# SCIMについて

# SCIMについて

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するために使用できます。

Bitwardenサーバーは、有効なSCIM APIキーを使用して、
ユーザーとグループのプロビジョニングおよびデプロビジョニングのリクエストをあなたのIDプロバイダー（IdP）
から受け入れるSCIMエンドポイントを提供します。

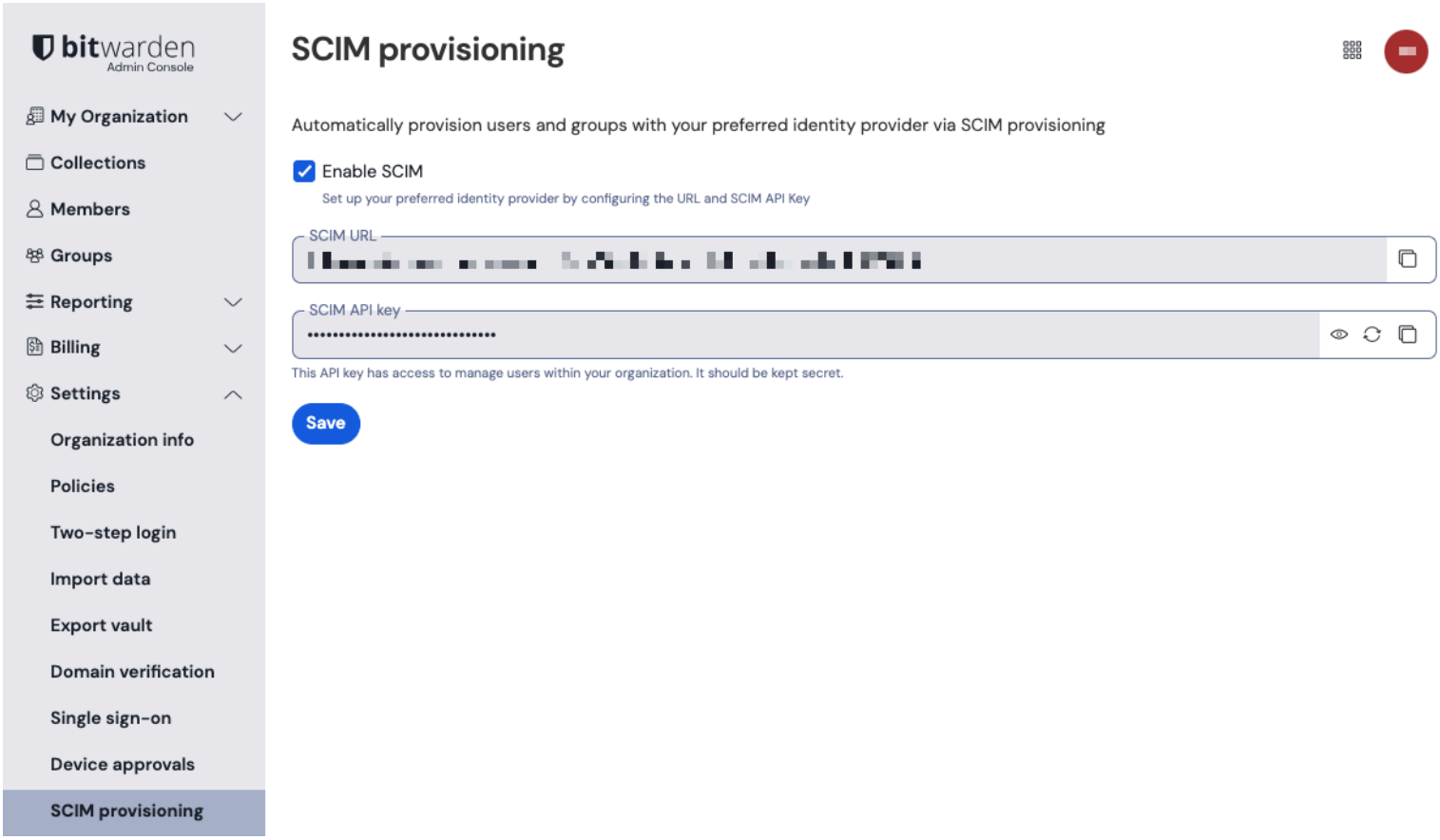
> **Note**
> SCIMインテグレーションは、**エンタープライズ組織**で利用可能です。SCIM互換のIDプロバイダーを使用していないチーム組織、
> または顧客は、プロビジョニングの代替手段としてディレクトリコネクタの使用を検討することがあります。

Bitwardenは標準的な属性マッピングを使用してSCIM v2をサポートし、以下の公式SCIM統合を提供しています：

- アジュール アクティブ ディレクトリ
- オクタ
- ワンログイン
- ジャンプクラウド

## SCIMの設定

SCIMを設定するには、あなたのIdPはSCIM URLとAPIキーを必要とし、
それによりBitwardenサーバーへの認証済みリクエストを行うことができます。これらの値は、**設定**→
**SCIMプロビジョニング**に移動して管理者コンソールから利用できます：




SCIM プロビジョニング

> **Tip**
> BitwardenとAzure AD、Okta、OneLogin、
> またはJumpCloudの間のSCIM統合を設定するための専用ガイドのいずれかを使用することをお勧めします。

## 必要な属性

Bitwardenは標準的なSCIM v2属性名を使用しますが、ここにリストされています。ただし、各IdPは代替名を使用する場合があり、それらはプロビジョニング中にBitwardenにマッピングされます。

### ユーザー属性

各ユーザーに対して、Bitwardenは次の属性を使用します：

- ユーザーが`アクティブ`であることを示す(**必須**)
- `メールアドレス`または`ユーザー名`（**必須**）
- `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。

### グループの属性

各グループに対して、Bitwardenは次の属性を使用します：

- `表示名` (**必須**)
- `メンバー`
- `外部ID`

ã - `members は` オブジェクトの配列であり、各オブジェクトはそのグループ内のユーザーを表します。

## アクセスの取り消しと復元

SCIMを使用してBitwardenにユーザーが設定されると、一時的に彼らの組甑とその保管庫のアイテムへのアクセスを取り消すことができます。
あなたのIdPでユーザーが一時的に停止/非活性化されると、そのユーザーのあなたの組電へのアクセスは自動的に取り消されます。

> **ⓘ Note**
> 所有者のみ 他の所有者へのアクセスを取り消したり復元したりできます。

アクセスが取り消されたユーザーは、組織の**メンバー**画面の**取り消し**タブに表示され、次の操作を行います：

- 組織の保管庫アイテム、コレクションにはアクセスできません。
- SSOを使用してログインする能力がない、または組織的なDuoを二段階ログインに使用する。
- 組織のポリシーの対象ではありません。
- ライセンス席を占有しないでください。

> **⚠ Warning**
> マスターパスワードがない結果としての信頼できるデバイスとのSSOを持つアカウントについては、
> 組織からの削除またはアクセス権の取り消しにより、以下の場合を除き、
> そのBitwardenアカウントへのすべてのアクセスが遮断されます：
>
> 1. あらかじめアカウント回復を使用して、マスターパスワードを割り当てます。
> 2. ユーザーは、アカウント回復ワークフローを完全に完了するために、アカウント回復後に少なくとも一度ログインします。

アクセスを取り消す方法とアクセスを復元する方法について詳しく学びましょう。

## SCIMイベント

あなたの組織は、ユーザーの招待や削除、グループの作成や削除を含むSCIM統合による行動のイベントログをキャプチャします。
SCIM由来のイベントは、メンバー列に**SCIM**を登録します。

## 既存のユーザーとグループ

SCIMを有効化する前に、手動またはディレクトリコネクタを使用してユーザーやグループをオンボーディングした組織は、
以下の点にメモしてください：

| | **...それはIdPに存在します。** | **...それはIdPに存在しません。** |
|---|---|---|
| **既存のユーザー** | •複製されません<br>•組織に再加入することを強制されません<br>•<br>彼らがすでにメンバーであるグループからは削除されません | •組織から削除されません<br>•<br>グループメンバーシップは追加も削除もされません |
| **既存のグループ** | •複製されません<br>IdPに従ってメンバーが追加されます。<br>•既存のメンバーは削除されません | •組織から削除されません<br>•メンバーは追加または削除されません |

> **⚠ Warning**
> Directory Connectorを使用している場合は、SCIMを有効にする前に同期をオフにしてください。