

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**:

bitwarden Admin Console

- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
 - Organization info
 - Policies
 - Two-step login
 - Import data
 - Export vault
 - Domain verification
 - Single sign-on
 - Device approvals
 - SCIM provisioning**

SCIM provisioning



Automatically provision users and groups with your preferred identity provider via SCIM provisioning

Enable SCIM

Set up your preferred identity provider by configuring the URL and SCIM API Key

SCIM URL

SCIM API key

This API key has access to manage users within your organization. It should be kept secret.

Save

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** :

🔍 Search...

Applications

📄 Help

Create App Integration

Browse App Catalog

Assign Users to App

More ▾

🔍 Search

STATUS

ACTIVE 0

INACTIVE 0



Okta Admin Console



Okta Browser Plugin



Okta Dashboard

Browse App Catalog

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

Browse App Integration Catalog

Create New App

Use Case

All Integrations 7453

Apps for Good 8

Automation 23

Centralized Logging 11

Directory and HR Sync 14

Bot or Fraud Detection 2

Identity Proofing 7

Identity Governance and Administration (IGA) 5

Lifecycle Management 534

Multi-factor Authentication 22

🔍 Bitwarden

POPULAR SEARCHES : Bookmark App SCIM 2.0 Test App Okta Org2Org Template App



Rearden Commerce
SAML, SWA



FSRS gov Awardees
SWA



Aquacrmsoftware
SWA



Forward
SWA



Awardco
SAML



Bitwarden

[See All Results →](#)

Workflow Connectors SCIM SAML SWA SCIM

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 :

The screenshot shows the Bitwarden integration configuration page in Okta. At the top, there is a header for 'Bitwarden' with an 'Active' dropdown, two user icons, and links for 'View Logs' and 'Monitor Imports'. Below this is a navigation bar with tabs for 'General', 'Provisioning' (selected), 'Import', 'Assignments', and 'Push Groups'. On the left, a 'Settings' sidebar has 'Integration' selected. The main content area features a 'Bitwarden: Configuration Guide' box with an information icon, stating 'Provisioning Certification: Okta Verified' and providing a contact link. Below this is a checkbox for 'Enable API integration' which is checked. A text prompt asks for Bitwarden credentials. There are input fields for 'Base URL' (containing 'https://scim.bitwarden.com/v2/6f012726-bff2-455b-a4ab-ac6eC') and 'API Token' (masked with dots). A 'Test API Credentials' button is located below the API token field. At the bottom right, there is a 'Save' button.

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** :

The screenshot shows the Bitwarden SCIM configuration interface. At the top, there's a header for "Bitwarden SCIM" with an "Active" status, two user icons, and links for "View Logs" and "Monitor Imports". Below this is a navigation bar with tabs: "General", "Mobile", "Provisioning" (selected), "Import", "Assignments", and "Push Groups". On the left, a sidebar lists "Settings", "To App" (selected), "To Okta", and "Integration". The main content area shows a diagram of "okta" pointing to the Bitwarden logo. Below the diagram, there are two sections: "Provisioning to App" with a "Cancel" button, and "Create Users" with an "Enable" checkbox checked. A description for "Create Users" states: "Creates or links a user in Bitwarden when assigning the app to a user in Okta. The default username used to create accounts is set to Okta username." Below that is the "Deactivate Users" section with an "Enable" checkbox checked. A description for "Deactivate Users" states: "Deactivates a user's Bitwarden account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta." At the bottom right, there is a "Save" button.

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.