ADMINISTRATOR KONSOLE > BENUTZERVERWALTUNG >

Microsoft Entra ID SCIM Integration

Ansicht im Hilfezentrum:
https://bitwarden.com/help/microsoft-entra-id-scim-integration/

Microsoft Entra ID 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.

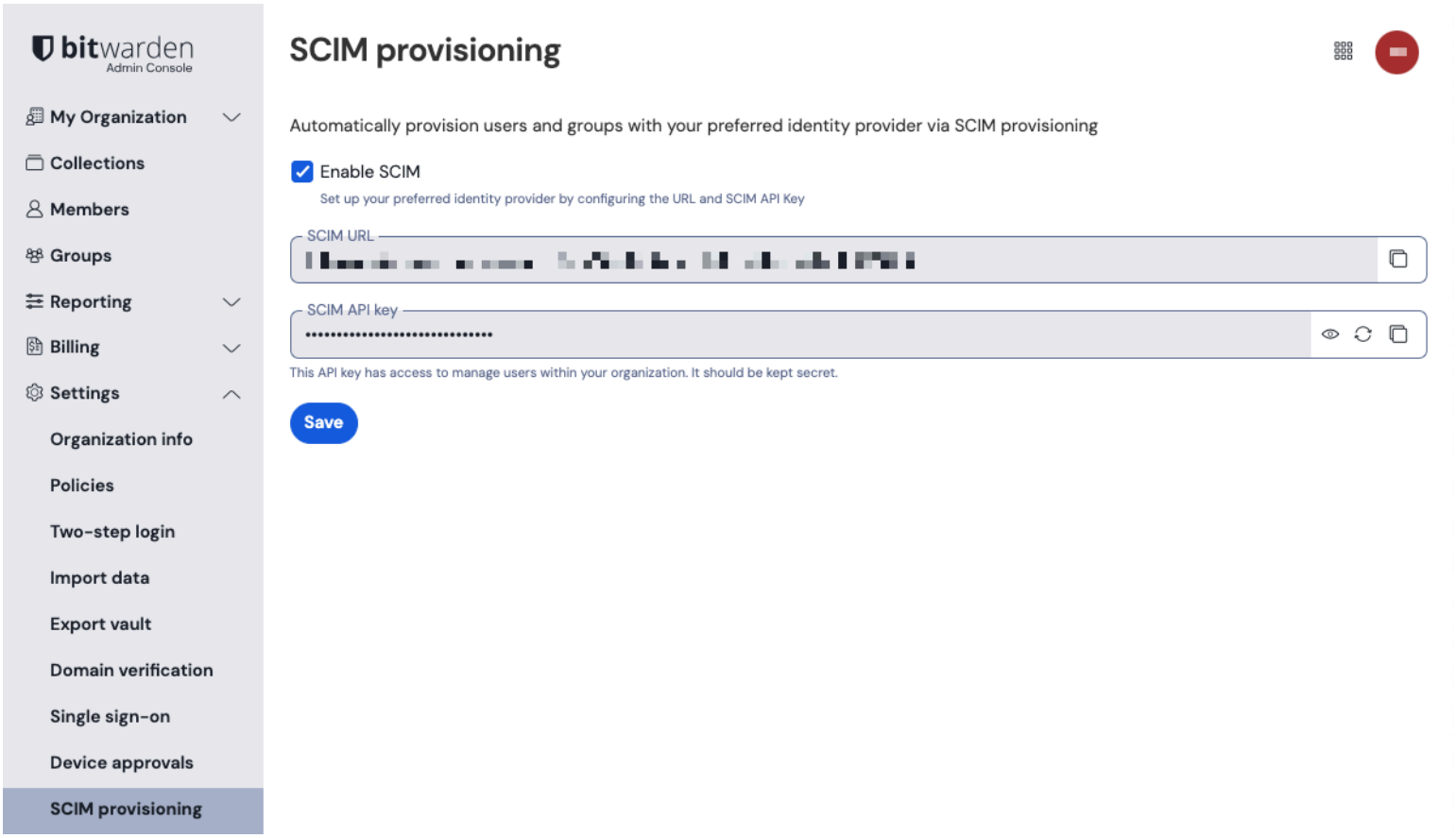
> **Note**
>
> SCIM-Integrationen sind verfügbar für **Enterprise-Organisationen**. Teams Organisationen oder Kunden, die keinen SCIM-kompatiblen Identitätsanbieter verwenden, sollten in Betracht ziehen, Directory Connector als alternative Methode zur Bereitstellung zu verwenden.

Dieser Artikel wird Ihnen helfen, eine SCIM-Integration mit Azure zu konfigurieren. Die Konfiguration beinhaltet die gleichzeitige Arbeit mit dem Bitwarden Web-Tresor und dem Azure 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**:



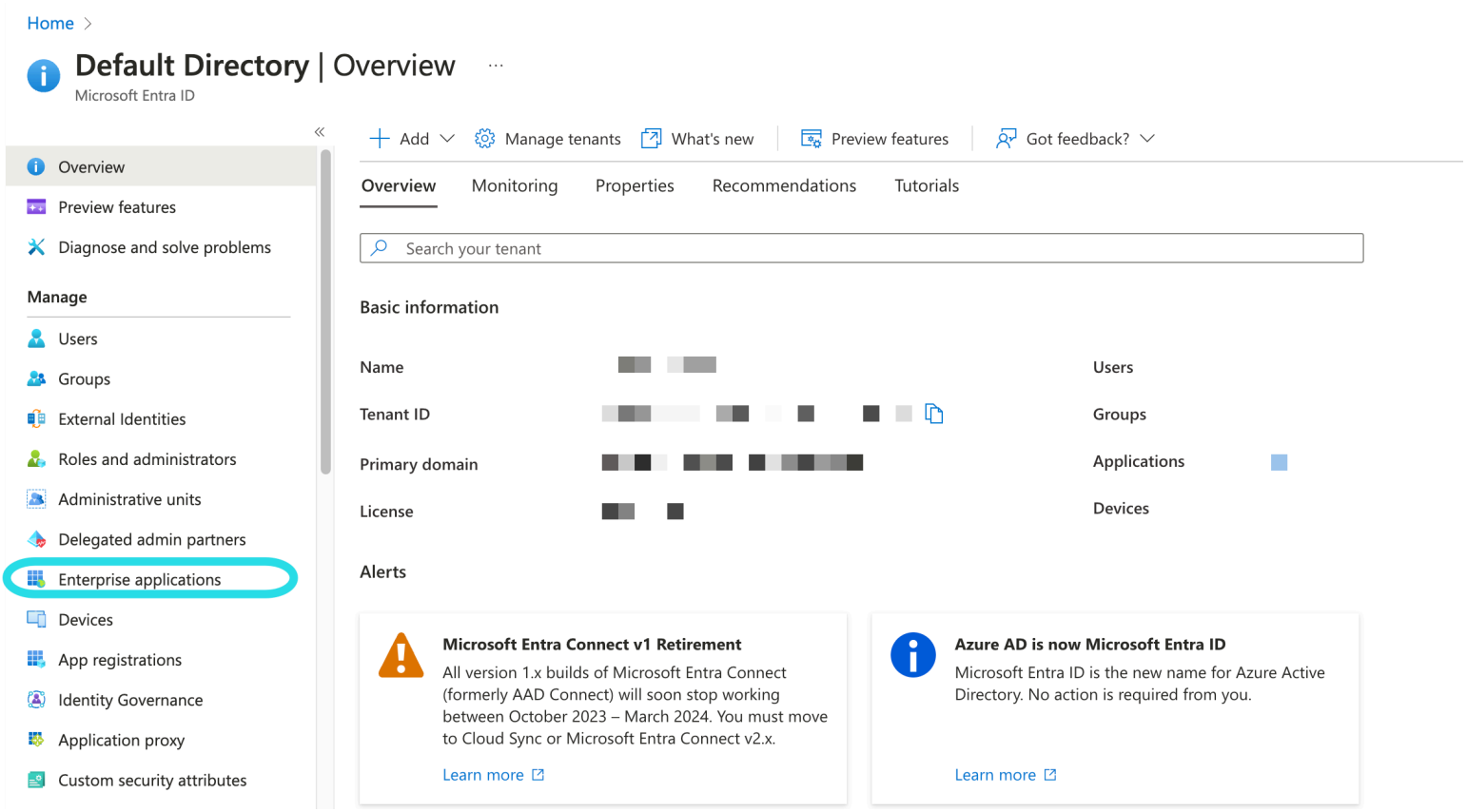
SCIM-Bereitstellung

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

Erstellen Sie eine Enterprise-Anwendung

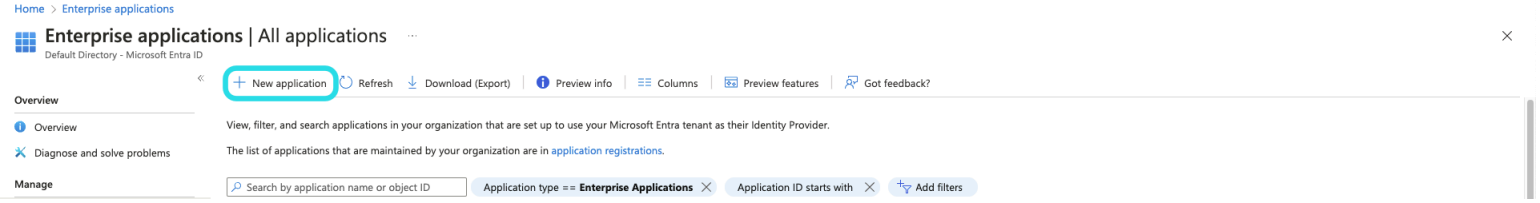
> **Tip**
>
> If you are already using this IdP for Login with SSO, open that existing enterprise application and skip to this step. Otherwise, proceed with this section to create a new application

Im Azure Portal navigieren Sie zu **Microsoft Entra ID** und wählen Sie **Enterprise-Anwendungen** aus dem Navigationsmenü:



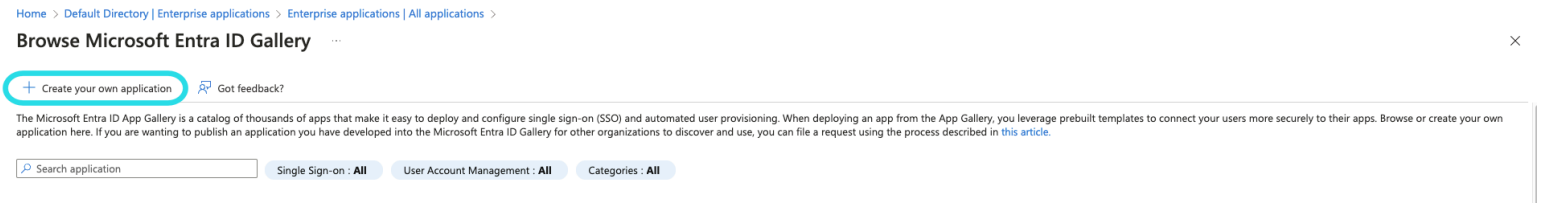
Enterprise applications

Wählen Sie die **+ Neue Anwendung** Schaltfläche:



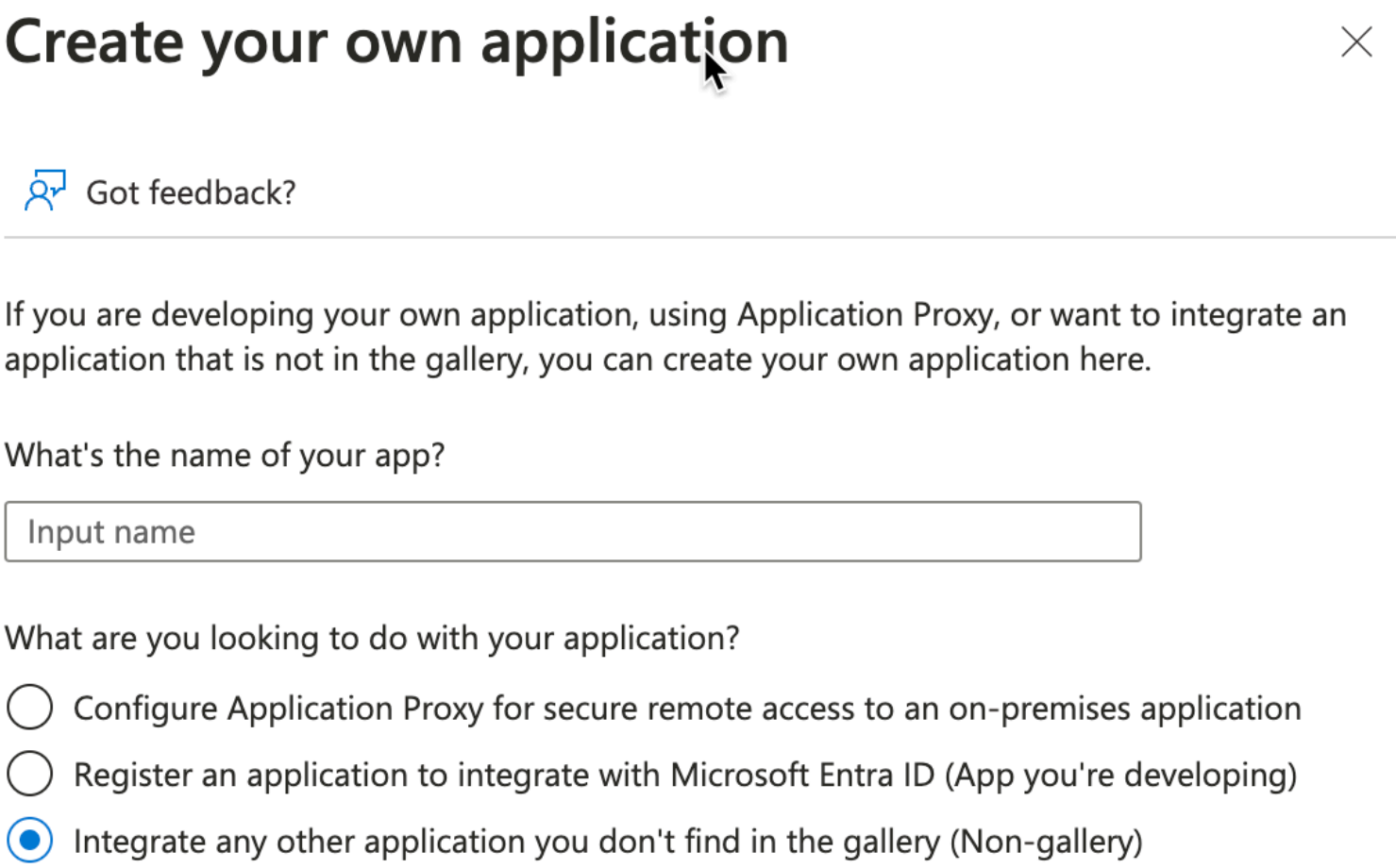
Create new application

Auf dem Bildschirm **Microsoft Entra ID** Galerie auswählen, wählen Sie die **+ Erstellen Sie Ihre eigene Anwendung** Schaltfläche:



Create your own application

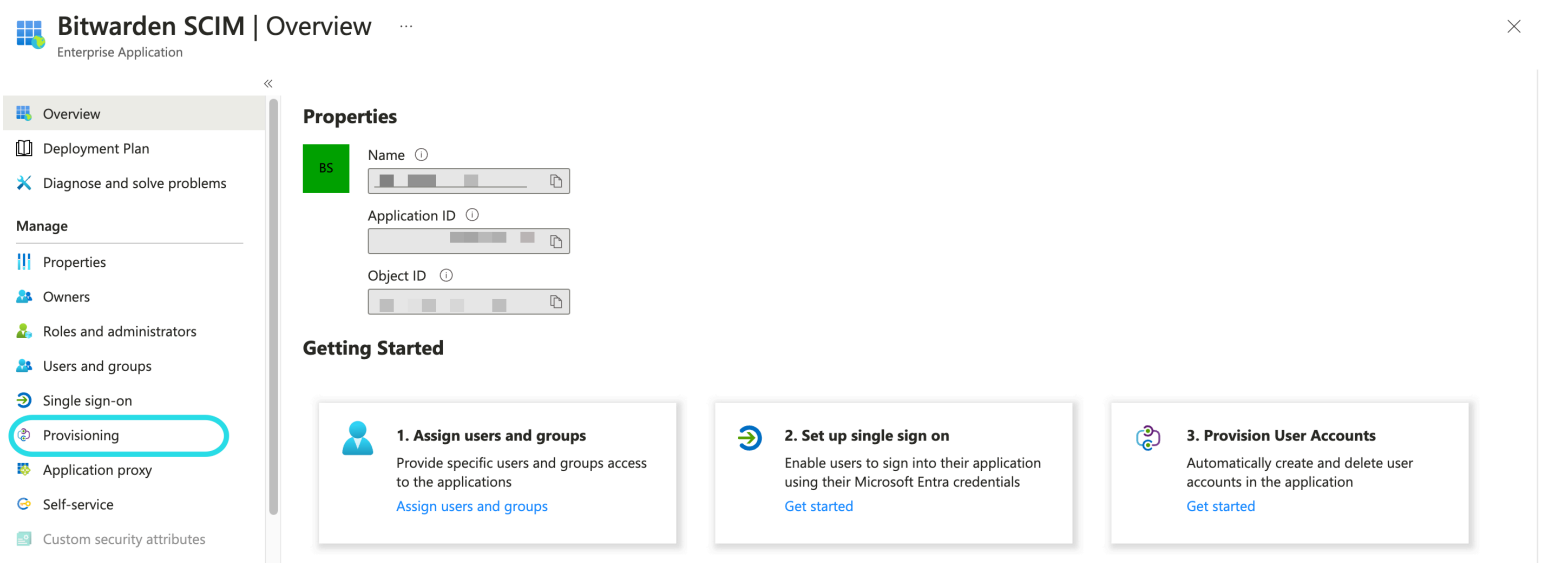
Auf dem Bildschirm "Erstellen Sie Ihre eigene Anwendung" geben Sie der Anwendung einen einzigartigen, Bitwarden-spezifischen Namen. Wählen Sie die **Nicht-Galerie** Option und klicken Sie dann auf den **Erstellen** Knopf.



Create Entra ID app

Provisionierung aktivieren

Wählen Sie **Bereitstellung** aus der Navigation aus und führen Sie die folgenden Schritte aus:



Select Provisioning

1. Wählen Sie die Schaltfläche **Starten**.
2. Wählen Sie **Automatisch** aus dem **Bereitstellungsmodus** Dropdown-Menü.
3. Geben Sie Ihre SCIM-URL (mehr erfahren) in das Feld **Mieter-URL** ein.
4. Geben Sie Ihren SCIM-API-Schlüssel (mehr erfahren) in das Feld **Geheimes Token** ein.
5. Wählen Sie die Schaltfläche **Verbindung testen**.
6. Wenn Ihr Verbindungstest erfolgreich ist, wählen Sie die **Speichern** Schaltfläche.

Zuordnungen

Bitwarden verwendet standardmäßige SCIM v2 Attributnamen, obwohl diese sich von den Attributnamen von Microsoft Entra ID unterscheiden können. Die Standardzuordnungen funktionieren, aber Sie können diesen Abschnitt verwenden, um Änderungen vorzunehmen, wenn Sie möchten. Bitwarden wird die folgenden Eigenschaften für Benutzer und Gruppen verwenden:

Benutzermapping

Bitwarden Attribut	Standard AAD Attribut
`aktiv`	`Wechsel([IstSoftGelöscht], , "Falsch", "Wahr", "Wahr", "Falsch")`
`E-Mails`[a] oder `Benutzername`	`Post` oder `userPrincipalName`
`Anzeigename`	`Anzeigename`

Bitwarden Attribut	Standard AAD Attribut
`ExterneId`	`E-Mail-Spitzname`

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

Gruppenzuordnung

Bitwarden Attribut	Standard AAD Attribut
`Anzeigename`	`Anzeigename`
`Mitglieder`	`Mitglieder`
`ExterneId`	`ObjektId`

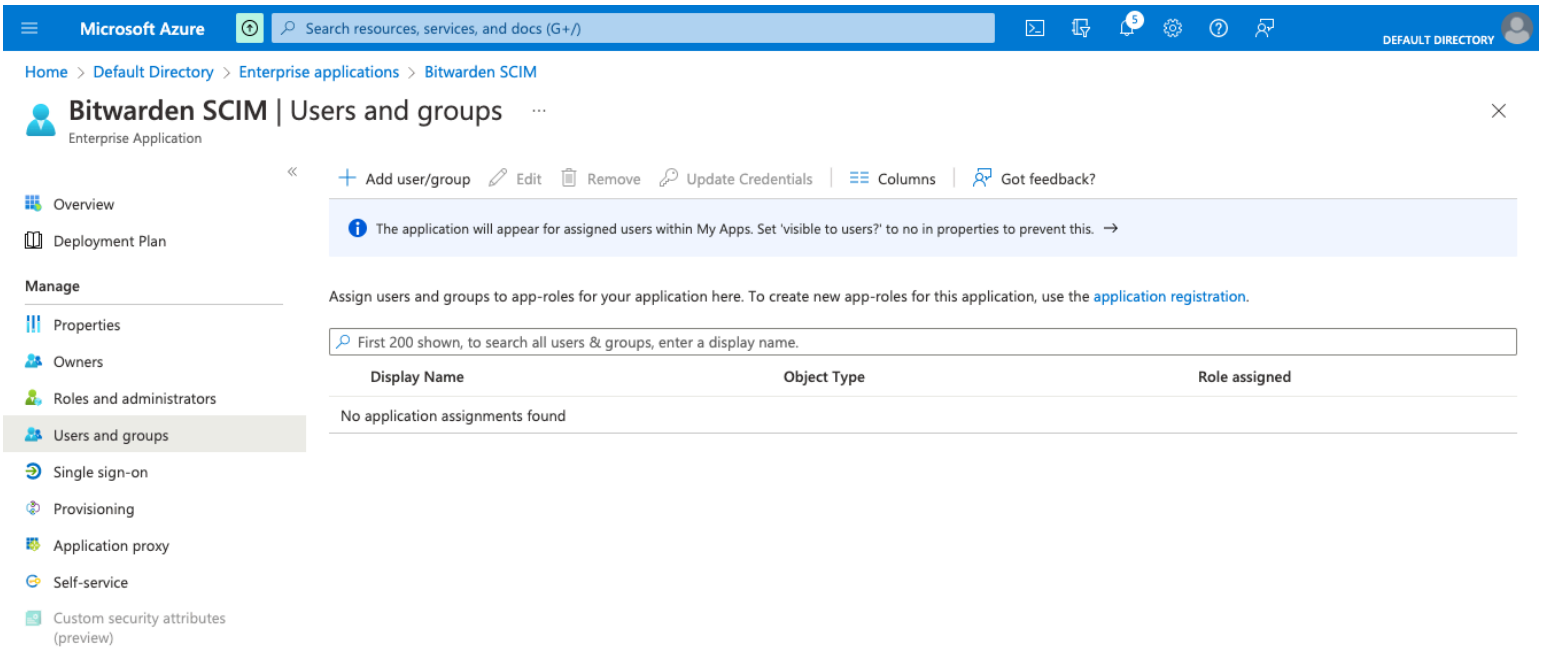
Einstellungen

Unter dem Dropdown-Menü **Einstellungen** wählen Sie:

- Ob eine E-Mail-Benachrichtigung gesendet werden soll, wenn ein Fehler auftritt, und wenn ja, an welche Adresse sie gesendet werden soll (empfohlen).
- Ob nur **zugewiesene Benutzer und Gruppen synchronisiert** werden sollen oder **alle Benutzer und Gruppen synchronisiert** werden sollen. Wenn Sie sich dafür entscheiden, alle Benutzer und Gruppen zu synchronisieren, überspringen Sie den nächsten Schritt.

Benutzer und Gruppen zuweisen

Führen Sie diesen Schritt aus, wenn Sie ausgewählt haben, nur **zugewiesene Benutzer und Gruppen zu synchronisieren** aus den Bereitstellungs-Einstellungen. Wählen Sie **Benutzer und Gruppen** aus der Navigation aus:



Enterprise application users and groups

Wählen Sie die Schaltfläche ┼ **Benutzer/Gruppe hinzufügen** , um den Zugriff auf die SCIM-Anwendung auf Benutzer- oder Gruppenebene zu gewähren. Die folgenden Abschnitte beschreiben, wie Änderungen an Benutzern und Gruppen in Azure ihre Entsprechungen in Bitwarden beeinflussen:

Benutzer

- Wenn einem neuen Benutzer in Azure zugewiesen wird, wird der Benutzer eingeladen, Ihrer Bitwarden Organisation beizutreten.
- Wenn ein Benutzer, der bereits ein Mitglied Ihrer Organisation ist, in Azure zugewiesen wird, wird der Bitwarden-Benutzer über ihren `Benutzername`-Wert mit dem Azure-Benutzer verknüpft.
  - Benutzer, die auf diese Weise verknüpft sind, unterliegen immer noch den anderen Workflows in dieser Liste, jedoch werden Werte wie `displayName` und `externalId/mailNickname` nicht automatisch in Bitwarden geändert.
- Wenn ein zugewiesener Benutzer in Azure gesperrt wird, wird dem Benutzer der Zugang zur Organisation entzogen.
- Wenn ein zugewiesener Benutzer in Azure gelöscht wird, wird der Benutzer aus der Organisation entfernt.
- Wenn ein zugewiesener Benutzer aus einer Gruppe in Azure entfernt wird, wird der Benutzer aus dieser Gruppe in Bitwarden entfernt, bleibt aber ein Mitglied der Organisation.

Gruppen

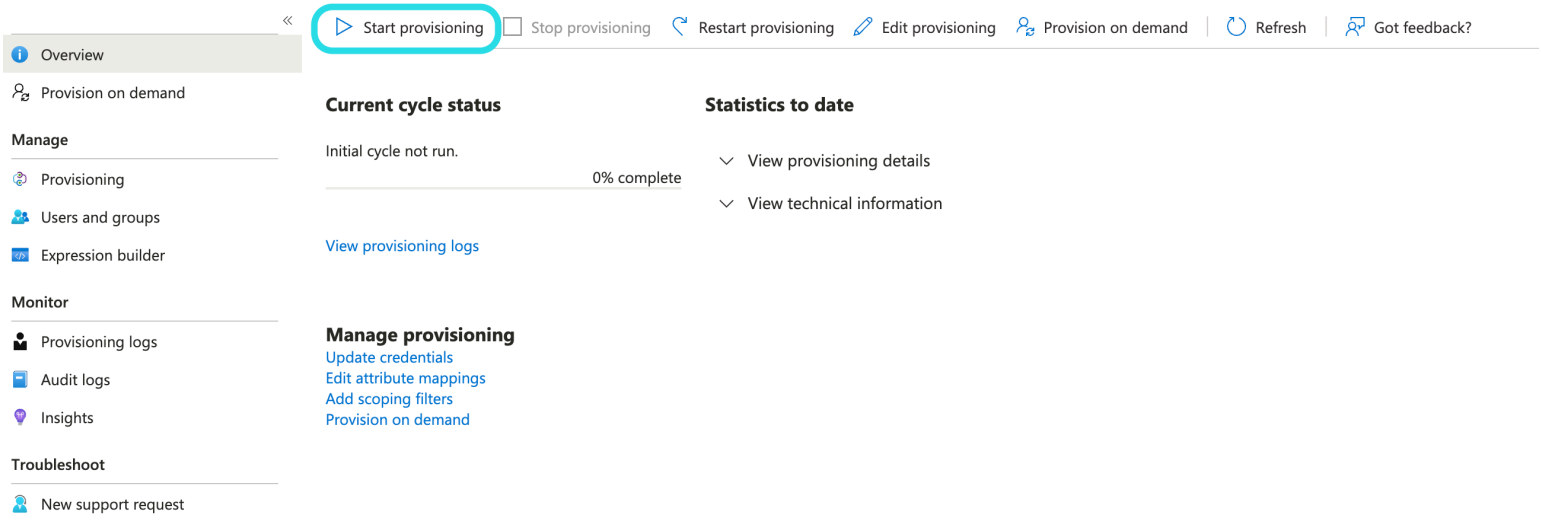
- Wenn in Azure eine neue Gruppe zugewiesen wird, wird die Gruppe in Bitwarden erstellt.
  - Gruppenmitglieder, die bereits Mitglieder Ihrer Bitwarden Organisation sind, werden der Gruppe hinzugefügt.
  - Gruppenmitglieder, die noch nicht Mitglieder Ihrer Bitwarden Organisation sind, werden eingeladen beizutreten.
- Wenn eine Gruppe, die bereits in Ihrer Bitwarden Organisation existiert, in Azure zugewiesen wird, wird die Bitwarden Gruppe über die `displayName` und `externalId`/`objectId` Werte mit Azure verknüpft.

  - Gruppen, die auf diese Weise verknüpft sind, werden ihre Mitglieder aus Azure synchronisieren.

- Wenn eine Gruppe in Azure umbenannt wird, wird sie in Bitwarden aktualisiert, solange die erste Synchronisation durchgeführt wurde.
  - Wenn eine Gruppe in Bitwarden umbenannt wird, wird sie wieder auf den Namen zurückgesetzt, den sie in Azure hat. Ändern Sie immer Gruppennamen auf der Azure-Seite.

Beginnen Sie mit der Bereitstellung

Sobald die Anwendung vollständig konfiguriert ist, starten Sie die Bereitstellung, indem Sie die ▷ **Bereitstellung starten** Schaltfläche auf der **Bereitstellungs** Seite der Enterprise-Anwendung auswählen:



Start provisioning

Benutzer-Onboarding abschließen

Jetzt, wo Ihre Benutzer bereitgestellt wurden, werden sie Einladungen erhalten, 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.