Microsoft Entra ID SCIM統合

Microsoft Entra ID 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。

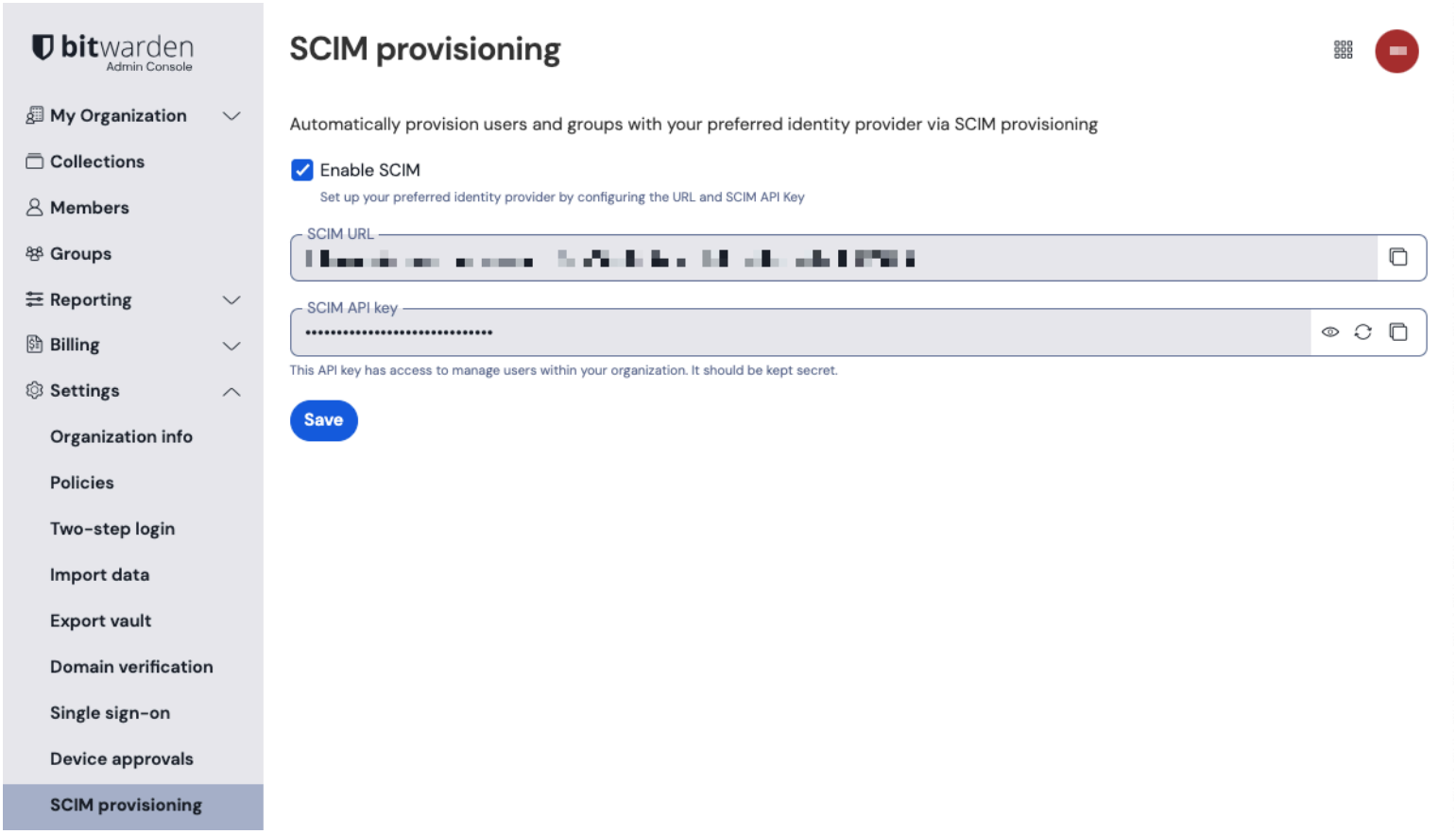
> **Note**
> SCIMインテグレーションは、**エンタープライズ組織**で利用可能です。SCIM互換のIDプロバイダーを使用していないチーム組織、または顧客は、プロビジョニングの代替手段としてディレクトリコネクタの使用を検討することがあります。

この記事は、AzureとのSCIM統合を設定するのに役立ちます。設定は、Bitwardenのウェブ保管庫とAzure Portal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。



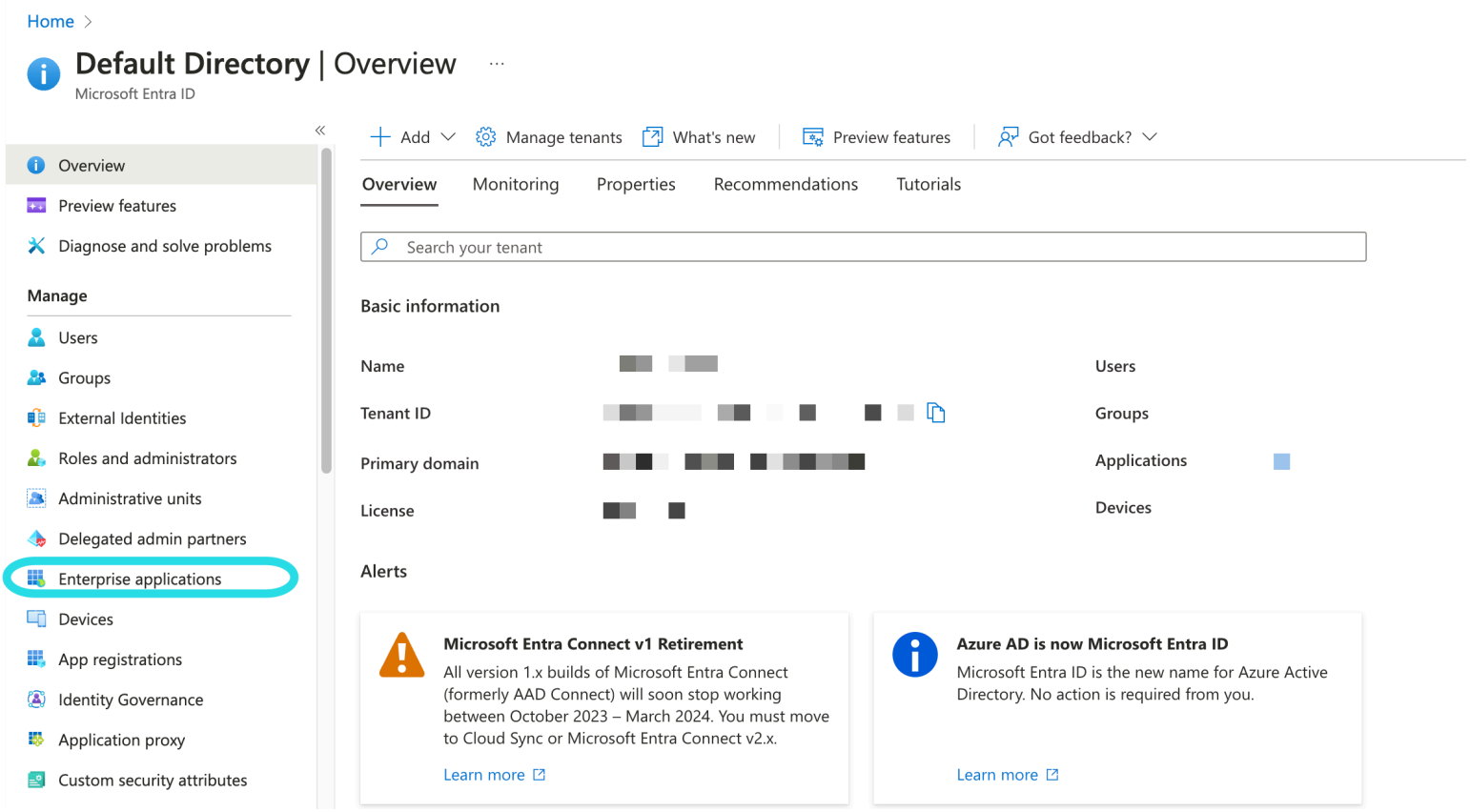
SCIM プロビジョニング

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。

エンタープライズアプリケーションを作成する

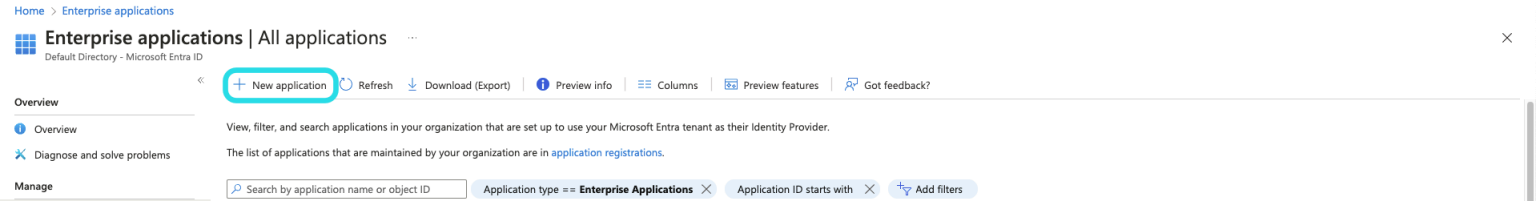
> **Tip**
> If you are already using this IdP for Login with SSO, open that existing enterprise application and skip to this step. Otherwise, proceed with this section to create a new application

Azure Portalで、**Microsoft Entra ID** に移動し、ナビゲーションメニューから**エンタープライズアプリケーション**を選択します。



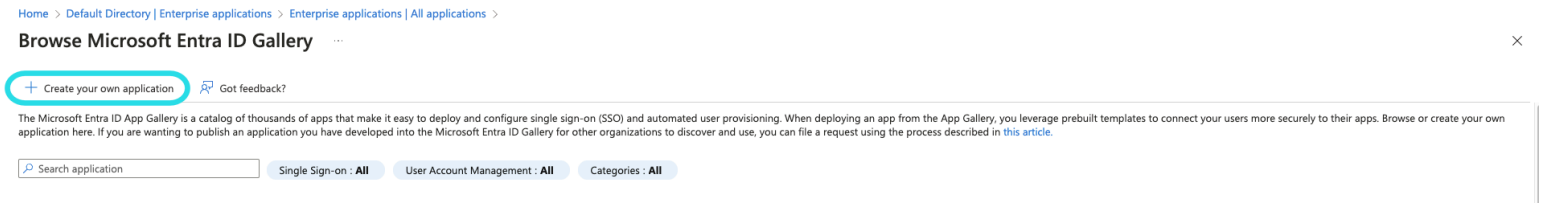
Enterprise applications

＋ **新しいアプリケーション** ボタンを選択してください。



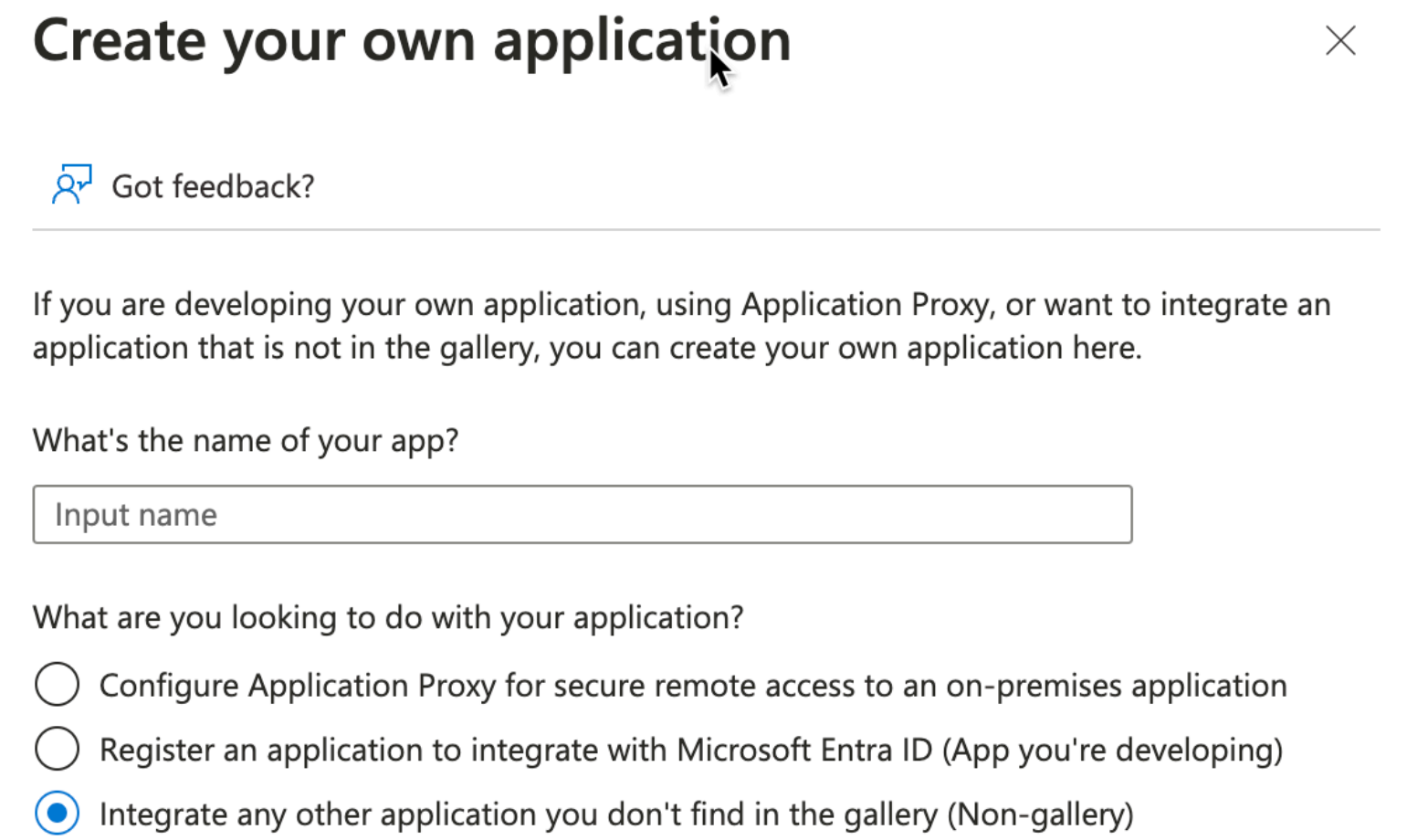
Create new application

Microsoft Entra IDギャラリー画面で、＋ **あなた自身のアプリケーションを作成する**ボタンを選択してください:



Create your own application

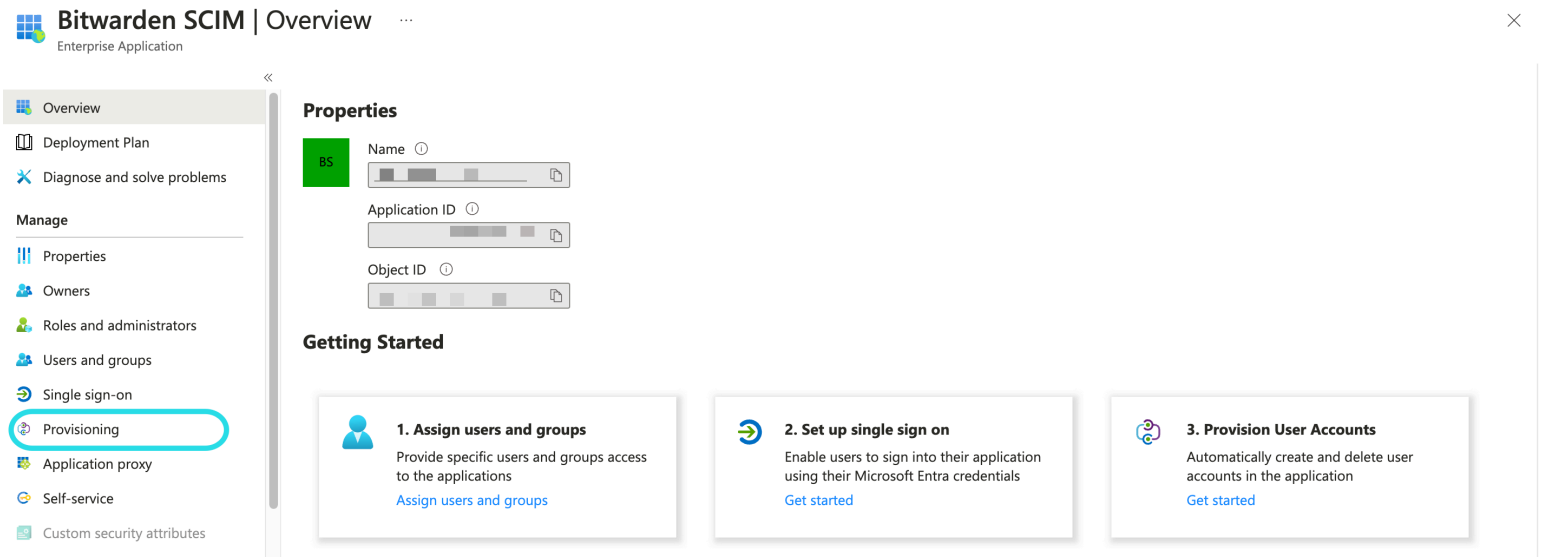
あなた自身のアプリケーションを作成する画面で、アプリケーションにはユニークで、Bitwarden特有の名前を付けてください。
ギャラリー以外のオプションを選択し、次に**作成**ボタンを選択してください。



Create Entra ID app

プロビジョニングを有効にする

ナビゲーションから**プロビジョニング**を選択し、次の手順を完了してください：



Select Provisioning

1. **開始**ボタンを選択してください。
2. **自動** を**プロビジョニングモード** のドロップダウンメニューから選択します。
3. あなたのSCIM URL（詳細を学ぶ）を**テナントURL**フィールドに入力してください。
4. あなたのSCIM APIキー（もっと詳しく）を**シークレットトークン**フィールドに入力してください。
5. **接続をテスト**ボタンを選択します。
6. あなたの接続テストが成功した場合、**保存**ボタンを選択してください。

マッピング

Bitwardenは標準的なSCIM v2属性名を使用しますが、これらはMicrosoft Entra ID属性名と異なる場合があります。
デフォルトのマッピングは機能しますが、必要に応じてこのセクションを使用して変更を加えることができます。Bitwardenは、
ユーザーとグループに以下のプロパティを使用します：

ユーザーマッピング

Bitwarden属性	デフォルトのAAD属性
アクティブ	`Switch([IsSoftDeleted], , "False", "True", "True", "False")`
メールアドレスまたはユーザー名	メールまたは`userPrincipalName`
表示名	表示名

Bitwarden属性	デフォルトのAAD属性
外部ID	メールニックネーム

– 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はオブジェクトの値を使用します。そのオブジェクトには`"primary": true`が含まれています。

グループマッピング

Bitwarden属性	デフォルトのAAD属性
表示名	表示名
メンバーたち	メンバーたち
外部ID	オブジェクトID

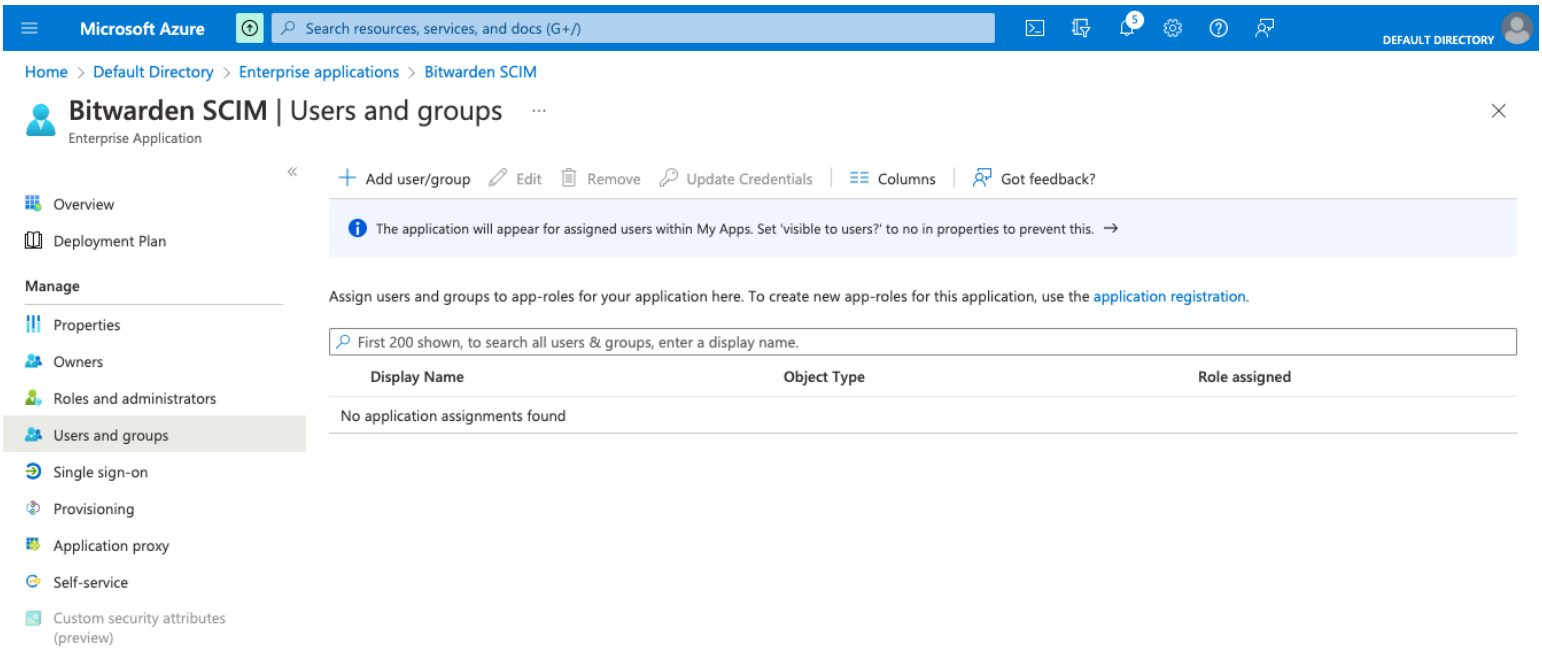
設定

設定 ドロップダウンから、選択してください：

- 障害が発生した場合にメール通知を送るかどうか、そして送る場合はどのメールアドレスに送るか（推奨）。
- **割り当てられたユーザーとグループのみを同期する**か、**すべてのユーザーとグループを同期する**か。
  すべてのユーザーとグループを同期することを選択した場合、次のステップをスキップしてください。

ユーザーとグループを割り当てる

このステップを完了してください。
あなたがプロビジョニングの**設定から割り当てられたユーザーとグループのみを同期**するように選択した場合。
ナビゲーションから**ユーザーとグループ**を選択してください。



Enterprise application users and groups

SCIMアプリケーションへのユーザーまたはグループレベルでのアクセスを割り当てるには、＋ **ユーザー/グループを追加** ボタンを選択してください。次のセクションでは、Azureでユーザーとグループを変更すると、それがBitwardenの対応する部分にどのような影響を与えるかについて説明します:

ユーザー

- Azureで新しいユーザーが割り当てられると、そのユーザーはあなたのBitwarden組織に招待されます。
- あなたの組織のメンバーであるユーザーがAzureに割り当てられると、Bitwardenのユーザーはそのユーザー名の値を通じてAzureのユーザーにリンクされます。
  - このようにリンクされたユーザーは、このリストの他のワークフローに依然として対象となりますが、`displayName`や`externalId/mailNickname`のような値はBitwardenで自動的に変更されません。
- Azureで指定されたユーザーが停止されると、そのユーザーは組電へのアクセスが取り消されます。
- Azureで指定されたユーザーが削除されると、そのユーザーは組織から削除されます。
- Azureのグループから割り当てられたユーザーが削除されると、そのユーザーはBitwardenのそのグループから削除されますが、組織のメンバーとして残ります。

グループ

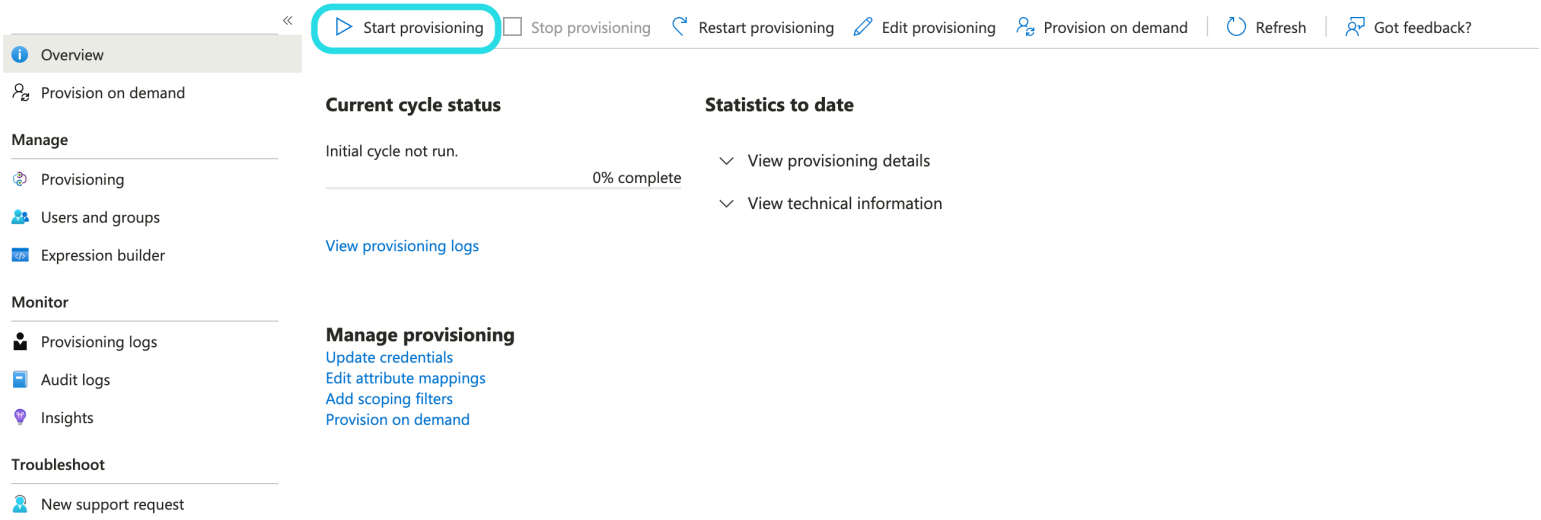
- Azureで新しいグループが割り当てられると、そのグループはBitwardenで作成されます。
  - あなたのBitwarden組織のメンバーであるグループメンバーは、グループに追加されます。
  - あなたのBitwarden組織のメンバーでないグループメンバーは、参加するために招待されています。
- あなたのBitwarden組織にすでに存在するグループがAzureに割り当てられると、Bitwardenグループは`displayName`および`externalId/objectId`の値を通じてAzureにリンクされます。

  - このようにリンクされたグループは、Azureからそのメンバーが同期されます。

- Azureでグループの名前が変更されると、初期の同期が行われている限り、Bitwardenでも更新されます。
  - Bitwardenでグループの名前が変更されると、それはAzureでの名前に戻されます。常にAzure側でグループ名を変更します。

プロビジョニングを開始します

アプリケーションが完全に設定されたら、エンタープライズアプリケーションの▷プロビジョニング**ページで**
プロビジョニングを開始ボタンを選択してプロビジョニングを開始します:



Start provisioning

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、彼らを組織に確認してください。

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