

管理者コンソール > ユーザー管理 >

OneLogin SCIM統合

ヘルプセンターで表示:

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

OneLogin SCIM統合

クロスドメインID管理 (SCIM) システムは、Bitwarden組織内のメンバーやグループを自動的にプロビジョニングおよびデプロビジョニングするために使用できます。

Note

SCIMインテグレーションは、**エンタープライズ組織**で利用可能です。SCIM互換のIDプロバイダーを使用していないチーム組織、または顧客は、プロビジョニングの代替手段としてディレクトリコネクタの使用を検討することがあります。

この記事は、OneLoginとのSCIM統合を設定するのに役立ちます。設定は、Bitwardenウェブ保管庫とOneLogin管理者ポータルを同時に操作することを含みます。進行するにあたり、両方をすぐに利用できる状態にして、記録されている順序で手順を完了することをお勧めします。

SCIM を有効にする

Note

あなたは自己ホスト型のBitwardenを使用していますか？それなら、進む前にサーバーでSCIMを有効にするためのこれらの手順を完了してください。

SCIM統合を開始するには、管理者コンソールを開き、**設定** → **SCIMプロビジョニング**に移動します。

The screenshot shows the Bitwarden Admin Console interface. On the left is a sidebar menu with options like My Organization, Collections, Members, Groups, Reporting, Billing, and Settings. The 'Settings' section is expanded, and 'SCIM provisioning' is selected. The main content area is titled 'SCIM provisioning' and contains the following elements:

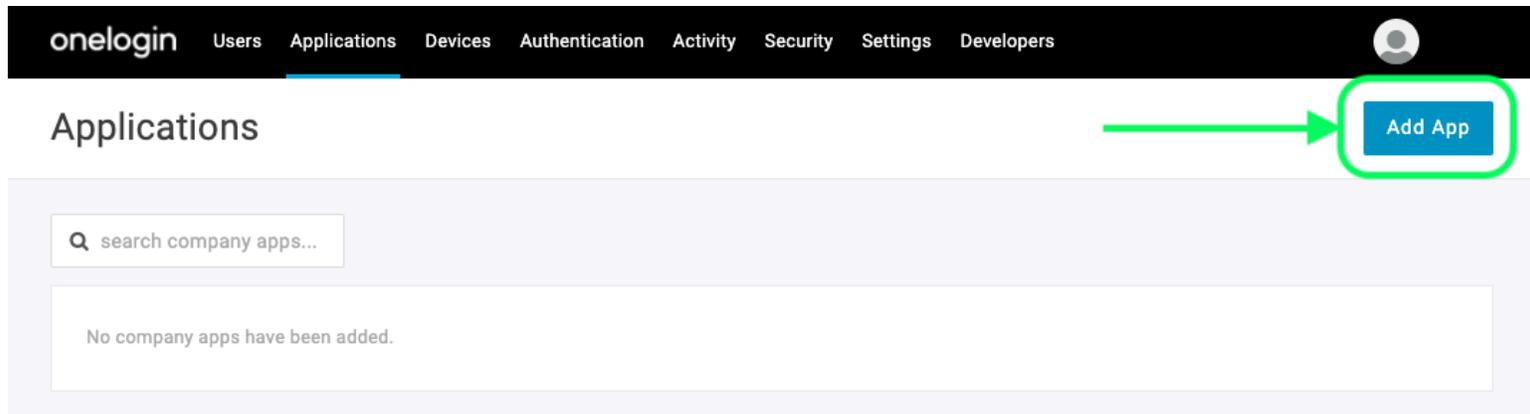
- A sub-header: 'Automatically provision users and groups with your preferred identity provider via SCIM provisioning'
- A checked checkbox labeled 'Enable SCIM' with a sub-note: 'Set up your preferred identity provider by configuring the URL and SCIM API Key'
- A text input field for 'SCIM URL' containing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

SCIM プロビジョニング

SCIMを有効にするチェックボックスを選択し、**SCIM URL**と**SCIM APIキー**をメモしてください。後のステップで両方の値を使用する必要があります。

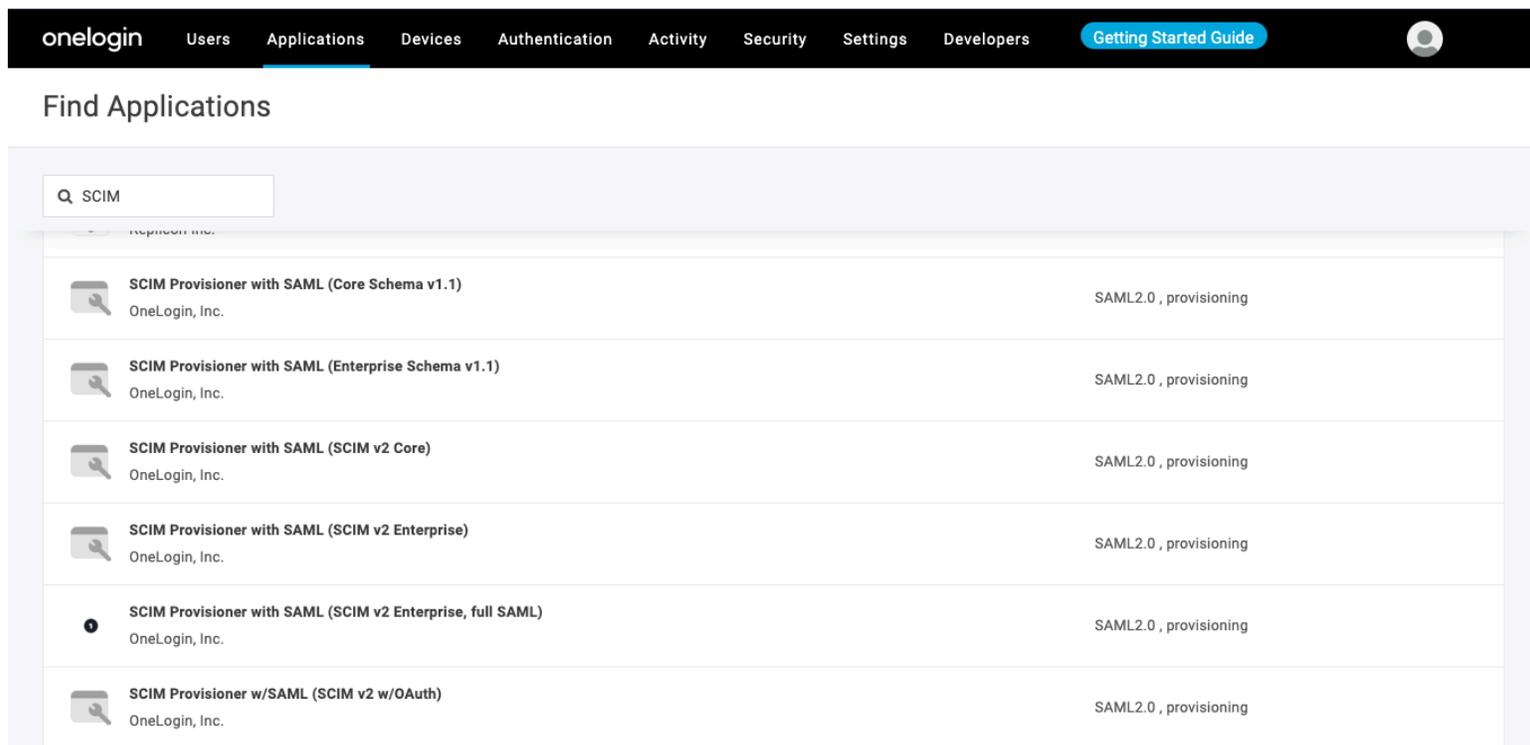
OneLoginアプリを作成します

OneLoginポータルで、**アプリケーション画面**に移動し、**アプリ追加ボタン**を選択します:



Add an Application

検索バーに**SCIM**とタイプし、**SCIM Provisioner with SAML (SCIM v2 エンタープライズ)**アプリを選択します:



SCIM Provisioner App

あなたのアプリケーションにBitwarden特有の**表示名**を付けて、**保存**ボタンを選択してください。

設定

左側のナビゲーションから**設定**を選択し、以下の情報を設定します。これらの一部は、BitwardenのシングルサインオンとSCIMプロビジョニング画面から取得する必要があります。

Applications /

SCIM Provisioner with SAML (SCIM v2 Enterprise)

More Actions ▾

Save

Info	Application details
Configuration	SAML Audience URL <input type="text"/>
Parameters	SAML Consumer URL <input type="text"/>
Rules	
SSO	
Access	
Users	API Connection
Privileges	API Status ● Disabled <input type="button" value="Enable"/>
	SCIM Base URL <input type="text"/>
	SCIM JSON Template

SCIM App Configuration

アプリケーションの詳細

OneLoginは、シングルサインオンを使用しない場合でも、**SAML Audience URL** および**SAML Consumer URL** フィールドを入力するように求めます。これらのフィールドに何を入力するかを学習してください。

API接続

次の値を**API接続**セクションに入力してください:

アプリケーション設定	説明
SCIMベースURL	このフィールドをSCIM URLに設定してください (詳細を学ぶ)。
SCIM ベアラー トークン	このフィールドをSCIM APIキーに設定してください (詳細を学ぶ)。

これらのフィールドを設定したら、**保存**を選択してください。

アクセス

左側のナビゲーションから**アクセス**を選択してください。**役割**セクションで、Bitwardenにプロビジョニングしたいすべての役割にアプリケーションアクセスを割り当ててください。あなたのBitwarden組織では、各役割がグループとして扱われ、任意の役割に割り当てられたユーザーは、複数の役割が割り当てられている場合でも、各グループに含まれます。

パラメーター

左側のナビゲーションからパラメータを選択してください。テーブルからグループを選択し、ユーザープロビジョニングに含めるチェックボックスを有効にし、保存ボタンを選択します。

The screenshot shows the 'Edit Field Groups' dialog box in the OneLogin interface. The dialog has a title bar 'Edit Field Groups'. Below the title, there are sections for 'Name' (containing 'Groups'), 'Value' (containing a dropdown menu with 'Select Groups' and an 'Add' button), 'Added Items' (an empty list), and 'Flags' (containing two checkboxes: 'Include in SAML assertion' which is unchecked, and 'Include in User Provisioning' which is checked). At the bottom right of the dialog are 'Cancel' and 'Save' buttons. The background shows the OneLogin navigation menu with 'Parameters' selected.

Include Groups in User Provisioning

ルール

OneLoginの役割をBitwardenのグループにマッピングするルールを作成します。

1. 左側のナビゲーションからルールを選択してください。
2. 新しいマッピングダイアログを開くために、[ルール追加]ボタンを選択してください。

New mapping

Name

Conditions

No conditions. Actions will apply to all users.

+

Actions

Set Groups in SCIM - SCIMonelogin - AJ From Existing Map from OneLogin

For each with value that matches

set SCIM - SCIMonelogin - AJ Groups named after roles.

+

Cancel

Role/Group Mapping

3. ルールに**名前**を付けてください。例えば、ルールからグループを作成するなど。
4. **条件**を空白にしてください。
5. **アクション**セクションで:
 1. 最初のドロップダウンから**中のグループを設定**を選択してください。
 2. OneLoginから**マップ**を選択するオプションを選んでください。
 3. "For each" ドロップダウンから **役割** を選択してください。
 4. "with value that matches"フィールドに.*を入力して、すべての役割をグループにマッピングします。または、特定の役割名を入力してください。

6. ルールの作成を終了するには、**保存**ボタンを選択してください。

接続をテストする

左側のナビゲーションから**設定**を選択し、**APIステータス:**の下の**有効化**ボタンを選択してください。

The screenshot shows the Bitwarden web 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 main content area is titled 'SCIM Provisioner with SAML (SCIM v2 Enterprise)' and has a 'More Actions' dropdown and a 'Save' button. On the left, there is a sidebar with 'Info', 'Configuration' (selected), 'Parameters', and 'Rules'. The 'API Connection' section shows 'API Status' as 'Enabled' with a 'Disable' button. Below this is the 'SCIM Base URL' field. At the bottom, there is a 'Test API Connection' button.

このテストはプロビジョニングを**開始しません**が、BitwardenにGETリクエストを行い、アプリケーションがBitwardenから正常に応答を得た場合、**有効**と表示します。

プロビジョニングを有効にする

左側のナビゲーションから**プロビジョニング**を選択します。

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

この画面で：

1. **プロビジョニングを有効にする**チェックボックスを選択します。
2. **OneLoginでユーザーが削除される**とき...ドロップダウンで、**削除**を選択します。
3. **OneLoginでユーザーアカウントが停止される**場合...のドロップダウンで、**停止**を選択します。

終了したら、プロビジョニングをトリガーするために**保存**を選択してください。

ユーザーオンボーディングを完了する

あなたのユーザーが準備されたので、彼らは組織に参加するための招待を受け取ります。ユーザーに招待を受け入れるよう指示し、それが完了したら、[組織に彼らを確認する](#)。

Note

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

付録

ユーザー属性

BitwardenとOneLoginの**SCIM Provisioner with SAML (SCIM v2 エンタープライズ)**アプリケーションは、標準的なSCIM v2属性名を使用します。Bitwardenは次の属性を使用します：

- アクティブ
- メールアドレスまたはユーザー名
- 表示名
- 外部ID

- SCIMはユーザーがオブジェクトの配列として複数のメールアドレスを持つことを可能にするため、Bitwardenは値を使用します。そのオブジェクトには"**primary**": trueが含まれています。