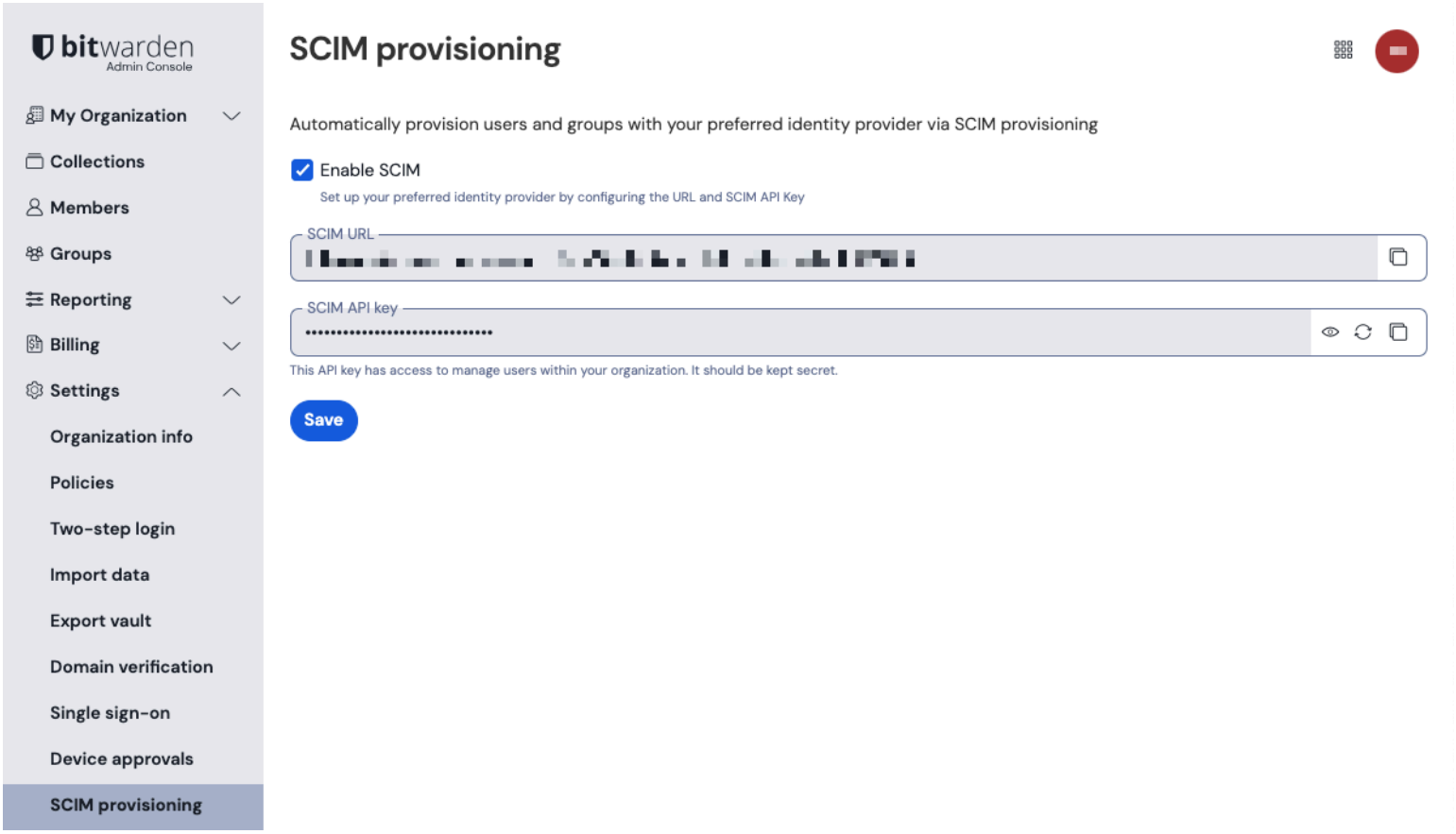
- **Utilisateurs poussés :** Les utilisateurs dans Okta qui sont assignés à Bitwarden sont ajoutés en tant qu'utilisateurs dans Bitwarden.
- **Désactiver les utilisateurs:** Quand les utilisateurs sont désactivés dans Okta, ils seront désactivés dans Bitwarden.
- **Pousser les groupes:** Les groupes et leurs utilisateurs dans Okta peuvent être poussés vers Bitwarden.

> **Note**
>
> Please note, Bitwarden does not support changing a user's email address once provisioned. Bitwarden also does not support changing a user's email address type, or using a type other than `primary`. The values entered for email and username should be the same. Learn more.

Activer SCIM

> **Note**
>
> **Hébergez-vous vous-même Bitwarden?** Si c'est le cas, terminez ces étapes pour activer SCIM pour votre serveur avant de continuer.

Pour commencer votre intégration SCIM, ouvrez la Console Admin et naviguez vers **Paramètres** → **Provisionnement SCIM**:

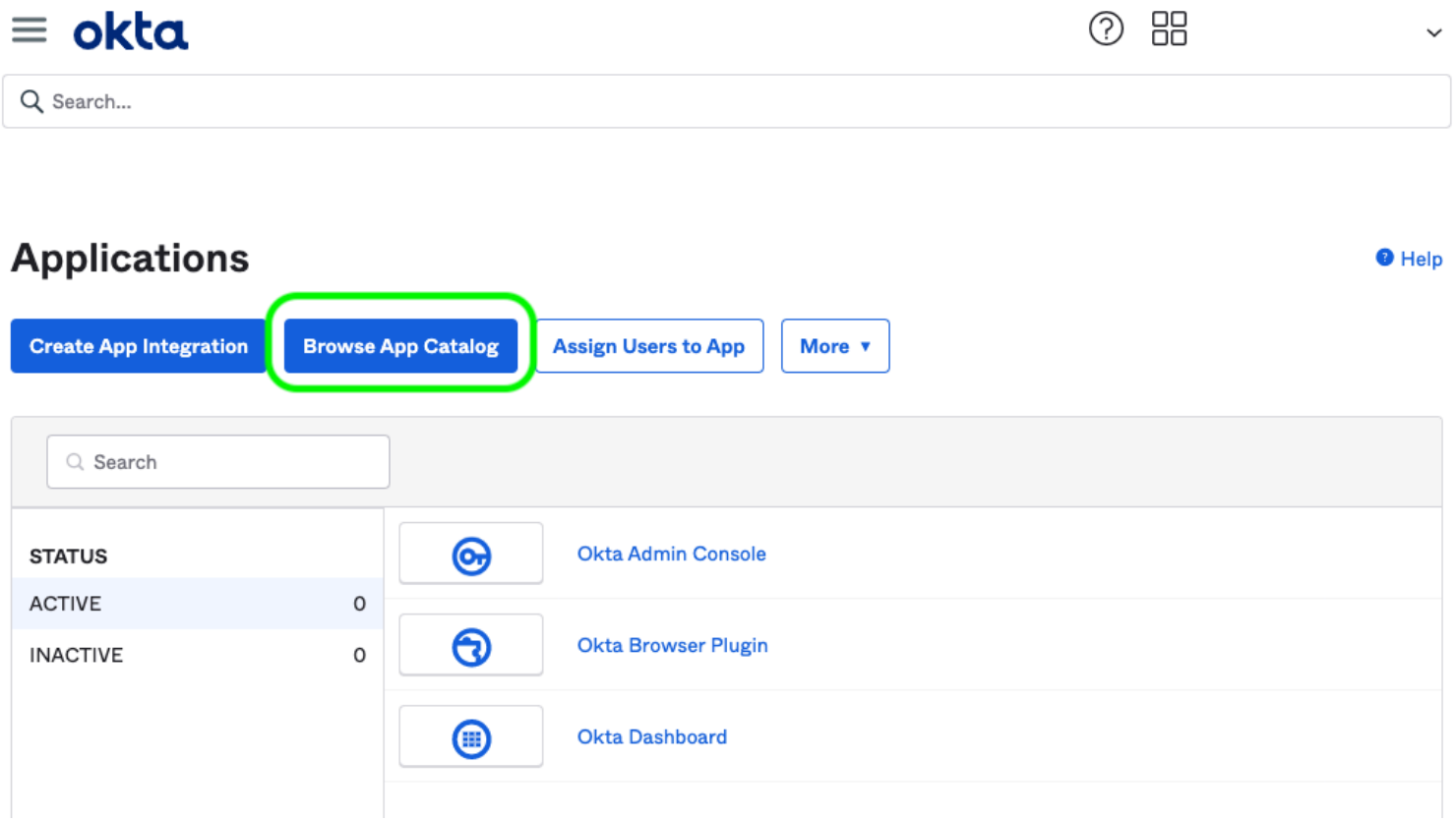


Provisionnement SCIM

Sélectionnez la case à cocher **Activer SCIM** et prenez note de votre **URL SCIM** et de votre **Clé API SCIM**. Vous devrez utiliser les deux valeurs dans une étape ultérieure.

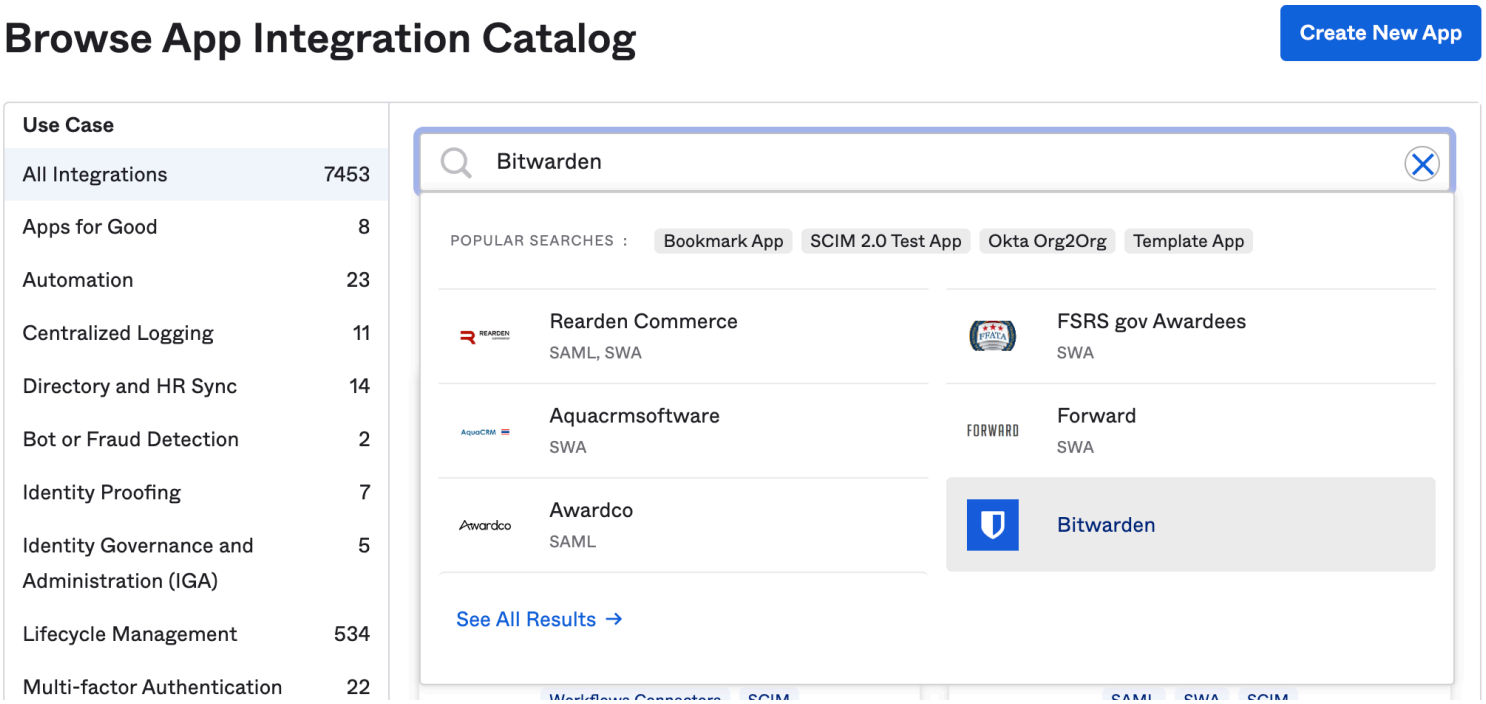
Ajoutez l'application Bitwarden

Dans le Portail Admin Okta, sélectionnez **Applications** → **Applications** à partir de la navigation. Sur l'écran de l'application, sélectionnez le bouton **Parcourir le catalogue d'applications** :



Browse App Catalog

Dans la barre de recherche, entrez `Bitwarden` et sélectionnez **Bitwarden** :



Bitwarden Okta App

Sélectionnez le bouton **Ajouter une intégration** pour procéder à la configuration.

Paramètres généraux

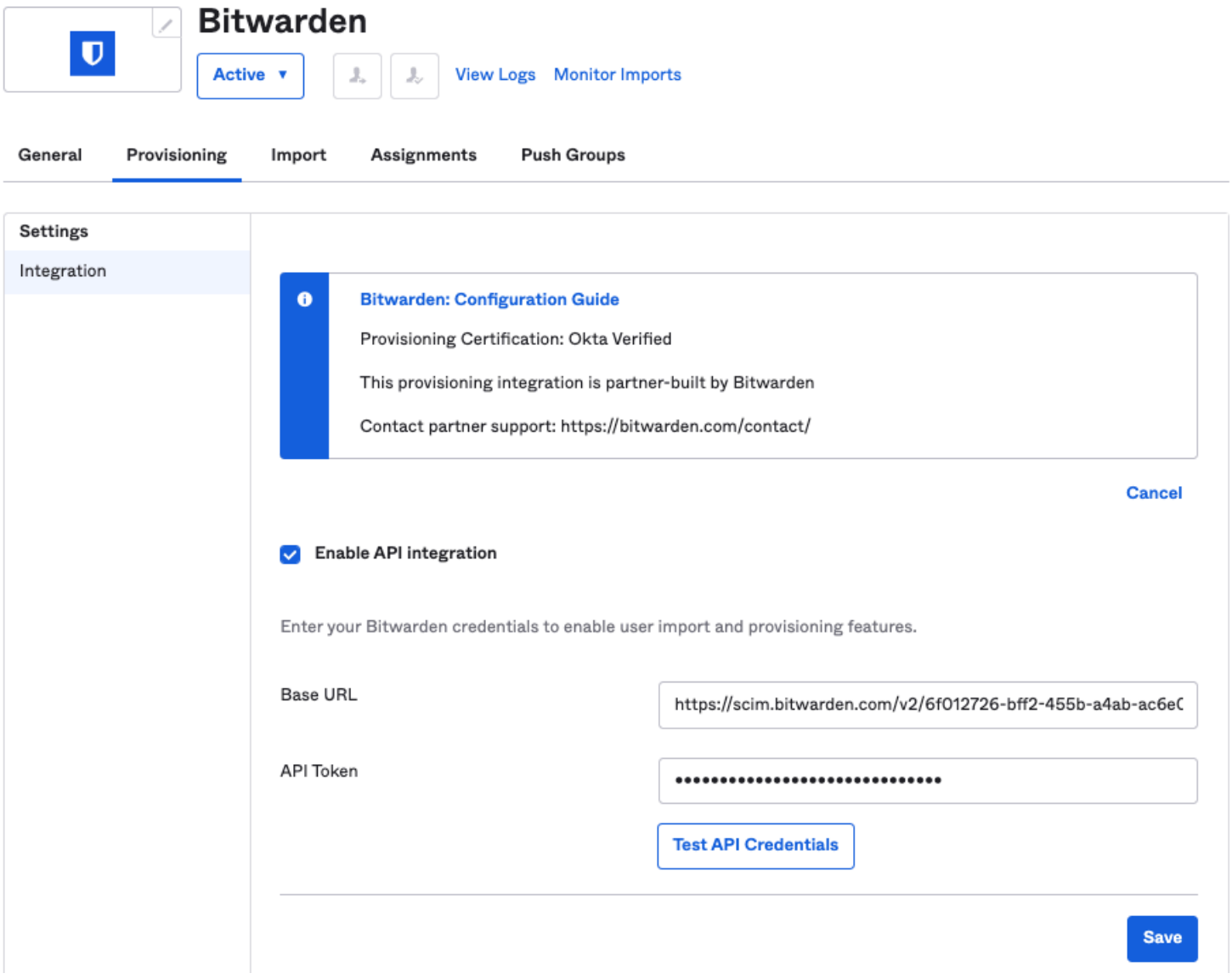
Sur l'**onglet Paramètres Généraux**, donnez à l'application une étiquette unique, spécifique à Bitwarden. Cochez les options **Ne pas afficher l'icône de l'application aux utilisateurs** et **Ne pas afficher l'icône de l'application dans l'application mobile Okta** et sélectionnez **Terminé**.

Configuration de la provision

Paramètres de provisionnement

Ouvrez l'**Approvisionnement** onglet et sélectionnez le bouton **Configurer l'intégration API** .

Une fois sélectionné, Okta vous proposera quelques options à configurer :



Configure API Integration

1. Cochez la case **Activer l'intégration API**.

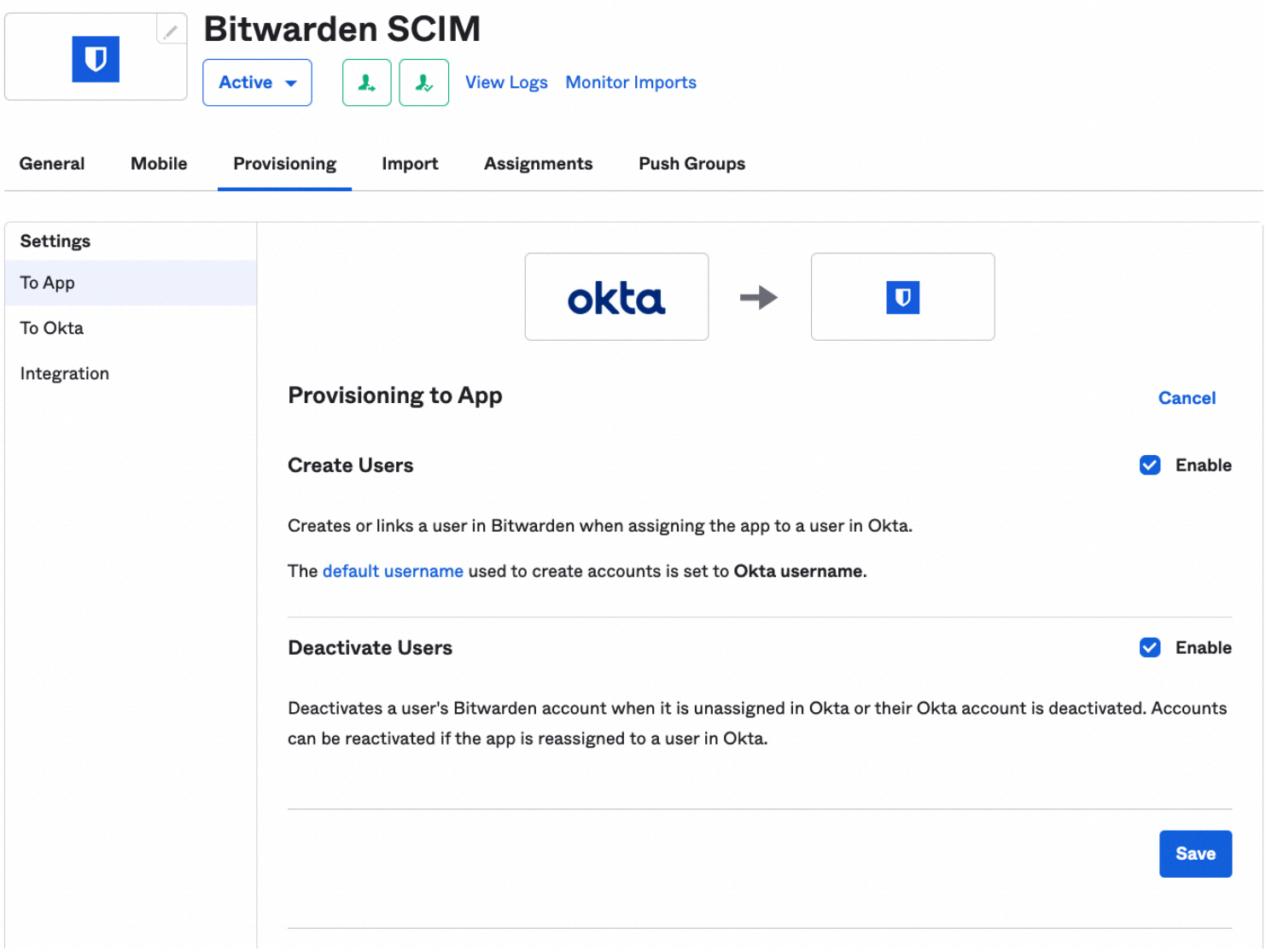
2. Dans le champ **URL de base**, entrez votre URL SCIM, qui peut être trouvée sur l'écran de provisionnement SCIM (en savoir plus).

3. Dans le champ **Jeton API**, entrez votre clé API SCIM (en savoir plus).

Une fois que vous avez terminé, utilisez le bouton **Tester les identifiants API** pour tester votre configuration. Si cela passe le test, sélectionnez le bouton **Enregistrer**.

Définir les actions de provisionnement

Sur l'écran **Provisionnement** → **Vers l'application**, sélectionnez le bouton **Éditer** :



Provisioning To App

Activez, au minimum, **Créer des utilisateurs** et **Désactiver des utilisateurs**. Sélectionnez **Enregistrer** lorsque vous avez terminé.

Devoirs

Ouvrez l'onglet **Assignations** et utilisez le menu déroulant Assigner pour attribuer des personnes ou des groupes à l'application. Les utilisateurs et groupes assignés recevront automatiquement une invitation. Selon votre flux de travail, vous devrez peut-être utiliser l'onglet **Push Groups** pour déclencher la provision du groupe une fois qu'ils sont attribués.

Terminez l'intégration de l'utilisateur

Maintenant que vos utilisateurs ont été provisionnés, ils recevront des invitations à rejoindre l'organisation. Instructez vos utilisateurs à accepter l'invitation et, une fois qu'ils l'ont fait, confirmez-les à l'organisation.

> **Note**
>
> The Invite → Accept → Confirm workflow facilitates the decryption key handshake that allows users to securely access organization vault data.