BEHEERCONSOLE > GEBRUIKERSBEHEER >

Microsoft Entra ID SCIM integratie

Microsoft Entra ID SCIM integratie

System for cross-domain identity management (SCIM) kan worden gebruikt om leden en groepen in uw Bitwarden-organisatie automatisch te provisioneren en de-provisioneren.

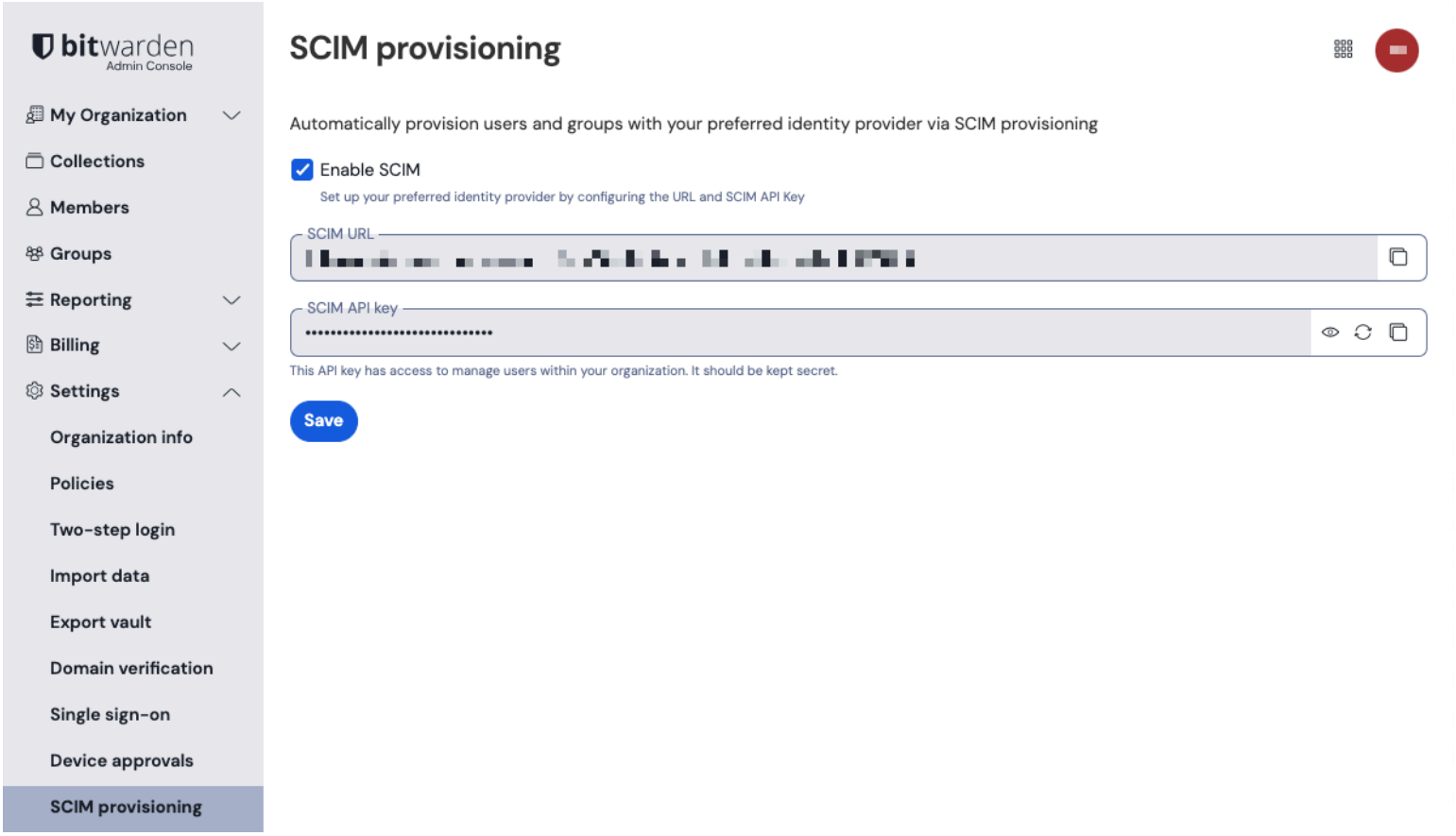
> **Note**
>
> SCIM-integraties zijn beschikbaar voor **Enterprise-organisaties**. Teams organisaties, of klanten die geen SCIM-compatibele identity provider gebruiken, kunnen overwegen Directory Connector te gebruiken als een alternatieve manier van provisioning.

Dit artikel zal je helpen om een SCIM integratie met Azure te configureren. Bij de configuratie wordt tegelijkertijd gewerkt met de Bitwarden web vault en Azure Portal. We raden u aan om beide documenten bij de hand te hebben en de stappen uit te voeren in de volgorde waarin ze zijn beschreven.

SCIM inschakelen

> **Note**
>
> **Host je Bitwarden zelf?** Zo ja, voer dan deze stappen uit om SCIM in te schakelen voor uw server voordat u verdergaat.

Om uw SCIM-integratie te starten, opent u de beheerconsole en navigeert u naar **Instellingen** → **SCIM-provisioning**:



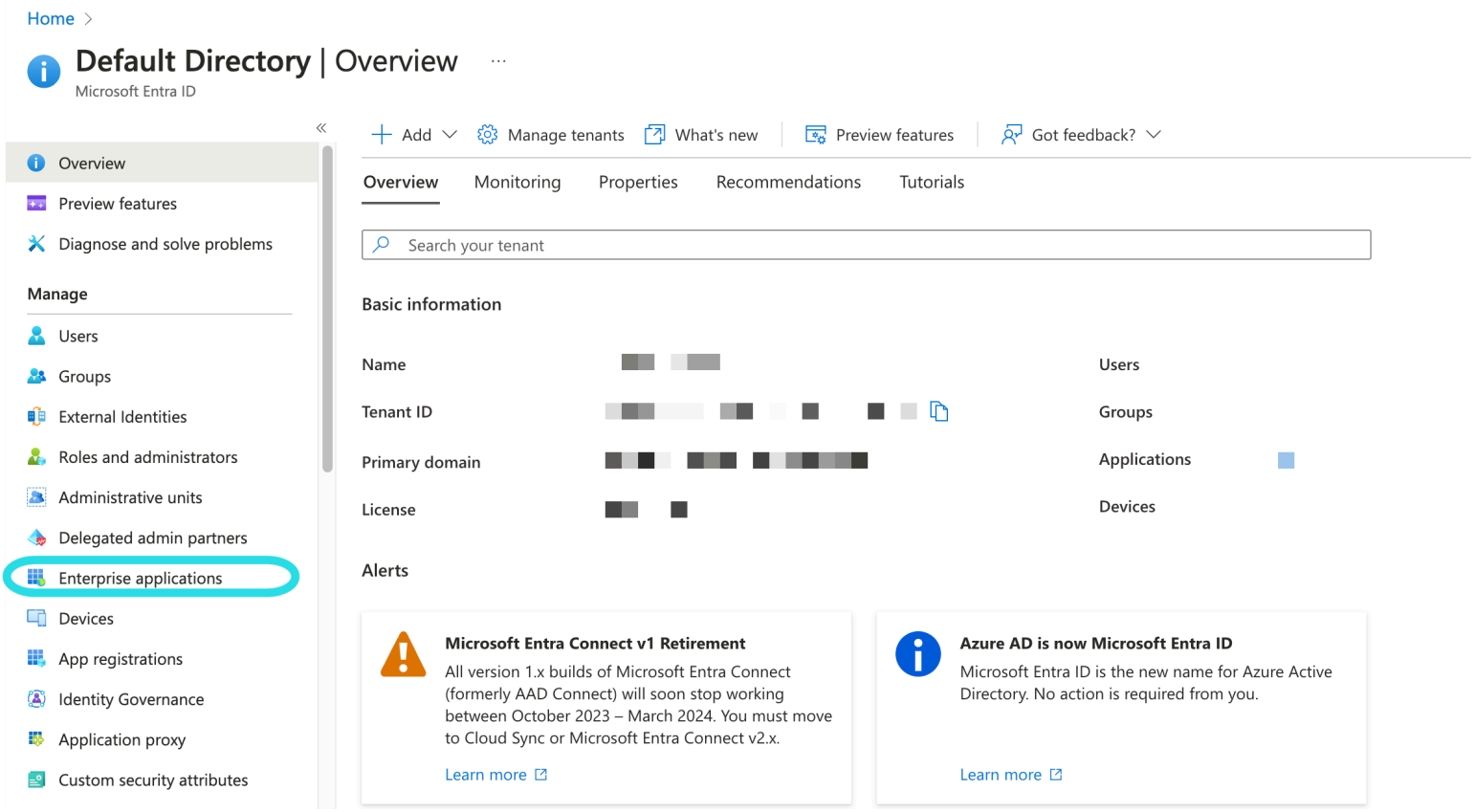
SCIM-voorziening

Schakel het selectievakje **Enable SCIM in** en noteer uw **SCIM URL** en **SCIM API Key**. Je zult beide waarden in een latere stap moeten gebruiken.

Een bedrijfsapplicatie maken

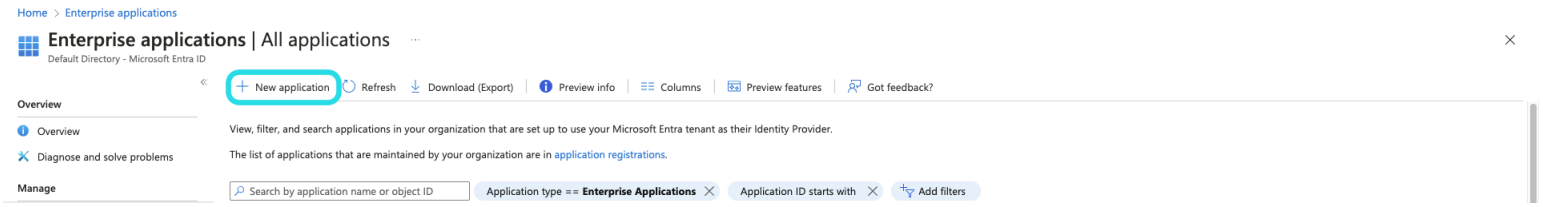
> **Tip**
>
> If you are already using this IdP for Login with SSO, open that existing enterprise application and skip to this step. Otherwise, proceed with this section to create a new application

Navigeer in de Azure Portal naar **Microsoft Entra ID** en selecteer **Enterprise toepassingen** in het navigatiemenu:



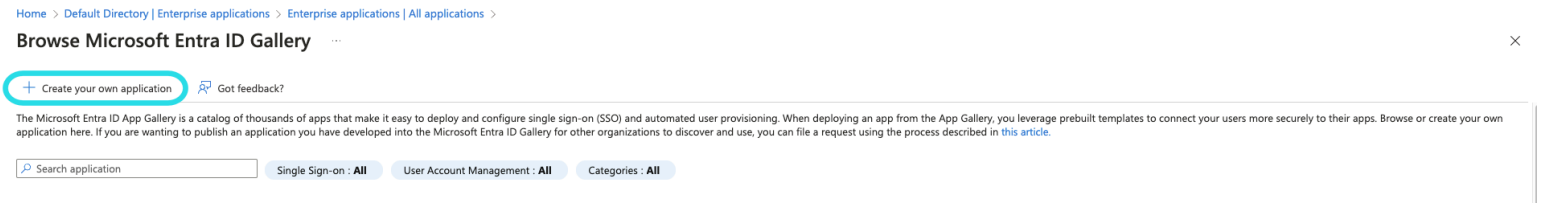
Enterprise applications

Selecteer de knop ＋ **Nieuwe toepassing**:



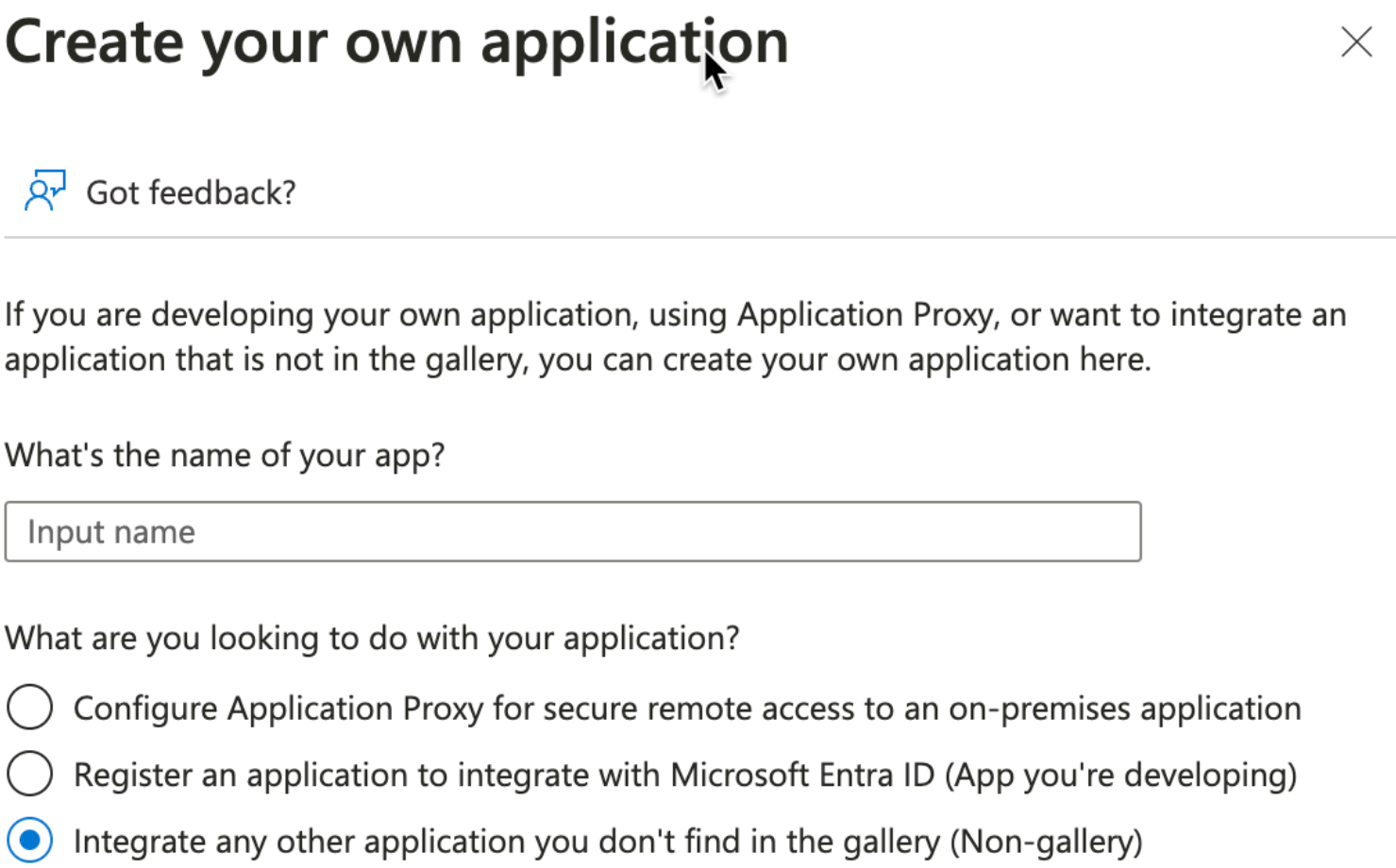
Create new application

Selecteer op het scherm Browse **Microsoft Entra ID** Gallery de knop ＋ **Maak uw eigen toepassing**:



Create your own application

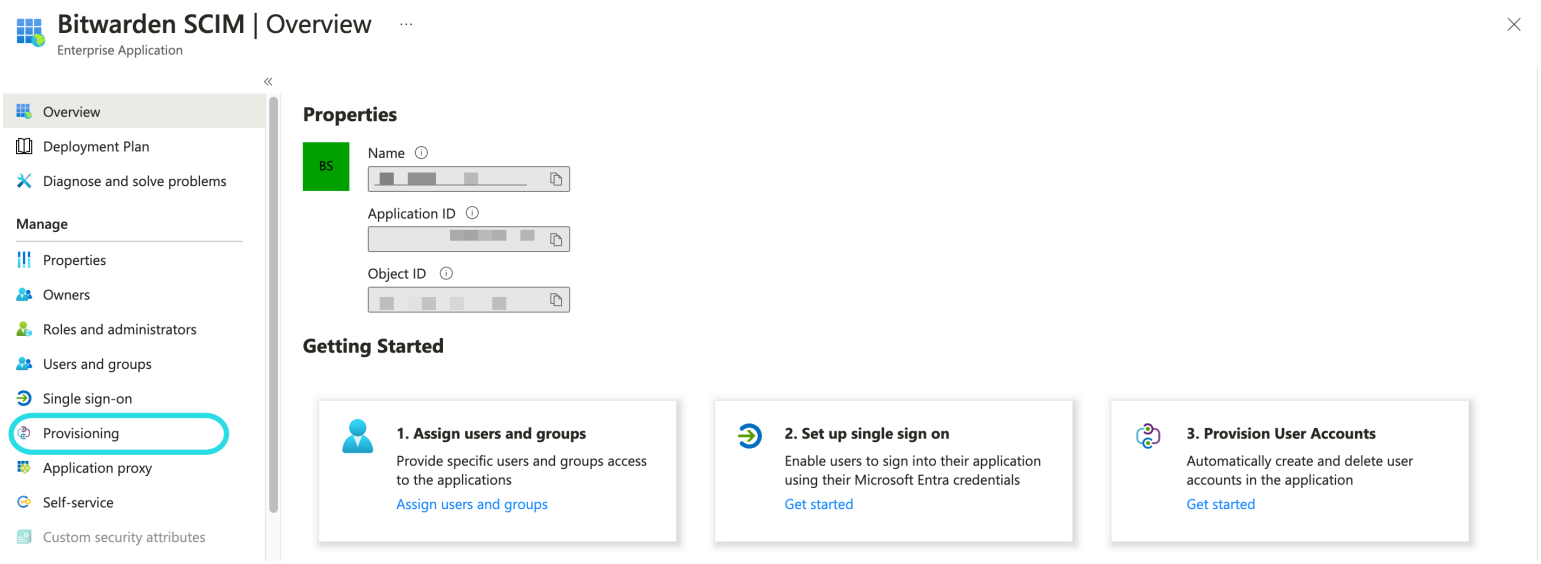
Geef de applicatie in het scherm Maak uw eigen applicatie een unieke, Bitwarden-specifieke naam. Kies de optie **Non-gallery** en selecteer dan de knop **Create**.



Create Entra ID app

Voorziening inschakelen

Selecteer **Provisioning** in de navigatie en voer de volgende stappen uit:



Select Provisioning

1. Selecteer de knop **Aan de slag**.
2. Selecteer **Automatisch** in het vervolgkeuzemenu **Provisioneringsmodus** .
3. Voer uw SCIM URL(meer informatie) in het veld **Tenant URL** in.
4. Voer uw SCIM API-sleutel(meer informatie) in het veld **Secret Token** in.
5. Selecteer de knop **Verbinding testen** .
6. Als je verbindingstest succesvol is, selecteer je de knop **Opslaan** .

Koppelingen

Bitwarden gebruikt standaard SCIM v2 attribuutnamen, hoewel deze kunnen afwijken van de Microsoft Entra ID attribuutnamen. De standaard toewijzingen zullen werken, maar je kunt dit gedeelte gebruiken om wijzigingen aan te brengen als je dat wilt. Bitwarden gebruikt de volgende eigenschappen voor gebruikers en groepen:

Gebruiker in kaart brengen

Bitwarden kenmerk	Standaard AAD-kenmerk
`actief`	`Schakelaar ([IsSoftDeleted], , "Vals", "Waar", "Waar", "Vals")`
`e-mail`ª of `gebruikersnaam`	`mail` of `userPrincipalName`
`weergavenaam`	`weergavenaam`

Bitwarden kenmerk	Standaard AAD-kenmerk
`externalId`	`mailNickname`

[a] - Omdat SCIM gebruikers toestaat om meerdere e-mailadressen te hebben uitgedrukt als een array van objecten, zal Bitwarden de `waarde` gebruiken van het object dat "primary" bevat `: true`.

Groep in kaart brengen

Bitwarden kenmerk	Standaard AAD-kenmerk
`weergavenaam`	`weergavenaam`
`leden`	`leden`
`externalId`	`objectId`

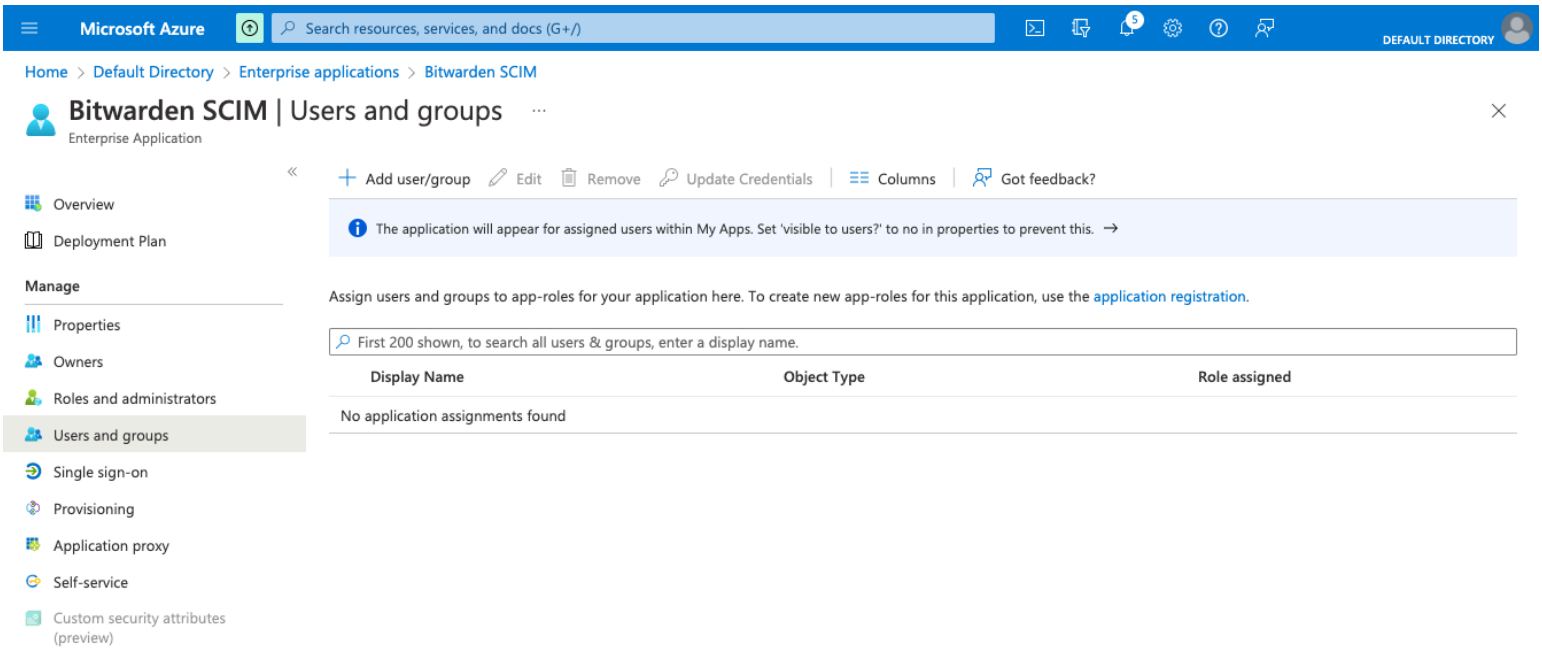
Instellingen

Kies in de vervolgkeuzelijst **Instellingen** :

- Of er een e-mailmelding moet worden verstuurd als er een storing optreedt en zo ja, naar welk adres (aanbevolen).
- Of **alleen toegewezen gebruikers en groepen gesynchroniseerd** moeten worden of **alle gebruikers en groepen**. Als je ervoor kiest om alle gebruikers en groepen te synchroniseren, sla dan de volgende stap over.

Gebruikers en groepen toewijzen

Voltooi deze stap als je ervoor hebt gekozen om **alleen toegewezen gebruikers en groepen te synchroniseren** vanuit de provisioning-instellingen. Selecteer **Gebruikers en groepen** in de navigatie:



Enterprise application users and groups

Selecteer de knop ┼ **Gebruiker/groep toevoegen** om toegang tot de SCIM-toepassing toe te wijzen op gebruikers- of groepsniveau. In de volgende paragrafen wordt beschreven hoe het wijzigen van gebruikers en groepen in Azure van invloed is op hun tegenhangers in Bitwarden:

Gebruikers

- Wanneer een nieuwe gebruiker wordt toegewezen in Azure, wordt de gebruiker uitgenodigd voor uw Bitwarden-organisatie.
- Wanneer een gebruiker die al lid is van uw organisatie wordt toegewezen in Azure, wordt de Bitwarden-gebruiker gekoppeld aan de Azure-gebruiker via hun `UserName-waarde`.
  - Gebruikers die op deze manier zijn gekoppeld, vallen nog steeds onder de andere workflows in deze lijst, maar waarden zoals `displayName` en `externalId/mailNickname` worden niet automatisch gewijzigd in Bitwarden.
- Wanneer een toegewezen gebruiker wordt opgeschort in Azure, wordt de toegang van de gebruiker tot de organisatie ingetrokken.
- Wanneer een toegewezen gebruiker wordt verwijderd in Azure, wordt de gebruiker verwijderd uit de organisatie.
- Wanneer een toegewezen gebruiker wordt verwijderd uit een groep in Azure, wordt de gebruiker verwijderd uit die groep in Bitwarden, maar blijft hij lid van de organisatie.

Groepen

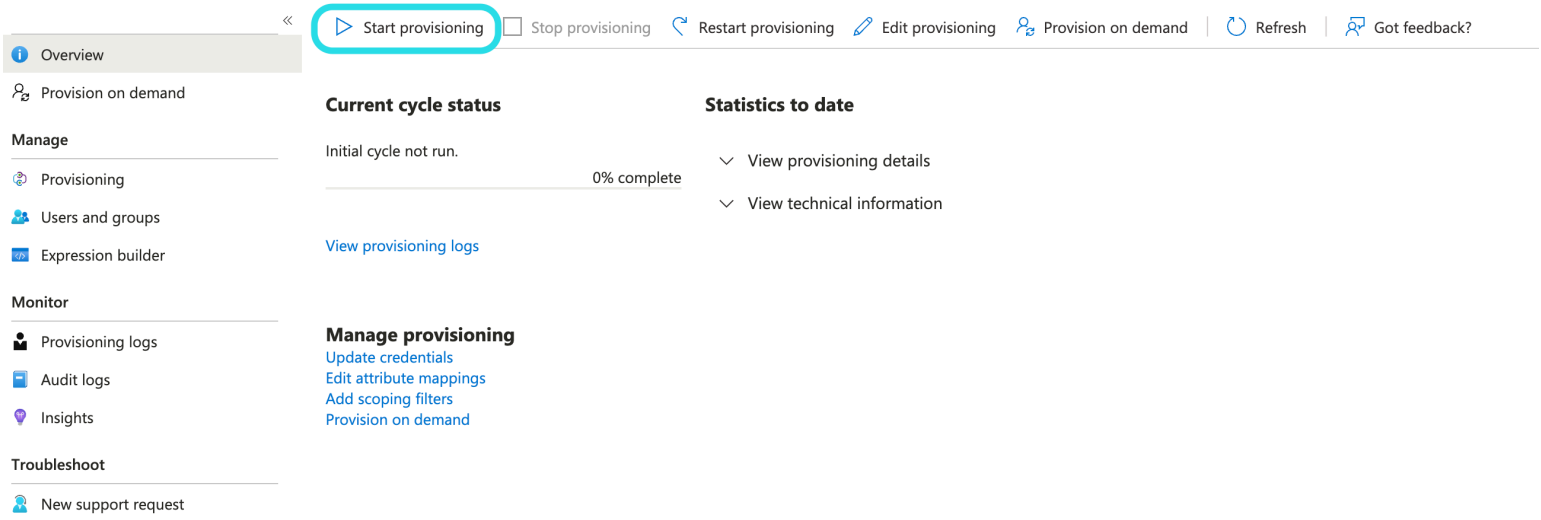
- Wanneer een nieuwe groep wordt toegewezen in Azure, wordt de groep aangemaakt in Bitwarden.
  - Groepsleden die al lid zijn van uw Bitwarden-organisatie worden toegevoegd aan de groep.
  - Groepsleden die nog geen lid zijn van je Bitwarden-organisatie worden uitgenodigd om lid te worden.
- Wanneer een groep die al bestaat in uw Bitwarden-organisatie wordt toegewezen in Azure, wordt de Bitwarden-groep aan Azure gekoppeld via de waarden `displayName` en `externalId` / `objectId` .

  - Groepen die op deze manier gelinkt zijn, zullen hun leden gesynchroniseerd zien vanuit Azure.

- Als een groep wordt hernoemd in Azure, wordt deze bijgewerkt in Bitwarden zolang de initiële synchronisatie heeft plaatsgevonden.
  - Als een groep een andere naam krijgt in Bitwarden, wordt deze terugveranderd naar de naam in Azure. Verander groepsnamen altijd Azure-side.

Provisioning starten

Zodra de applicatie volledig is geconfigureerd, start je de provisioning door de knop ▷ **Start provisioning** te selecteren op de pagina **Provisioning** van de bedrijfsapplicatie:



Start provisioning

Onboarding van gebruikers voltooien

Nu je gebruikers zijn voorzien, ontvangen ze uitnodigingen om lid te worden van de organisatie. Instrueer je gebruikers om de uitnodiging te accepteren en bevestig ze daarna aan de organisatie.

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