bitwarden | Artikel Helpcentrum

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.

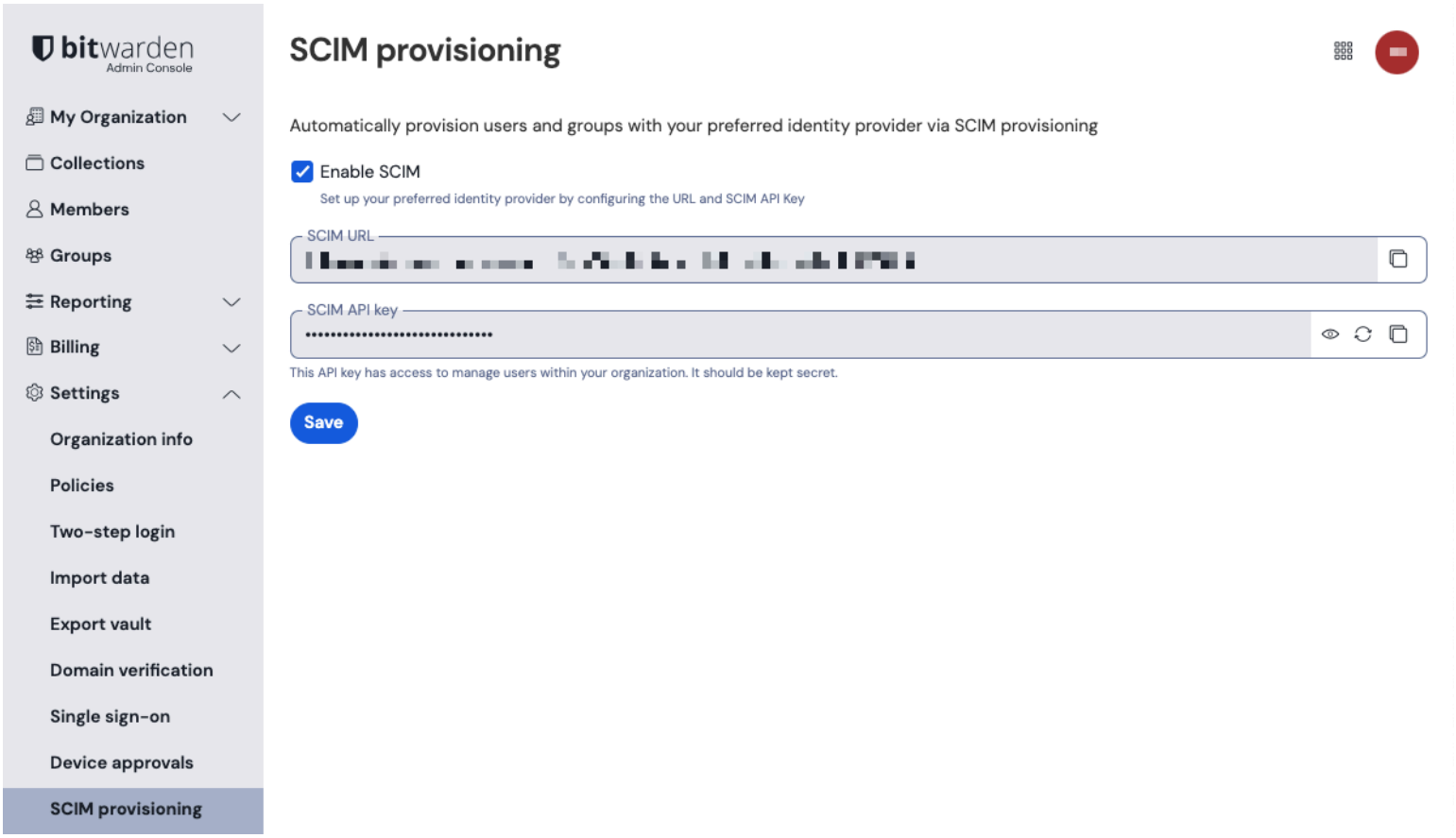
> **Note**
>
> SCIM-integraties zijn beschikbaar voor **Enterprise-organisaties**. Teams organisaties, of klanten die geen SCIM-compatibele identity provider gebruiken, kunnen overwegen Directory Connector te gebruiken als een alternatieve manier van provisioning.

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**:

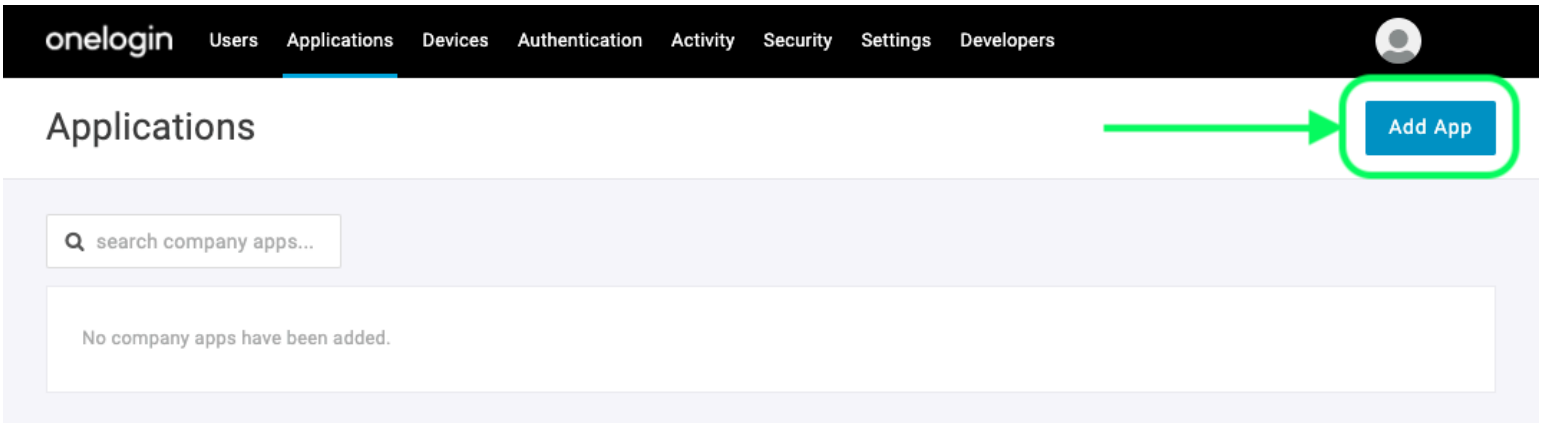


SCIM-voorziening

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.

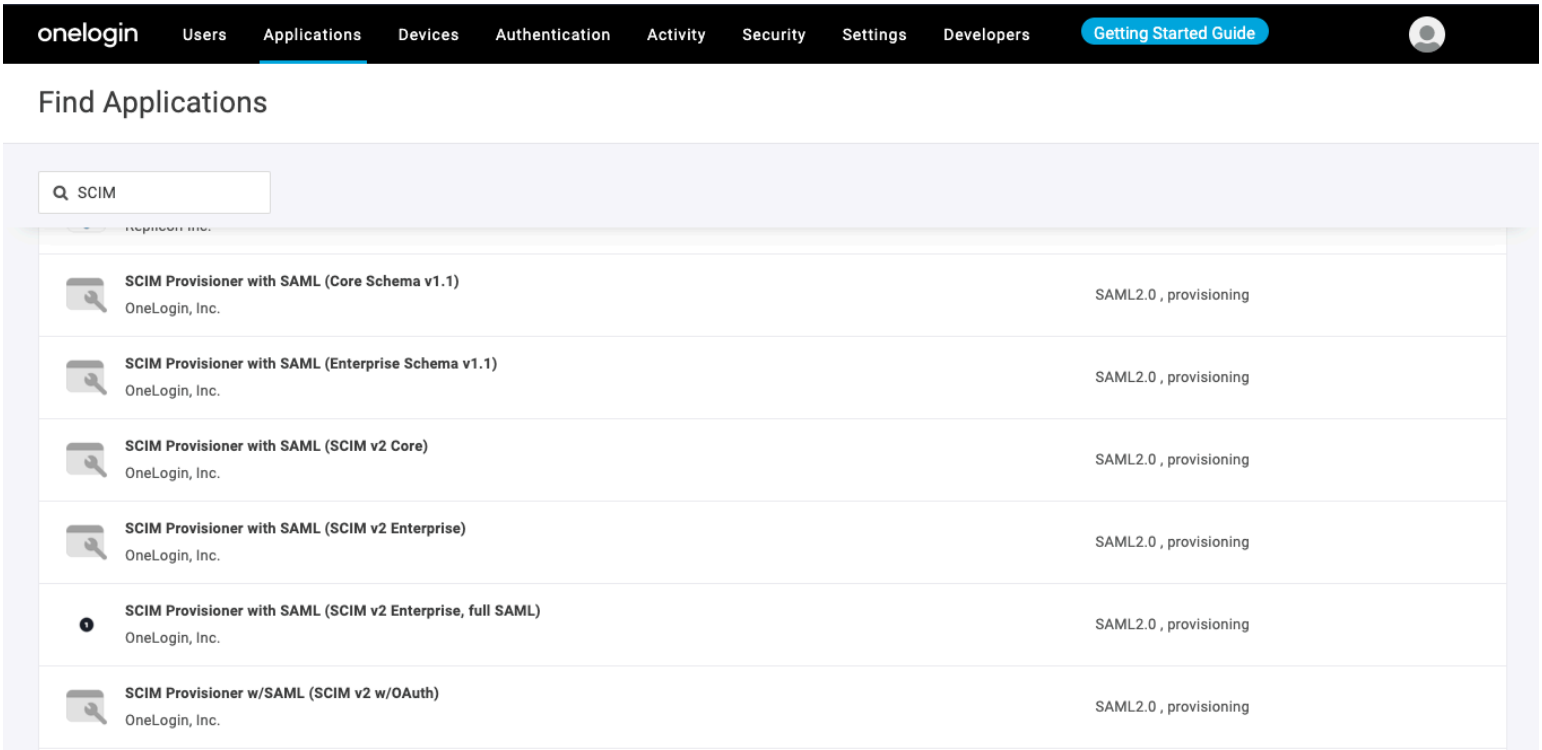
Een OneLogin-app maken

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)**:

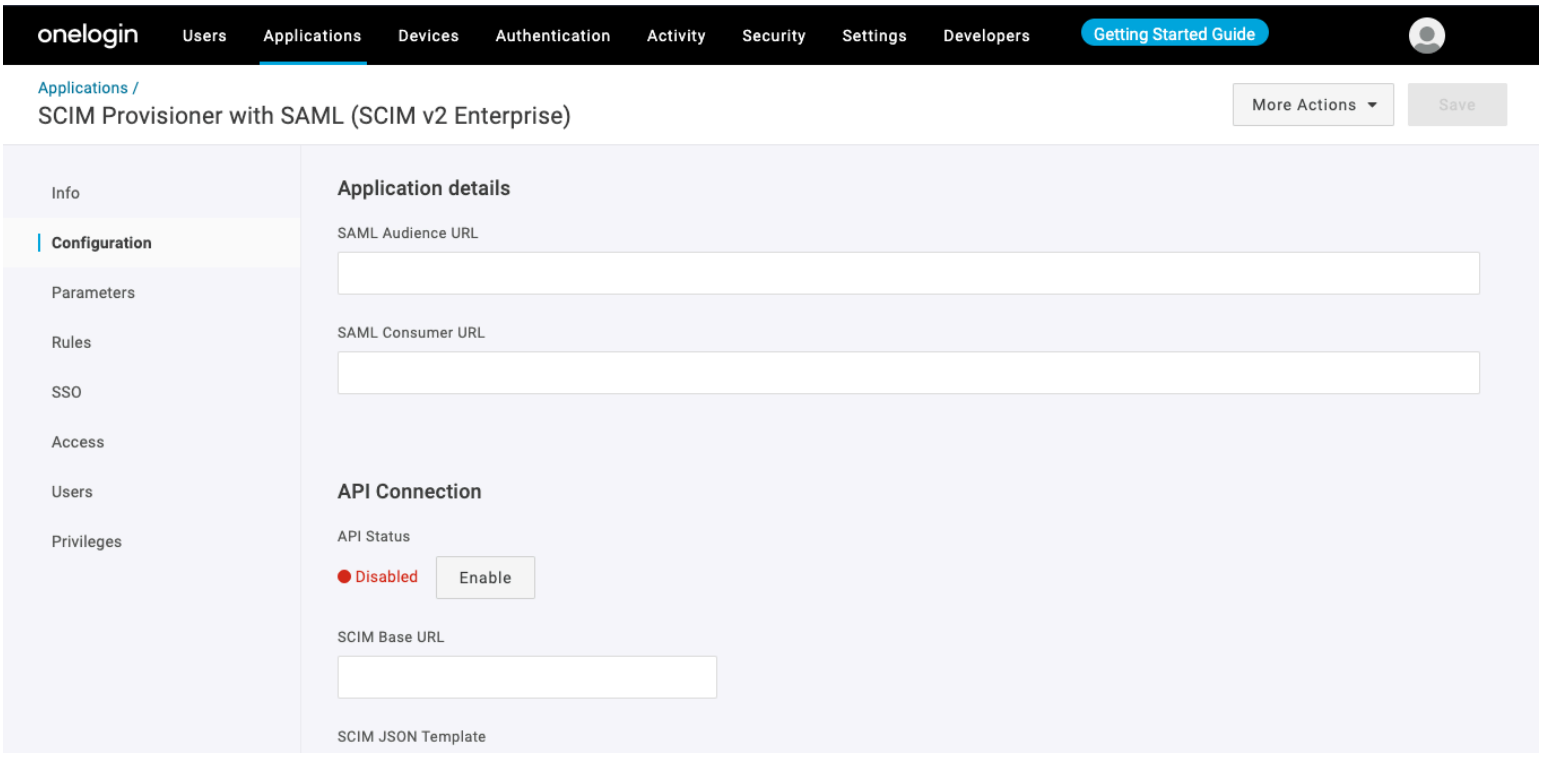


SCIM Provisioner App

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.



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(meer informatie).
SCIM draagtoken	Stel dit veld in op de SCIM API-sleutel(meer informatie).

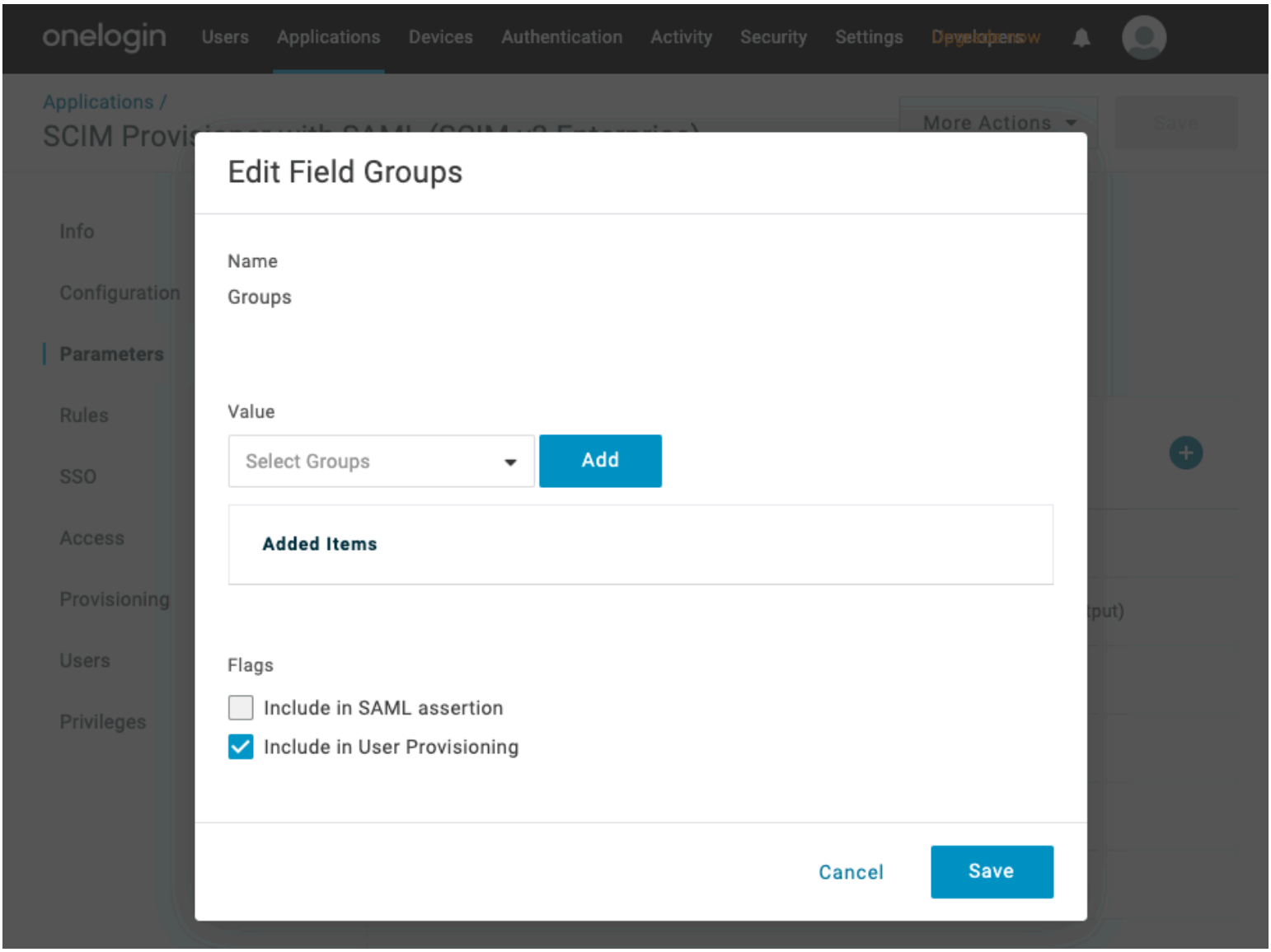
Selecteer **Opslaan** zodra je deze velden hebt geconfigureerd.

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** :

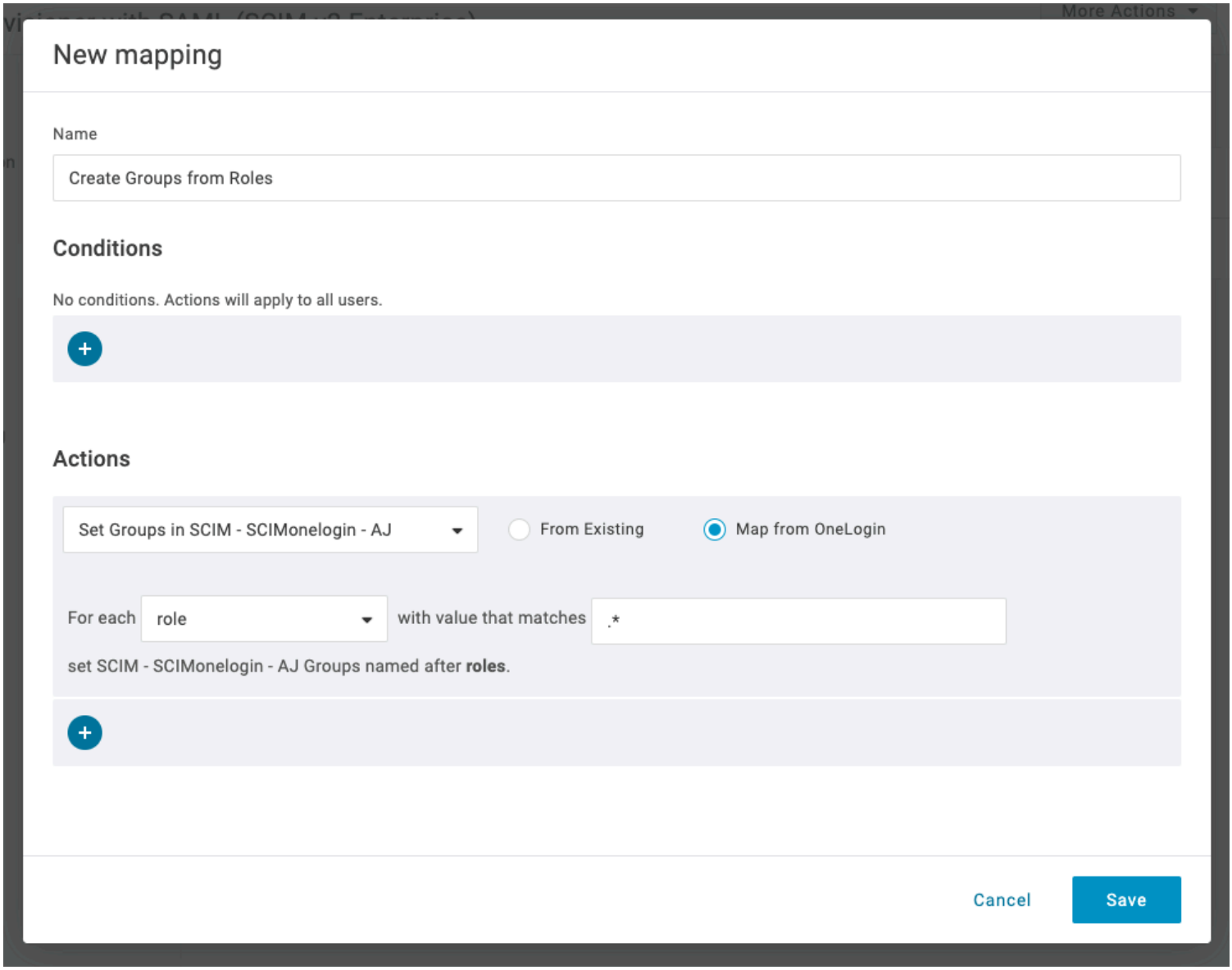


Include Groups in User Provisioning

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:



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**.

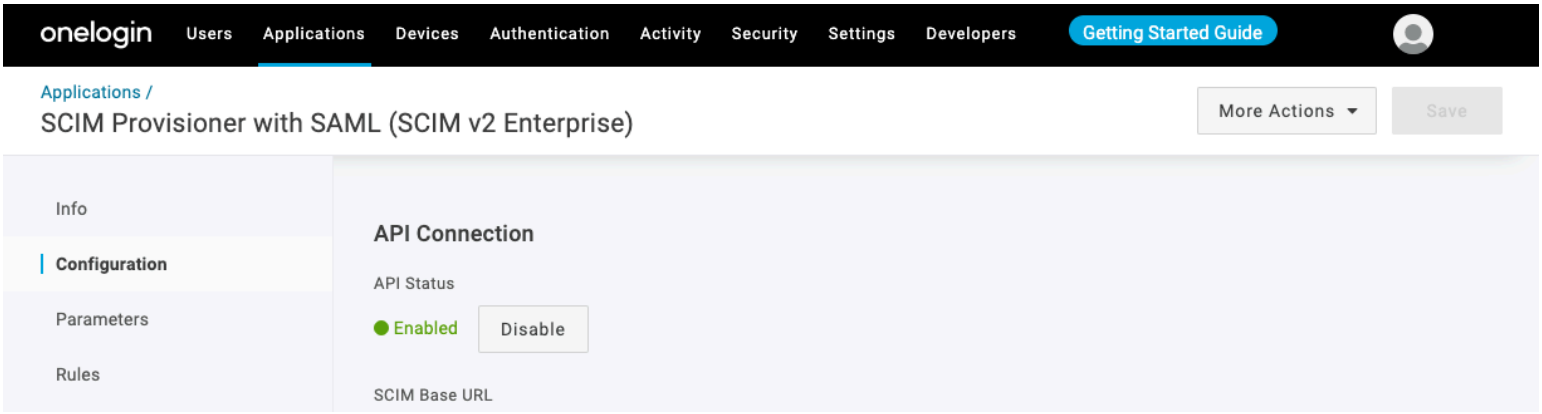
    3. Selecteer **de rol** in de vervolgkeuzelijst "Voor elk".

    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:**

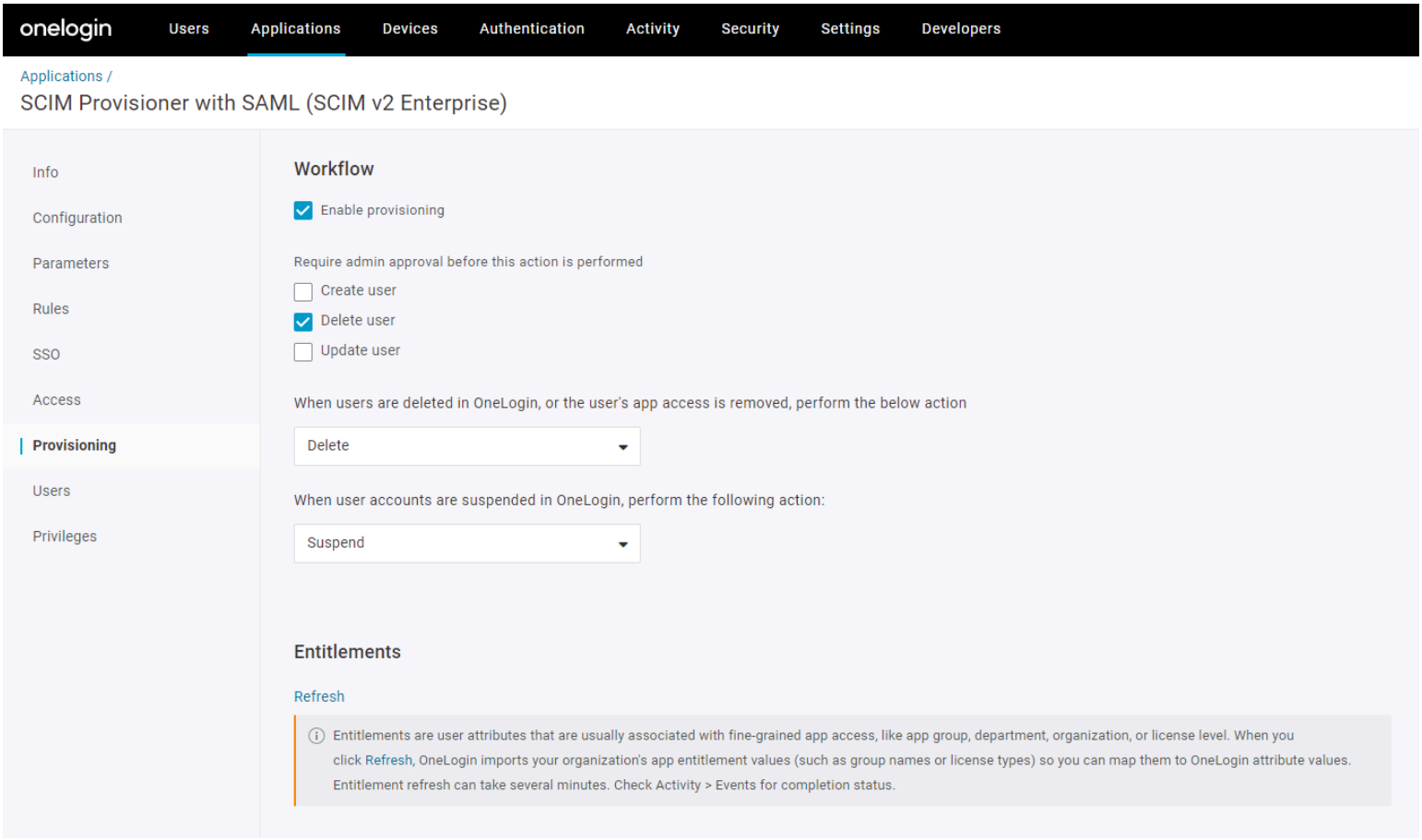


Test API Connection

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:



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 voltooien

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-mail`[a] of `gebruikersnaam`
- `weergavenaam`
- `externalId`

[a] - Omdat SCIM gebruikers toestaat om meerdere e-mailadressen te hebben uitgedrukt als een array van objecten, zal Bitwarden de `waarde` gebruiken van het object dat "primary" bevat `: true`.