

ADMINISTRATOR KONSOLE > BENUTZERVERWALTUNG >

# OneLogin SCIM-Integration

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

## OneLogin SCIM-Integration

System für Identitätsmanagement über Domänen hinweg (SCIM) kann verwendet werden, um Mitglieder und Gruppen in Ihrer Bitwarden Organisation automatisch bereitzustellen und zu deaktivieren.

### Note

SCIM-Integrationen sind verfügbar für **Enterprise-Organisationen**. Teams Organisationen oder Kunden, die keinen SCIM-kompatiblen Identitätsanbieter verwenden, sollten in Betracht ziehen, [Directory Connector](#) als alternative Methode zur Bereitstellung zu verwenden.

Dieser Artikel wird Ihnen helfen, eine SCIM-Integration mit OneLogin zu konfigurieren. Die Konfiguration beinhaltet die gleichzeitige Arbeit mit dem Bitwarden Web-Tresor und dem OneLogin Administrator Portal. Während Sie fortfahren, empfehlen wir, beides griffbereit zu haben und die Schritte in der Reihenfolge durchzuführen, in der sie dokumentiert sind.

## SCIM aktivieren

### Note

**Hosten Sie Bitwarden selbst?** Falls ja, führen Sie [diese Schritte zur Aktivierung von SCIM für Ihren Server](#) durch, bevor Sie fortfahren.

Um Ihre SCIM-Integration zu starten, öffnen Sie die Admin-Konsole und navigieren Sie zu **Einstellungen → 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:

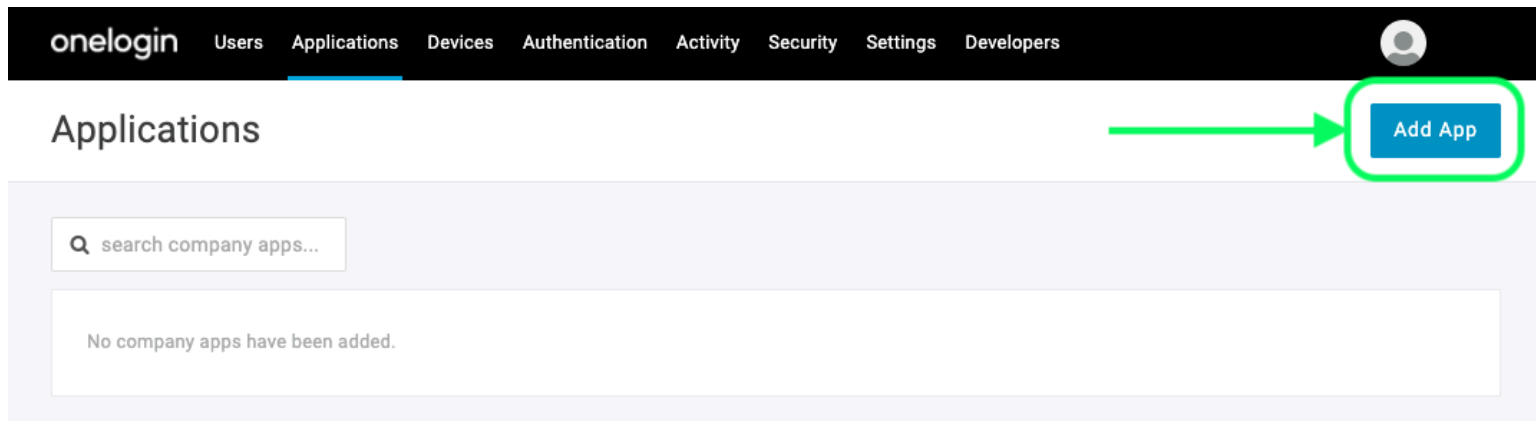
- A sub-header: 'Automatically provision users and groups with your preferred identity provider via SCIM provisioning'
- A checked checkbox labeled 'Enable SCIM' with a sub-note: 'Set up your preferred identity provider by configuring the URL and SCIM API Key'
- A text input field for 'SCIM URL' containing a long alphanumeric string, with a copy icon on the right.
- A text input field for 'SCIM API key' containing a series of dots, with an eye icon, a refresh icon, and a copy icon on the right.
- A warning note: 'This API key has access to manage users within your organization. It should be kept secret.'
- A blue 'Save' button.

SCIM-Bereitstellung

Wählen Sie das **SCIM aktivieren** Kontrollkästchen aus und machen Sie eine Notiz von Ihrer **SCIM URL** und Ihrem **SCIM API Schlüssel**. Sie werden beide Werte in einem späteren Schritt benötigen.

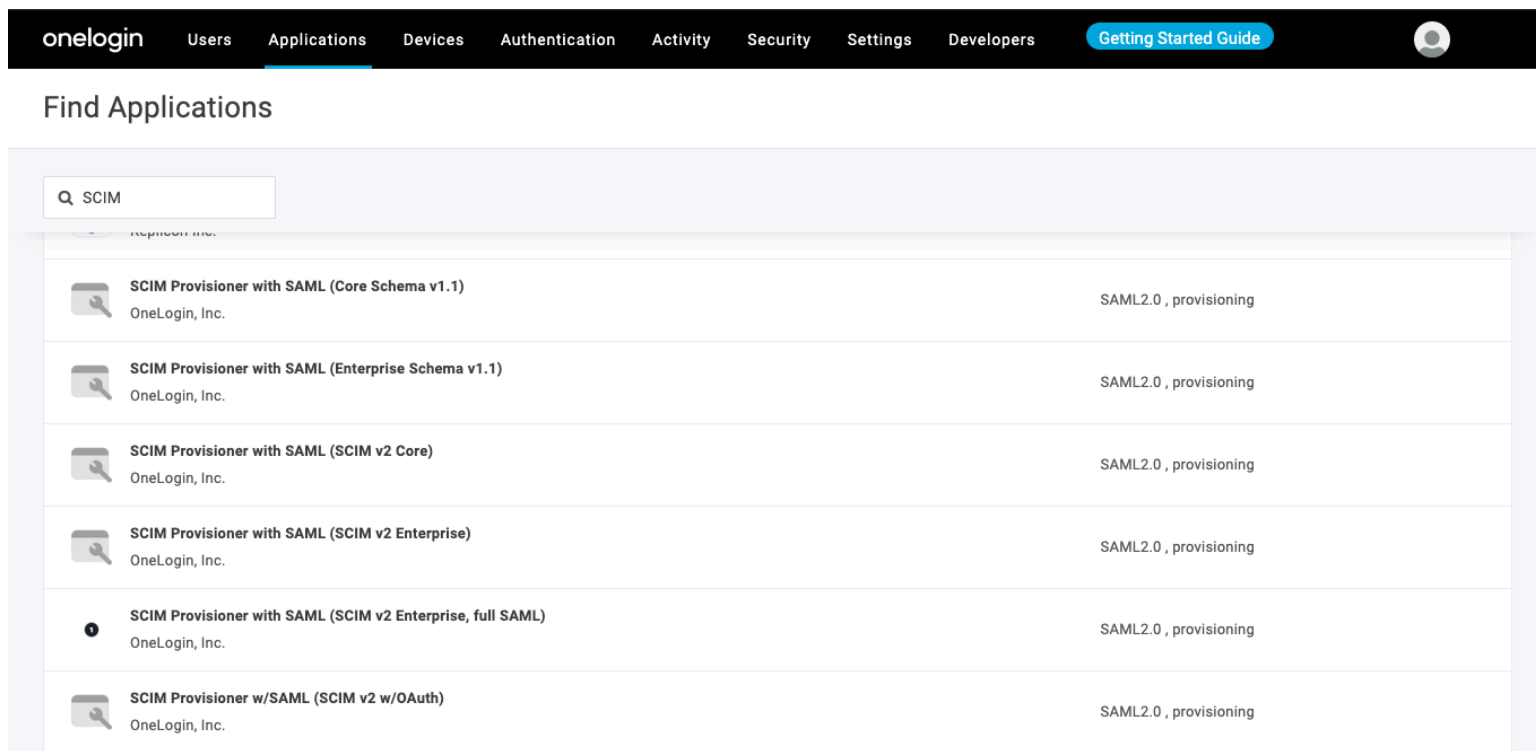
## Erstellen Sie eine OneLogin-App

Im OneLogin Portal navigieren Sie zum **Anwendungen** Bildschirm und wählen Sie die Schaltfläche **App hinzufügen**:



Add an Application

In der Suchleiste geben Sie **SCIM** ein und wählen Sie die **SCIM Provisioner mit SAML (SCIM v2 Enterprise)** App aus:



SCIM Provisioner App

Geben Sie Ihrer Anwendung einen Bitwarden-spezifischen **Anzeigenamen** und wählen Sie die **Speichern** Schaltfläche.

## Konfiguration

Wählen Sie **Konfiguration** aus der linken Navigation aus und konfigurieren Sie die folgenden Informationen, einige davon müssen Sie von den Bildschirmen für Single Sign-On und SCIM-Provisioning in Bitwarden abrufen.

SCIM App Configuration

### Einzelheiten zur Bewerbung

OneLogin wird Sie auffordern, die Felder **SAML Audience URL** und **SAML Consumer URL** auszufüllen, auch wenn Sie Single Sign-On nicht verwenden werden. [Erfahren Sie, was Sie in diese Felder eingeben müssen](#).

### API-Verbindung

Geben Sie die folgenden Werte im Abschnitt **API-Verbindung** ein:

Anwendungseinstellungen	Beschreibung
SCIM-Basis-URL	Setzen Sie dieses Feld auf die SCIM-URL ( <a href="#">mehr erfahren</a> ).
SCIM Bearer-Token	Setzen Sie dieses Feld auf den SCIM API-Schlüssel ( <a href="#">mehr erfahren</a> ).

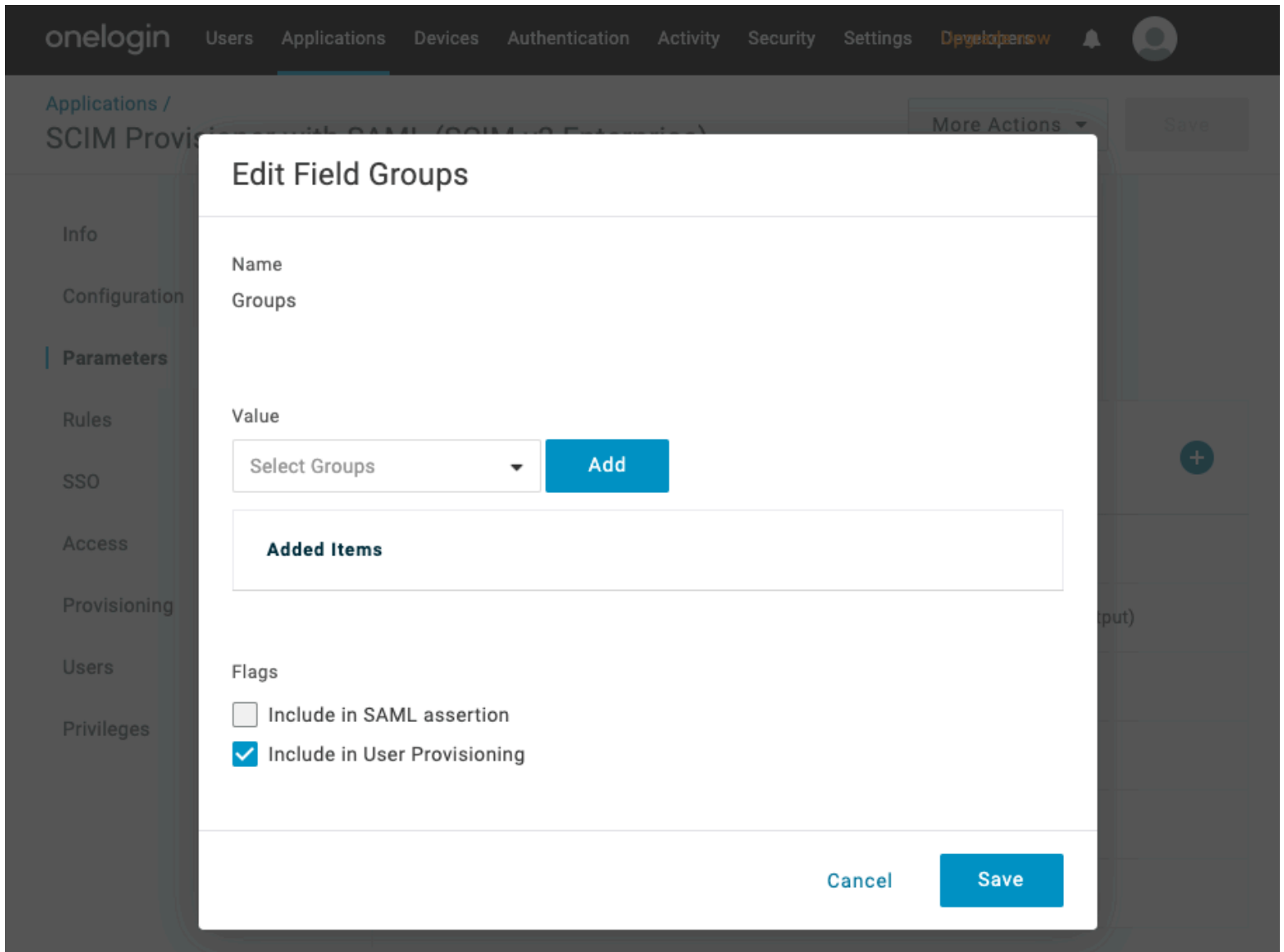
Wählen Sie **Speichern**, sobald Sie diese Felder konfiguriert haben.

## Zugriff

Wählen Sie **Zugang** aus der linken Navigation aus. Im Abschnitt **Rollen** weisen Sie allen Rollen, die Sie in Bitwarden bereitstellen möchten, den Zugriff auf die Anwendung zu. Jede Rolle wird als eine Gruppe in Ihrer Bitwarden Organisation behandelt, und Benutzer, die einer beliebigen Rolle zugewiesen sind, werden in jeder Gruppe eingeschlossen, einschließlich wenn sie mehreren Rollen zugewiesen sind.

## Parameter

Wählen Sie **Parameter** aus der linken Navigation aus. Wählen Sie **Gruppen** aus der Tabelle aus, aktivieren Sie das **In Benutzerbereitstellung einbeziehen** Kontrollkästchen und wählen Sie die **Speichern** Schaltfläche:



Include Groups in User Provisioning

## Regeln

Erstellen Sie eine Regel, um OneLogin Rollen auf Bitwarden Gruppen abzubilden:

1. Wählen Sie **Regeln** aus der linken Navigation aus.

2. Wählen Sie die Schaltfläche Regel hinzufügen, um den **Neue Zuordnung** Dialog zu öffnen:

**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. Geben Sie der Regel einen **Namen** wie Gruppen aus Regeln erstellen.

4. Lassen Sie **Bedingungen** leer.

5. Im **Aktionen** Bereich:

1. Wählen Sie **Gruppen festlegen in** aus dem ersten Dropdown-Menü.
2. Wählen Sie die Option **Karte von OneLogin**.
3. Wählen Sie **Rolle** aus dem "Für jeden" Dropdown-Menü.

4. Geben Sie .\* in das Feld "mit Wert, der übereinstimmt" ein, um alle Rollen auf Gruppen abzubilden, oder geben Sie einen spezifischen Rollennamen ein.

6. Wählen Sie die **Speichern** Schaltfläche, um die Erstellung der Regel abzuschließen.

## Verbindung testen

Wählen Sie **Konfiguration** aus der linken Navigation aus und klicken Sie auf die Schaltfläche **Aktivieren** unter **API-Status**:

The screenshot shows the OneLogin interface for configuring a SCIM Provisioner. The navigation bar includes 'onelogin', 'Users', 'Applications', 'Devices', 'Authentication', 'Activity', 'Security', 'Settings', 'Developers', and a 'Getting Started Guide' button. The main content area is titled 'Applications / SCIM Provisioner with SAML (SCIM v2 Enterprise)'. On the left, there is a sidebar with 'Info', 'Configuration', 'Parameters', and 'Rules'. The 'Configuration' section is active, showing 'API Connection' details. Under 'API Status', there is a green dot next to 'Enabled' and a 'Disable' button. Below this, there is a 'SCIM Base URL' field and a 'Test API Connection' button.

Dieser Test **wird nicht** beginnen zu provisionieren, sondern wird eine GET-Anfrage an Bitwarden stellen und **Aktiviert** anzeigen, wenn die Anwendung erfolgreich eine Antwort von Bitwarden erhält.

## Provisionierung aktivieren

Wählen Sie **Bereitstellung** aus der linken Navigation:

onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers

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

Auf diesem Bildschirm:

1. Wählen Sie das **Provisioning aktivieren** Kontrollkästchen.
2. Im Dropdown **Wenn Benutzer in OneLogin gelöscht werden...**, wählen Sie **Löschen** aus.
3. Im Dropdown-Menü **Wenn Benutzerkonten in OneLogin gesperrt sind...**, wählen Sie **Sperren** aus.

Wenn Sie fertig sind, wählen Sie **Speichern** aus, um die Bereitstellung auszulösen.

## Benutzer-Onboarding abschließen

Jetzt, wo Ihre Benutzer bereitgestellt wurden, erhalten sie Einladungen, der Organisation beizutreten. Weisen Sie Ihre Benutzer an, **die Einladung anzunehmen** und, sobald sie dies getan haben, **bestätigen Sie sie für die Organisation**.

**Note**

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



## Anhang

### Benutzerattribute

Sowohl Bitwarden als auch OneLogins **SCIM Provisioner mit SAML (SCIM v2 Enterprise)** Anwendung verwenden standard SCIM v2 Attributnamen. Bitwarden wird die folgenden Attribute verwenden:

- `aktiv`
- `E-Mailsa` oder `Benutzername`
- `Anzeigename`
- `ExterneId`

- Da SCIM es Benutzern ermöglicht, mehrere E-Mail-Adressen als ein Array von Objekten zu haben, wird Bitwarden den **Wert** des Objekts verwenden, das `"primary": true` enthält.