

BEHEERCONSOLE > GEBRUIKERSBEHEER >

# OneLogin SCIM integratie

Weergeven in het Helpcentrum:

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

## OneLogin SCIM integratie

System for cross-domain identity management (SCIM) kan worden gebruikt om leden en groepen in uw Bitwarden-organisatie automatisch te provisioneren en de-provisioneren.

### Note

SCIM-integraties zijn beschikbaar voor **Enterprise-organisaties**. Teams organisaties, of klanten die geen SCIM-compatibele identity provider gebruiken, kunnen overwegen [Directory Connector](#) te gebruiken als een alternatieve manier van provisioning.

Dit artikel helpt je bij het configureren van een SCIM integratie met OneLogin. Bij de configuratie wordt tegelijkertijd gewerkt met de Bitwarden webkluis en het OneLogin beheerportaal. We raden u aan om beide documenten bij de hand te hebben en de stappen uit te voeren in de volgorde waarin ze zijn beschreven.

## SCIM inschakelen

### Note

**Host je Bitwarden zelf?** Zo ja, voer dan deze stappen uit [om SCIM in te schakelen voor uw server](#) voordat u verdergaat.

Om uw SCIM-integratie te starten, opent u de beheerconsole en navigeert u naar **Instellingen** → **SCIM-provisioning**:

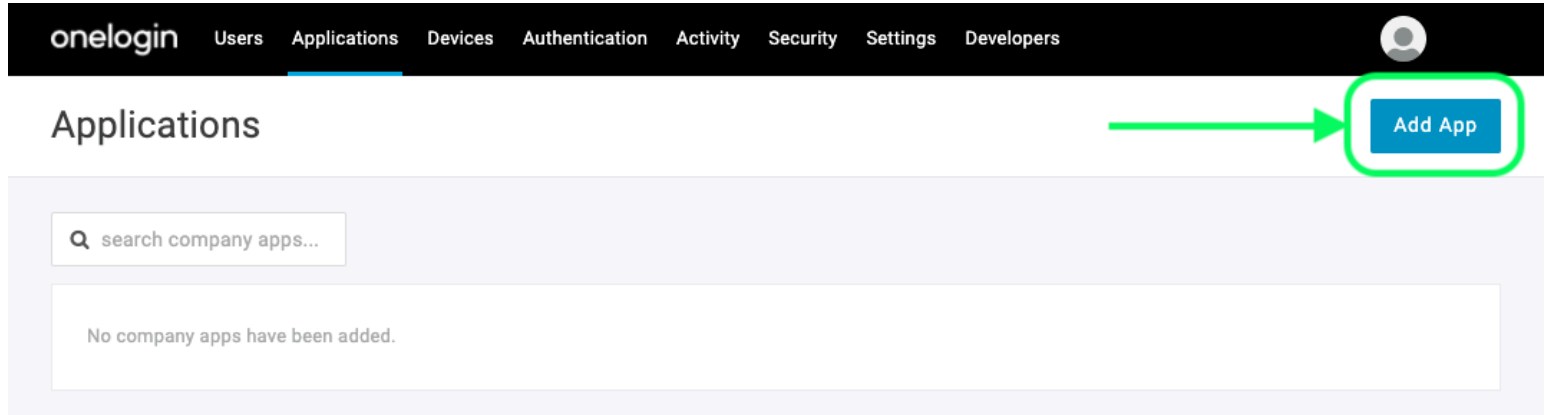
The screenshot shows the Bitwarden Admin Console interface. On the left is a sidebar with navigation options: My Organization, Collections, Members, Groups, Reporting, Billing, and Settings. The 'Settings' menu is expanded, showing options like Organization info, Policies, Two-step login, Import data, Export vault, Domain verification, Single sign-on, Device approvals, and SCIM provisioning (which is highlighted). The main content area is titled 'SCIM provisioning' and contains the following elements: a sub-header 'Automatically provision users and groups with your preferred identity provider via SCIM provisioning', a checked checkbox for 'Enable SCIM' with a sub-note 'Set up your preferred identity provider by configuring the URL and SCIM API Key', a text input field for 'SCIM URL' containing a masked URL, a text input field for 'SCIM API key' containing a masked key, a warning note 'This API key has access to manage users within your organization. It should be kept secret.', and a blue 'Save' button.

### SCIM-voorziening

Schakel het selectievakje **Enable SCIM in** en noteer uw **SCIM URL** en **SCIM API Key**. Je zult beide waarden in een latere stap moeten gebruiken.

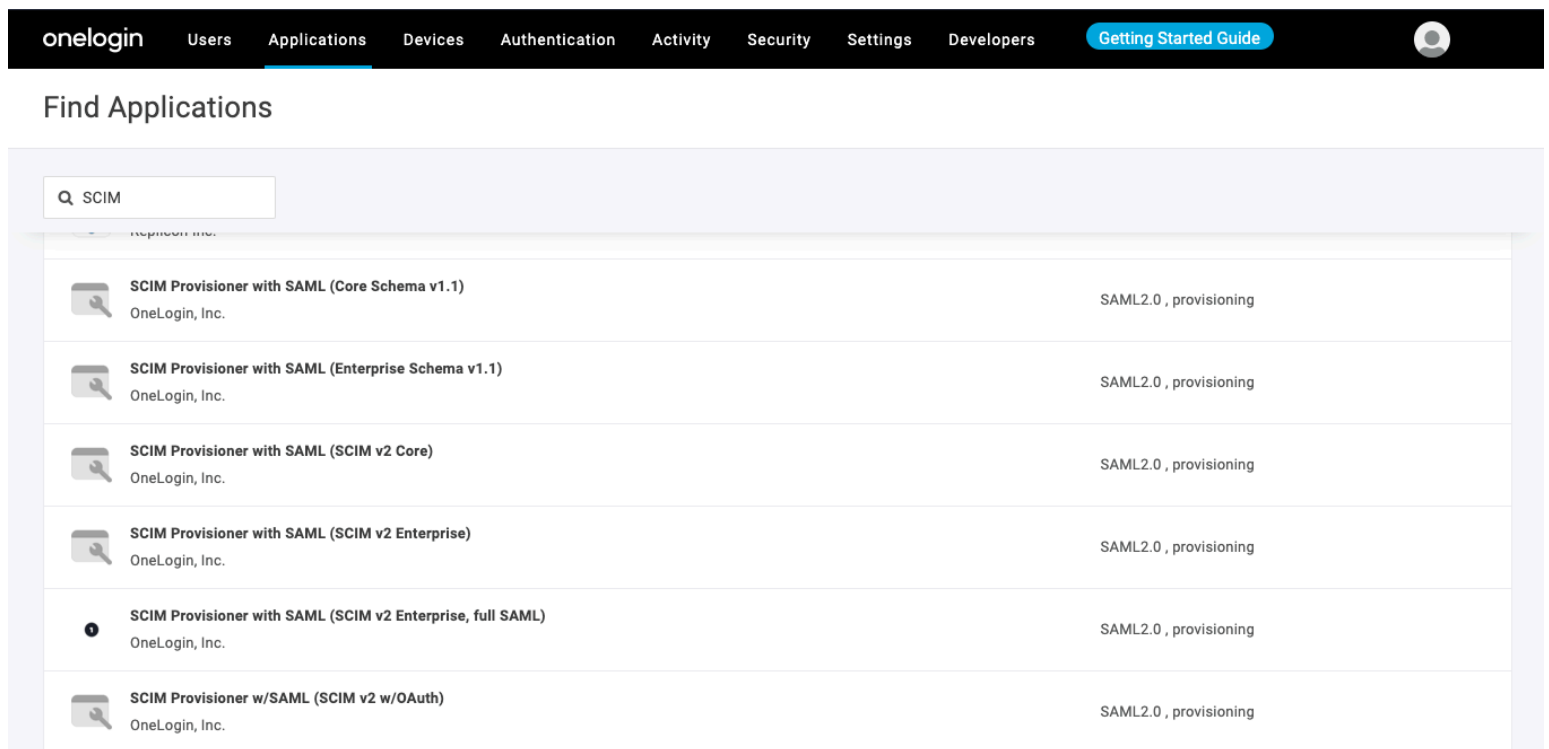
## Een OneLogin-app maken

Navigeer in de OneLogin Portal naar het scherm **Toepassingen** en selecteer de knop **App toevoegen**:



*Add an Application*

Typ **SCIM** in de zoekbalk en selecteer de app **SCIM Provisioner with SAML (SCIM v2 Enterprise)**:



*SCIM Provisioner App*

Geef uw toepassing een Bitwarden-specifieke **weergavenaam** en selecteer de knop **Opslaan**.

## Configuratie

Selecteer **Configuratie** in de linker navigatie en configureer de volgende informatie, waarvan u sommige moet ophalen uit de schermen Single Sign-On en SCIM Provisioning in 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

## Details toepassing

OneLogin vereist dat je de **SAML Audience URL** en **SAML Consumer URL** velden invult, zelfs als je geen single sign-on gaat gebruiken. [Leer wat je in deze velden moet invoeren.](#)

## API-verbinding

Voer de volgende waarden in bij het onderdeel **API-verbinding**:

Toepassingsinstelling	Beschrijving
SCIM basis URL	Stel dit veld in op de SCIM URL( <a href="#">meer informatie</a> ).
SCIM draagtoken	Stel dit veld in op de SCIM API-sleutel( <a href="#">meer informatie</a> ).

Selecteer **Opslaan** zodra je deze velden hebt geconfigureerd.

## Toegang

Selecteer **Toegang** in de linkernavigatie. Wijs in het gedeelte **Rollen** applicatietoegang toe aan alle rollen die u in Bitwarden wilt aanbieden. Elke rol wordt behandeld als een groep in uw Bitwarden-organisatie en gebruikers die zijn toegewezen aan een rol worden opgenomen in elke groep, ook als ze meerdere rollen zijn toegewezen.

## Parameters

Selecteer **Parameters** in de linkernavigatie. Selecteer **Groups** in de tabel, schakel het selectievakje **Include in User Provisioning** in en selecteer de knop **Save** :

The screenshot shows the OneLogin interface with a modal dialog titled "Edit Field Groups". The dialog contains the following elements:

- Name:** Groups
- Value:** A dropdown menu showing "Select Groups" and an "Add" button.
- Added Items:** An empty box with the header "Added Items".
- Flags:**
  - Include in SAML assertion
  - Include in User Provisioning
- Buttons:** "Cancel" and "Save" at the bottom right.

*Include Groups in User Provisioning*

## Regels

Maak een regel om OneLogin-rollen toe te wijzen aan Bitwarden-groepen:

1. Selecteer **Regels** in de linkernavigatie.
2. Selecteer de knop Regel toevoegen om het dialoogvenster **Nieuwe toewijzing** te openen:

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. Geef de regel een **naam** zoals Groepen maken van regels.
4. Laat **Voorwaarden** leeg.
5. In het gedeelte **Acties** :
  1. Selecteer **Groepen instellen in** in de eerste vervolgkeuzelijst.
  2. Selecteer de optie **Map from OneLogin**.
  3. Selecteer **de rol** in de vervolgkeuzelijst "Voor elk".
  4. Voer .\* in het veld "met waarde die overeenkomt" in om alle rollen aan groepen toe te wijzen of voer een specifieke rolnaam in.

6. Selecteer de knop **Opslaan** om het aanmaken van de regel te voltooien.

## Testaansluiting

Selecteer **Configuratie** in de linkernavigatie en selecteer de knop **Inschakelen** onder **API-status**:

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 shows the 'API Connection' section with 'API Status' set to 'Enabled' (indicated by a green dot) and a 'Disable' button. Below this is the 'SCIM Base URL' field. At the bottom right of the configuration area, there is a 'Test API Connection' button.

Deze test start de provisioning **niet**, maar doet een GET-verzoek aan Bitwarden en geeft **Ingeschakeld** weer als de applicatie met succes een antwoord krijgt van Bitwarden.

## Voorziening inschakelen

Selecteer **Provisioning** in de linkernavigatie:

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*

Op dit scherm:

1. Schakel het selectievakje **Provisioning inschakelen in** .
2. Selecteer in de vervolgkeuzelijst **Wanneer gebruikers worden verwijderd in OneLogin. ..** de optie **Verwijderen**.
3. Selecteer in de vervolgkeuzelijst **Wanneer gebruikersaccounts worden opgeschort in OneLogin...** de optie **Opschorten**.

Als je klaar bent, selecteer je **Opslaan** om de provisioning te starten.

## Onboarding van gebruikers voltooiën

Nu je gebruikers zijn voorzien, ontvangen ze uitnodigingen om lid te worden van de organisatie. Instrueer je gebruikers om [de uitnodiging te accepteren](#) en [bevestig ze daarna aan de organisatie](#).

**Note**

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



## Bijlage

### Gebruikersattributen

Zowel Bitwarden als OneLogin's **SCIM Provisioner met SAML (SCIM v2 Enterprise)** applicatie gebruiken standaard SCIM v2 attribuutnamen. Bitwarden gebruikt de volgende attributen:

- `actief`
- `e-maila` of `gebruikersnaam`
- `weergavenaam`
- `externalId`

<sup>a</sup> – Omdat SCIM gebruikers toestaat om meerdere e-mailadressen te hebben uitgedrukt als een array van objecten, zal Bitwarden de `waar` de gebruiken van het object dat "primary" bevat : `true`.