

CONSOLE ADMIN > GESTION DES UTILISATEURS >

# Intégration SCIM OneLogin

Afficher dans le centre d'aide:

<https://bitwarden.com/help/onelogin-scim-integration/>

## Intégration SCIM OneLogin

Le système de gestion d'identité inter-domaine (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 OneLogin. La configuration implique de travailler simultanément avec le coffre web Bitwarden et le portail admin OneLogin. Au fur et à mesure que vous avancez, nous vous recommandons d'avoir les deux à portée de main et de compléter les étapes dans l'ordre où elles sont documentées.

## 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**:

**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  
[Alphanumeric string]

SCIM API key  
[Masked key]

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

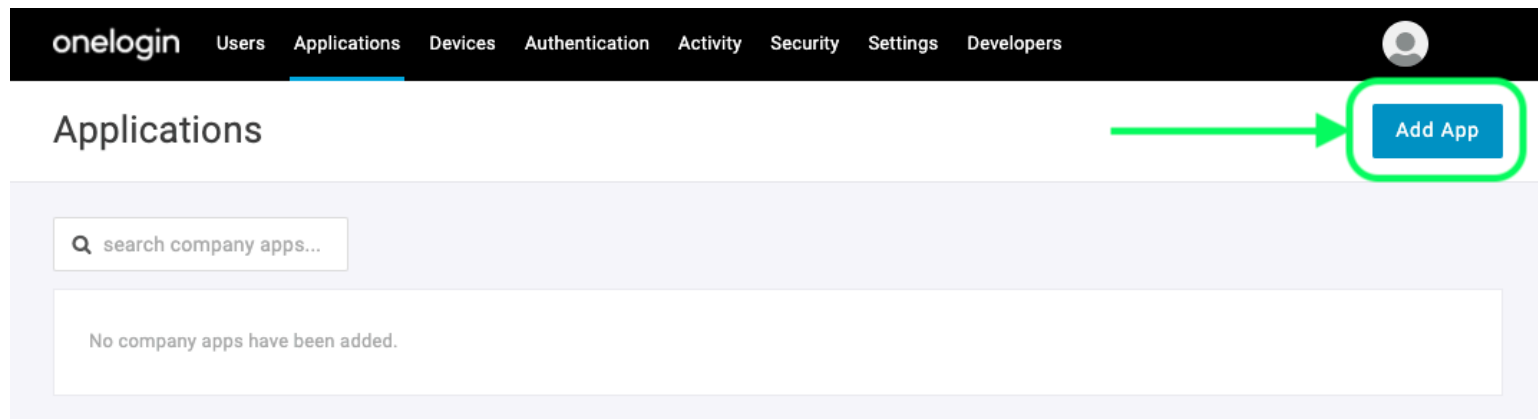
Save

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.

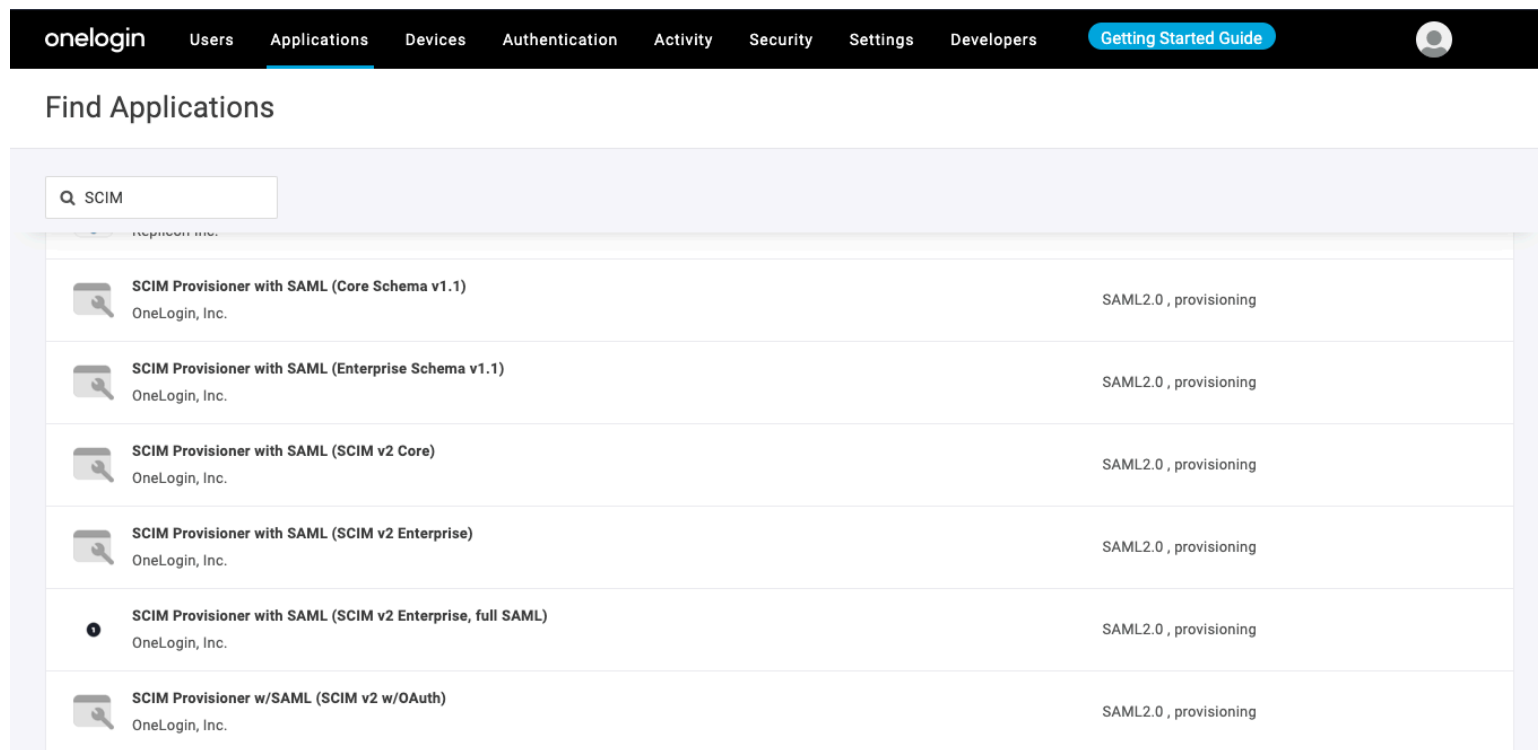
## Créez une application OneLogin

Dans le portail OneLogin, naviguez vers l'écran **Applications** et sélectionnez le bouton **Ajouter une application** :



*Add an Application*

Dans la barre de recherche, saisissez **SCIM** et sélectionnez l'application **Provisionneur SCIM avec SAML (SCIM v2 Entreprise)** :



*SCIM Provisioner App*

Donnez à votre application un **Nom d'affichage** spécifique à Bitwarden et sélectionnez le bouton **Enregistrer**.

## Configuration

Sélectionnez **Configuration** depuis la navigation à gauche et configurez les informations suivantes, dont certaines que vous devrez récupérer depuis les écrans de Single Sign-On et de Provisionnement SCIM dans Bitwarden.

onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Getting Started Guide

Applications /
SCIM Provisioner with SAML (SCIM v2 Enterprise)

More Actions ▾
Save

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

### Application details

SAML Audience URL

SAML Consumer URL

### API Connection

API Status

● Disabled
Enable

SCIM Base URL

SCIM JSON Template

SCIM App Configuration

## Détails de l'application

OneLogin vous demandera de remplir les champs **URL de l'audience SAML** et **URL du consommateur SAML** même si vous n'allez pas utiliser la connexion unique. [Découvrez quoi saisir dans ces champs](#) .

## Connexion API

Entrez les valeurs suivantes dans la section **Connexion API** :

Paramètres de l'application	Description
URL de base SCIM	Définissez ce champ sur l'URL SCIM ( <a href="#">en savoir plus</a> ).
Jeton porteur SCIM	Définissez ce champ sur la clé API SCIM ( <a href="#">en savoir plus</a> ).

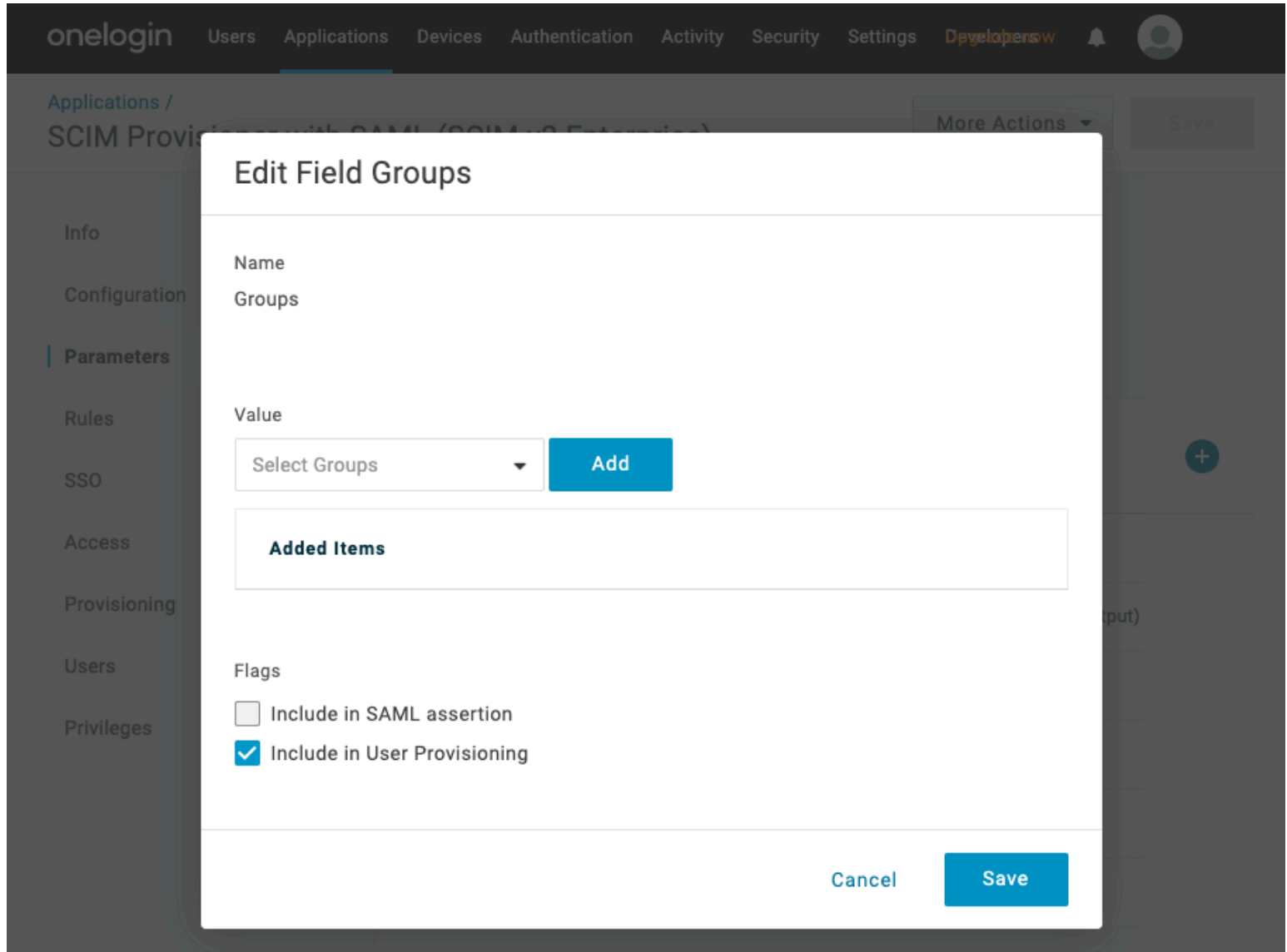
Sélectionnez **Enregistrer** une fois que vous avez configuré ces champs.

## Accès

Sélectionnez **Accès** dans la navigation à gauche. Dans la section **Rôles**, attribuez l'accès à l'application à tous les rôles que vous souhaitez provisionner dans Bitwarden. Chaque rôle est traité comme un groupe dans votre organisation Bitwarden, et les utilisateurs assignés à n'importe quel rôle seront inclus dans chaque groupe, y compris s'ils sont assignés à plusieurs rôles.

## Paramètres

Sélectionnez **Paramètres** de la navigation à gauche. Sélectionnez **Groupes** de la table, activez la case à cocher **Inclure dans la Provision d'Utilisateur**, et sélectionnez le bouton **Enregistrer** :



*Include Groups in User Provisioning*

## Règles

Créez une règle pour mapper les rôles OneLogin aux groupes Bitwarden :

1. Sélectionnez **Règles** de la navigation à gauche.
2. Sélectionnez le bouton Ajouter une règle pour ouvrir la boîte de dialogue **Nouveau mappage** :

More Actions ▾

## New mapping

---

**Name**

Create Groups from Roles

**Conditions**

No conditions. Actions will apply to all users.

+

**Actions**

Set Groups in SCIM - SCIMonelogin - AJ ▾

From Existing

Map from OneLogin

For each role ▾ with value that matches .\*

set SCIM - SCIMonelogin - AJ Groups named after **roles**.

+

Cancel
Save

*Role/Group Mapping*

3. Donnez à la règle un **Nom** comme Créer des Groupes à partir des Règles.
4. Laissez **Conditions** vide.
5. Dans la section **Actions** :
  1. Sélectionnez **Définir les groupes dans** dans le premier menu déroulant.
  2. Sélectionnez l'option **Carte de OneLogin**.
  3. Sélectionnez **rôle** dans le menu déroulant "Pour chaque".
  4. Entrez .\* dans le champ "avec une valeur qui correspond" pour mapper tous les rôles aux groupes, ou entrez un nom de rôle spécifique.

6. Sélectionnez le bouton **Enregistrer** pour terminer la création de la règle.

## Tester la connexion

Sélectionnez **Configuration** depuis la navigation à gauche, et sélectionnez le bouton **Activer** sous **Statut de l'API** :

The screenshot shows the OneLogin interface for configuring a SCIM Provisioner with SAML (SCIM v2 Enterprise). The navigation bar includes 'onelogin', 'Users', 'Applications', 'Devices', 'Authentication', 'Activity', 'Security', 'Settings', 'Developers', and a 'Getting Started Guide' button. The left sidebar has 'Info', 'Configuration', 'Parameters', and 'Rules'. The main content area is titled 'SCIM Provisioner with SAML (SCIM v2 Enterprise)' and has 'More Actions' and 'Save' buttons. Under 'API Connection', the 'API Status' is 'Enabled' (indicated by a green dot) with a 'Disable' button. Below that is the 'SCIM Base URL' field and a 'Test API Connection' button.

Ce test **ne commencera pas** la provision, mais fera une requête GET à Bitwarden et affichera **Activé** si l'application obtient une réponse de Bitwarden avec succès.

## Activer la provision

Sélectionnez **Provisioning** dans la navigation à gauche :

Applications /

SCIM Provisioner with SAML (SCIM v2 Enterprise)

- Info
- Configuration
- Parameters
- Rules
- SSO
- Access
- Provisioning**
- Users
- Privileges

### Workflow

Enable provisioning

Require admin approval before this action is performed

Create user

Delete user

Update user

When users are deleted in OneLogin, or the user's app access is removed, perform the below action

Delete ▼

When user accounts are suspended in OneLogin, perform the following action:

Suspend ▼

### Entitlements

[Refresh](#)

ⓘ Entitlements are user attributes that are usually associated with fine-grained app access, like app group, department, organization, or license level. When you click [Refresh](#), OneLogin imports your organization's app entitlement values (such as group names or license types) so you can map them to OneLogin attribute values. Entitlement refresh can take several minutes. Check Activity > Events for completion status.

*Provisioning Settings*

Sur cet écran :

1. Sélectionnez la case à cocher **Activer la Provision** .
2. Dans le menu déroulant **Lorsque les utilisateurs sont supprimés dans OneLogin...** , sélectionnez **Supprimer**.
3. Dans le menu déroulant **Quand les comptes utilisateurs sont suspendus dans OneLogin...**, sélectionnez **Suspendre**.

Lorsque vous avez terminé, sélectionnez **Enregistrer** pour déclencher la provision.

## Terminez l'intégration de l'utilisateur

Maintenant que vos utilisateurs ont été provisionnés, ils recevront des invitations pour 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.



## Annexe

### Attributs de l'utilisateur

Bitwarden et l'application **SCIM Provisioner avec SAML (SCIM v2 Entreprise)** de OneLogin utilisent des noms d'attributs SCIM v2 standard. Bitwarden utilisera les attributs suivants :

- `actif`
- `courrielsa` ou `nom d'utilisateur`
- `nom d'affichage`
- `identifiant externe`

<sup>a</sup> - 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`.