CONSOLE ADMIN > GESTION DES UTILISATEURS >

Intégration SCIM de Microsoft Entra ID

Intégration SCIM de Microsoft Entra ID

Le système de gestion d'identité inter-domaines (SCIM) peut être utilisé pour provisionner et déprovisionner automatiquement les membres et les groupes dans votre organisation Bitwarden.

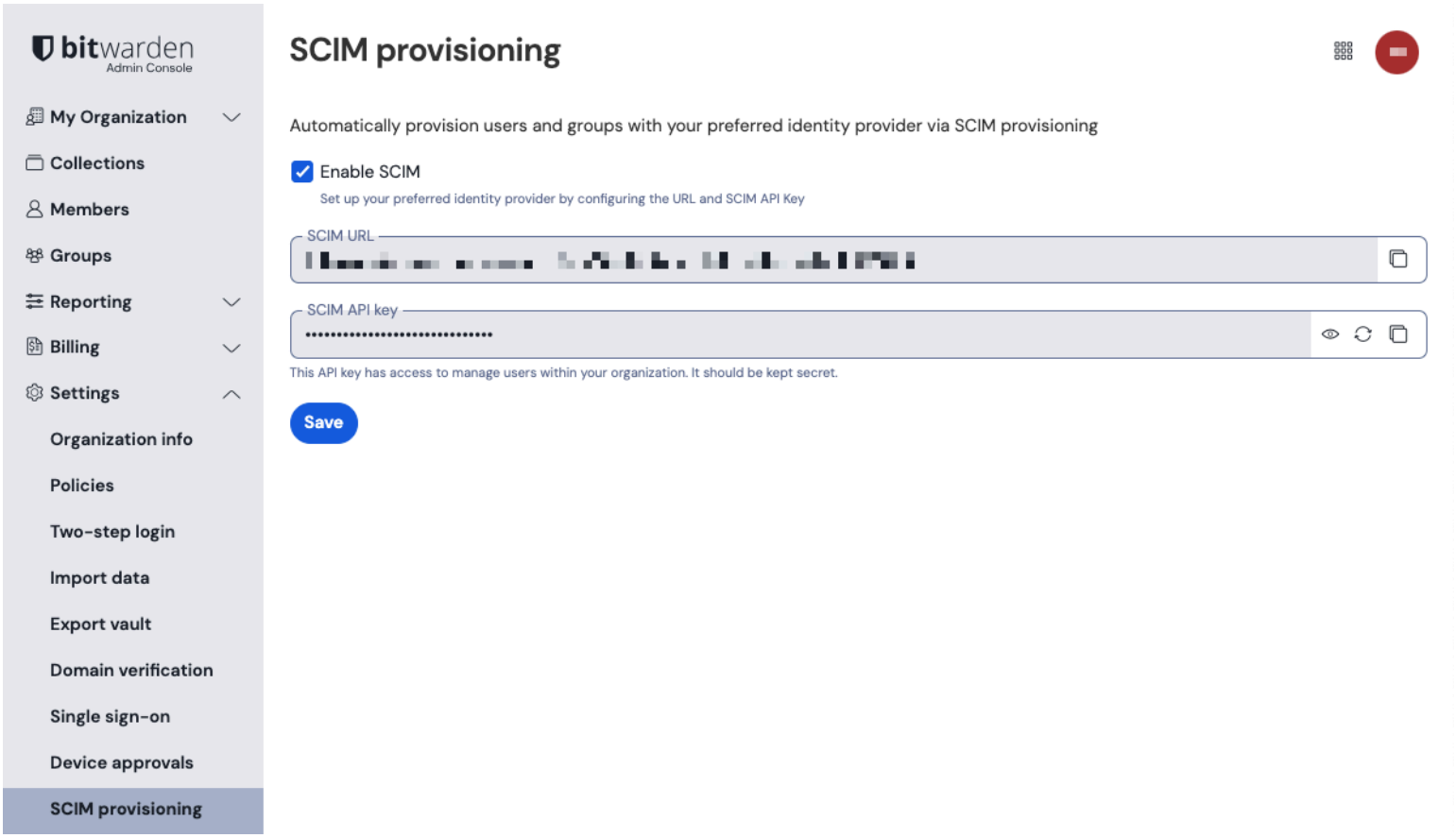
> **Note**
>
> Les intégrations SCIM sont disponibles pour les **organisations d'Entreprise**. Les organisations d'Équipes, ou les clients n'utilisant pas un fournisseur d'identité compatible SCIM, peuvent envisager d'utiliser Directory Connector comme moyen alternatif de provisionnement.

Cet article vous aidera à configurer une intégration SCIM avec Azure. La configuration implique de travailler simultanément avec le coffre web Bitwarden et Azure Portal. Au fur et à mesure que vous avancez, nous vous recommandons d'avoir les deux facilement disponibles et de compléter les étapes dans l'ordre où elles sont documentées.

Activer SCIM

> **Note**
>
> **Hébergez-vous vous-même Bitwarden?** Si c'est le cas, terminez ces étapes pour activer SCIM pour votre serveur avant de continuer.

Pour commencer votre intégration SCIM, ouvrez la Console Admin et naviguez vers **Paramètres** → **Provisionnement SCIM**:



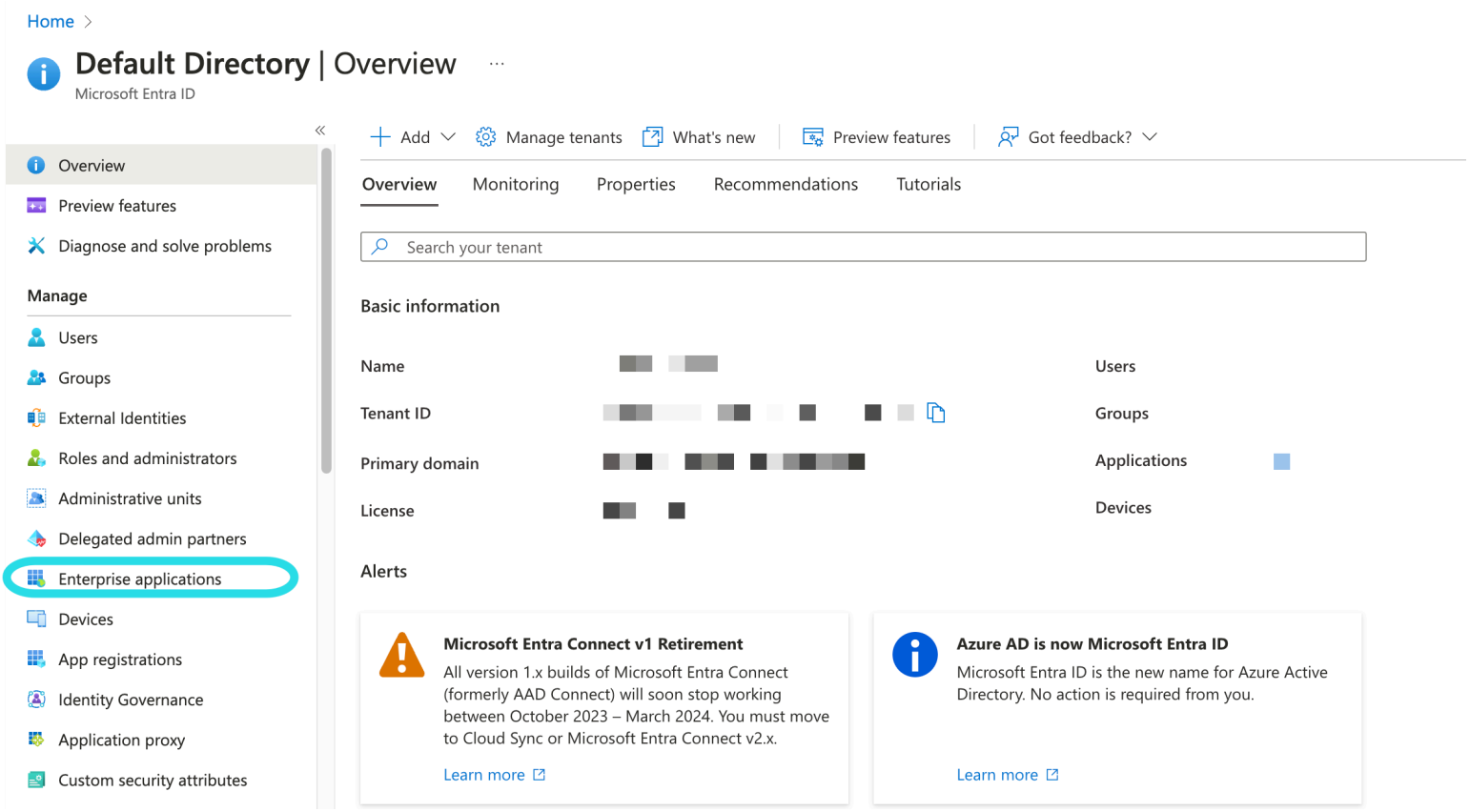
Provisionnement SCIM

Sélectionnez la case à cocher **Activer SCIM** et prenez note de votre **URL SCIM** et de votre **Clé API SCIM**. Vous devrez utiliser les deux valeurs dans une étape ultérieure.

Créez une application d'entreprise

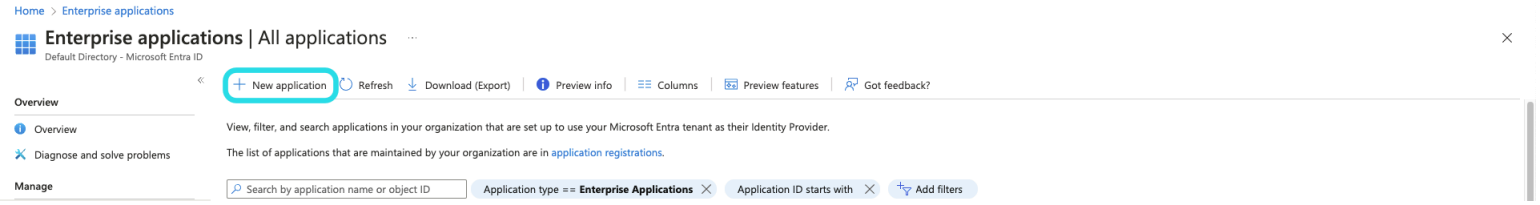
> **Tip**
>
> If you are already using this IdP for Login with SSO, open that existing enterprise application and skip to this step. Otherwise, proceed with this section to create a new application

Dans le Portail Azure, naviguez jusqu'à **Microsoft Entra ID** et sélectionnez **Applications d'entreprise** à partir du menu de navigation :



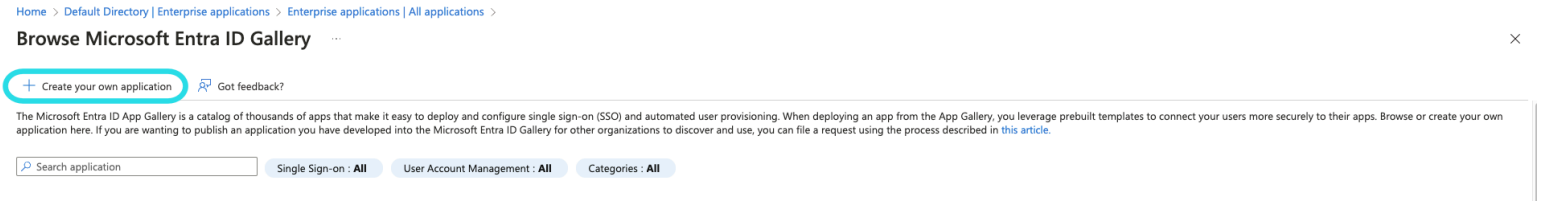
Enterprise applications

Sélectionnez le bouton **+ Nouvelle application** :



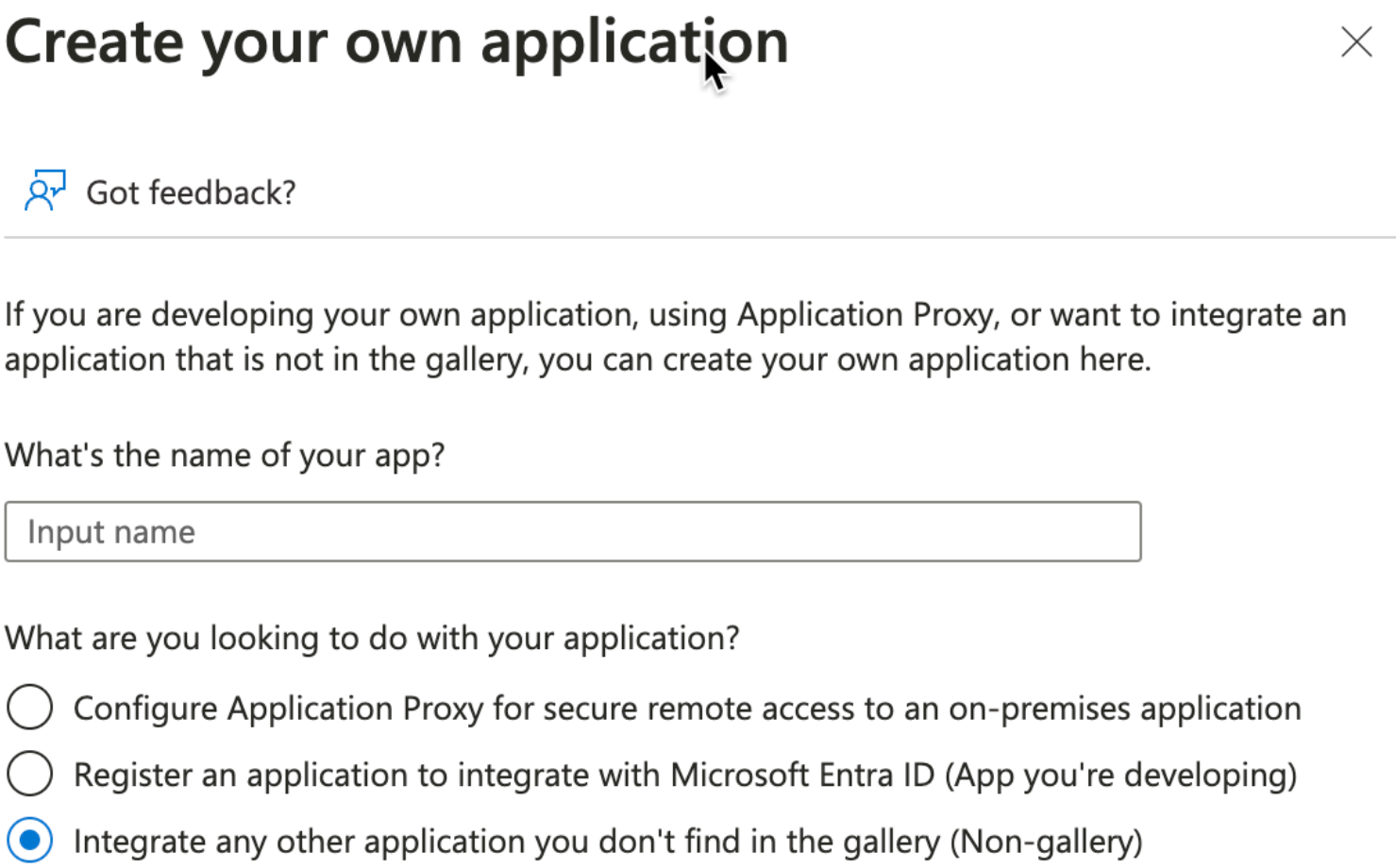
Create new application

Sur l'écran de la galerie **Microsoft Entra ID**, sélectionnez le bouton **+ Créez votre propre application** :



Create your own application

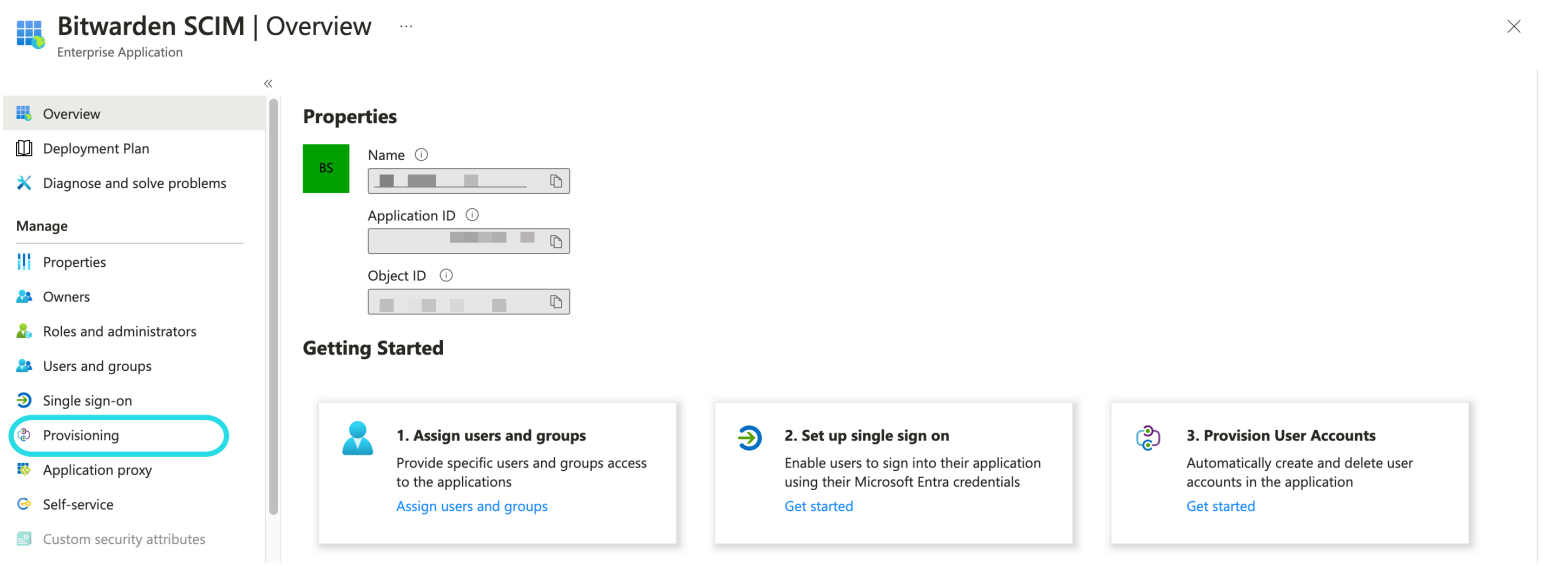
Sur l'écran Créez votre propre application, donnez à l'application un nom unique spécifique à Bitwarden. Choisissez l'option **Non-galerie** puis sélectionnez le bouton **Créer**.



Create Entra ID app

Activer la provision

Sélectionnez **Provisioning** dans la navigation et suivez les étapes suivantes:



Select Provisioning

1. Sélectionnez le bouton **Commencer**.
2. Sélectionnez **Automatique** dans le menu déroulant **Mode de Provisionnement** .
3. Entrez votre URL SCIM (en savoir plus) dans le champ **URL du locataire**.
4. Entrez votre clé API SCIM (en savoir plus) dans le champ **Jeton Secret**.
5. Sélectionnez le bouton **Tester la Connexion** .
6. Si votre test de connexion réussit, sélectionnez le bouton **Enregistrer** .

Cartographies

Bitwarden utilise les noms d'attributs SCIM v2 standard, bien que ceux-ci puissent différer des noms d'attributs Microsoft Entra ID. Les mappages par défaut fonctionneront, mais vous pouvez utiliser cette section pour apporter des modifications si vous le souhaitez. Bitwarden utilisera les propriétés suivantes pour les utilisateurs et les groupes :

Cartographie utilisateur

Attribut Bitwarden	Attribut AAD par défaut
`actif`	`Switch([IsSoftDeleted], , "Faux", "Vrai", "Vrai", "Faux")`
`courriels`[a] ou `nom d'utilisateur`	`courrier` ou `nomPrincipalUtilisateur`
`nom d'affichage`	`nom d'affichage`

Attribut Bitwarden	Attribut AAD par défaut
`identifiant externe`	`surnom de courrier`

[a] - Parce que SCIM permet aux utilisateurs d'avoir plusieurs adresses de courriel exprimées sous forme de tableau d'objets, Bitwarden utilisera la `valeur` de l'objet qui contient `"primary": true`.

Cartographie de groupe

Attribut Bitwarden	Attribut AAD par défaut
`nom d'affichage`	`nom d'affichage`
`membres`	`membres`
`identifiant externe`	`identifiant d'objet`

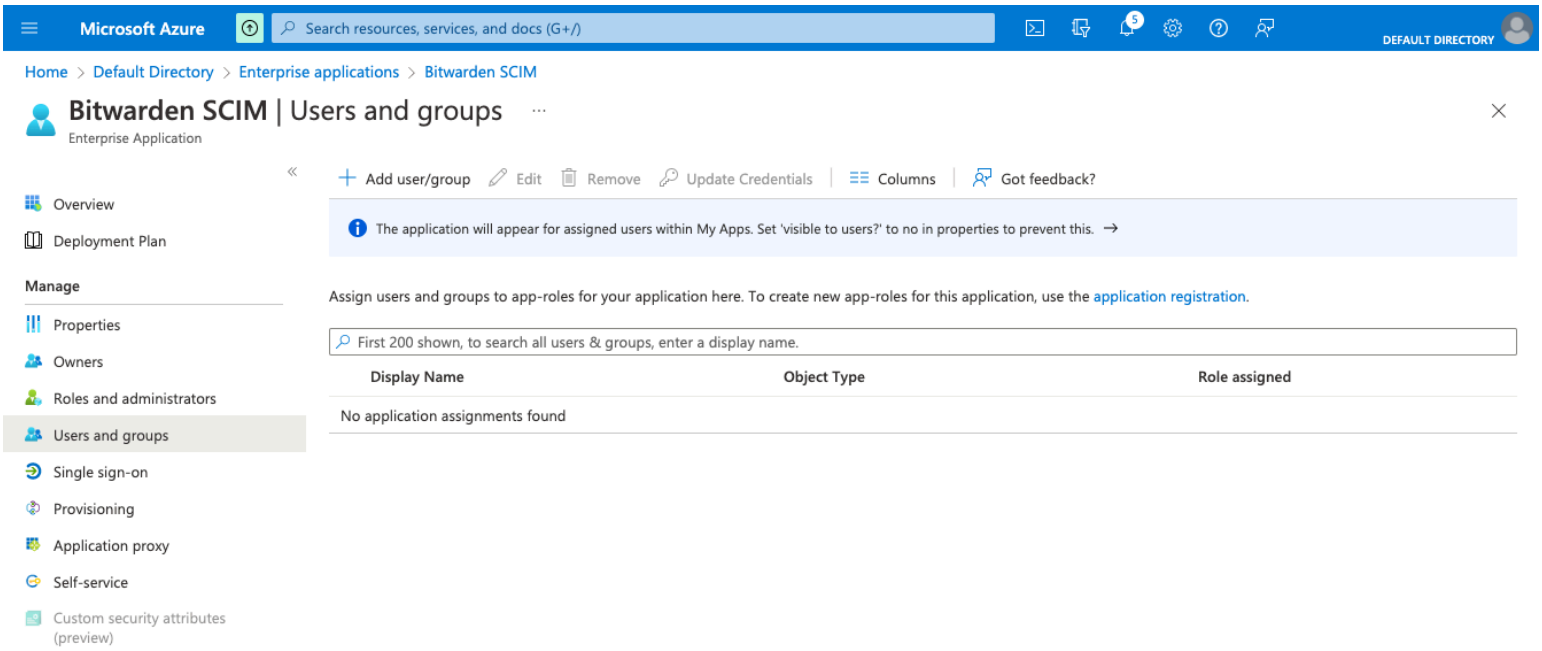
Paramètres

Sous le menu déroulant des **Paramètres** , choisissez :

- Que ce soit pour envoyer une notification par courriel en cas d'échec, et si oui, à quelle adresse l'envoyer (recommandé).
- Que ce soit pour **synchroniser uniquement les utilisateurs et les groupes assignés** ou pour **synchroniser tous les utilisateurs et les groupes**. Si vous choisissez de synchroniser tous les utilisateurs et groupes, passez à l'étape suivante.

Attribuer des utilisateurs et des groupes

Terminez cette étape si vous avez choisi de **synchroniser uniquement les utilisateurs et les groupes assignés** à partir des paramètres de provisionnement. Sélectionnez **Utilisateurs et groupes** dans la navigation:



Enterprise application users and groups

Sélectionnez le bouton ┼ **Ajouter utilisateur/groupe** pour attribuer l'accès à l'application SCIM à un utilisateur ou à un niveau de groupe. Les sections suivantes décrivent comment la modification des utilisateurs et des groupes dans Azure aura un impact sur leurs homologues dans Bitwarden :

Utilisateurs

- Lorsqu'un nouvel utilisateur est assigné dans Azure, l'utilisateur est invité à rejoindre votre organisation Bitwarden.
- Lorsqu'un utilisateur qui est déjà un membre de votre organisation est assigné dans Azure, l'utilisateur Bitwarden est lié à l'utilisateur Azure via leur valeur de `nom d'utilisateur`.
  - Les utilisateurs liés de cette manière sont toujours soumis aux autres flux de travail dans cette liste, cependant des valeurs comme `displayName` et `externalId/mailNickname` ne sont pas automatiquement modifiées dans Bitwarden.
- Lorsqu'un utilisateur assigné est suspendu dans Azure, l'utilisateur se voit révoquer son accès à l'organisation.
- Lorsqu'un utilisateur assigné est supprimé dans Azure, l'utilisateur est retiré de l'organisation.
- Lorsqu'un utilisateur assigné est retiré d'un groupe dans Azure, l'utilisateur est retiré de ce groupe dans Bitwarden mais reste un membre de l'organisation.

Groupes

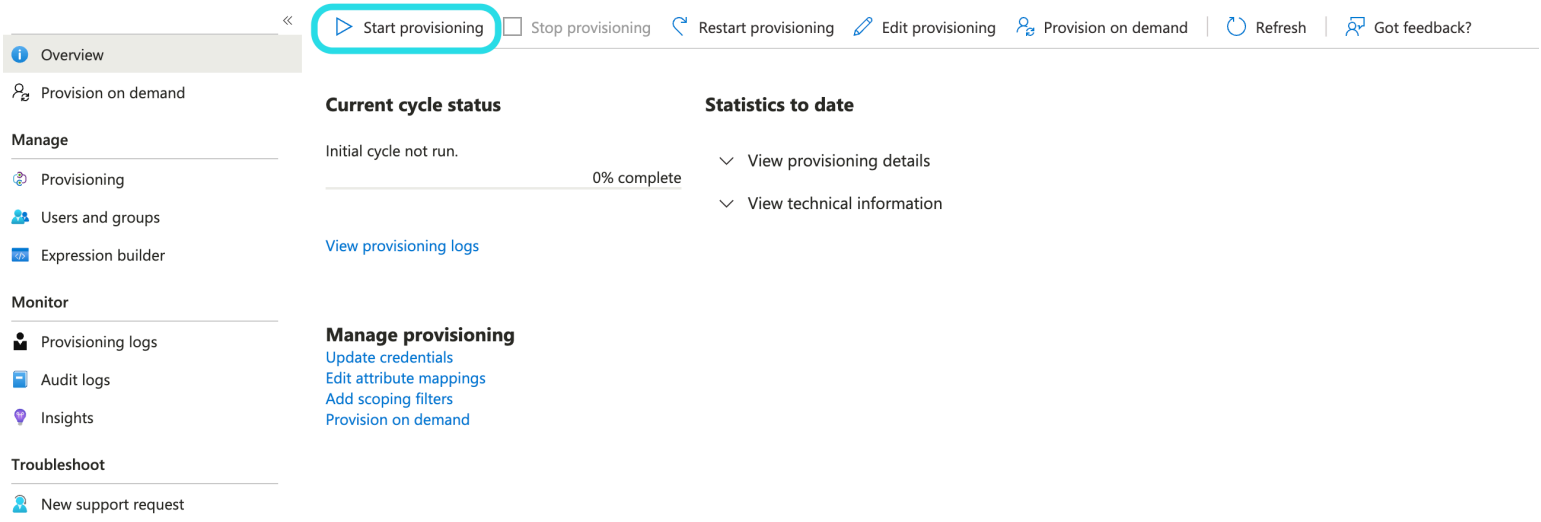
- Lorsqu'un nouveau groupe est attribué dans Azure, le groupe est créé dans Bitwarden.
  - Les membres du groupe qui sont déjà membres de votre organisation Bitwarden sont ajoutés au groupe.
  - Les membres du groupe qui ne sont pas déjà membres de votre organisation Bitwarden sont invités à rejoindre.
- Lorsqu'un groupe qui existe déjà dans votre organisation Bitwarden est assigné dans Azure, le groupe Bitwarden est lié à Azure par le biais des valeurs `displayName` et `externalId`/`objectId`.

- Les groupes liés de cette manière auront leurs membres synchronisés à partir d'Azure.

- Lorsqu'un groupe est renommé dans Azure, il sera mis à jour dans Bitwarden tant que la synchronisation initiale a été effectuée.
  - Lorsqu'un groupe est renommé dans Bitwarden, il sera remis à ce qu'il est nommé dans Azure. Changez toujours les noms de groupe du côté Azure.

Commencez la provision

Une fois l'application entièrement configurée, commencez la provision en sélectionnant le bouton ▷ **Commencer la provision** sur la page de **Provision** de l'application d'entreprise :



Start provisioning

Terminez l'intégration de l'utilisateur

Maintenant que vos utilisateurs ont été provisionnés, ils recevront des invitations pour rejoindre l'organisation. Demandez à vos utilisateurs d'accepter l'invitation et, une fois qu'ils l'ont fait, confirmez-les à l'organisation.

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