CONSOLA DE ADMINISTRADOR > GESTIÓN DE USUARIOS >

Integración SCIM de Microsoft Entra ID

Integración SCIM de Microsoft Entra ID

El sistema para la gestión de identidad entre dominios (SCIM) se puede utilizar para aprovisionar y desaprovisionar automáticamente miembros y grupos en su organización Bitwarden.

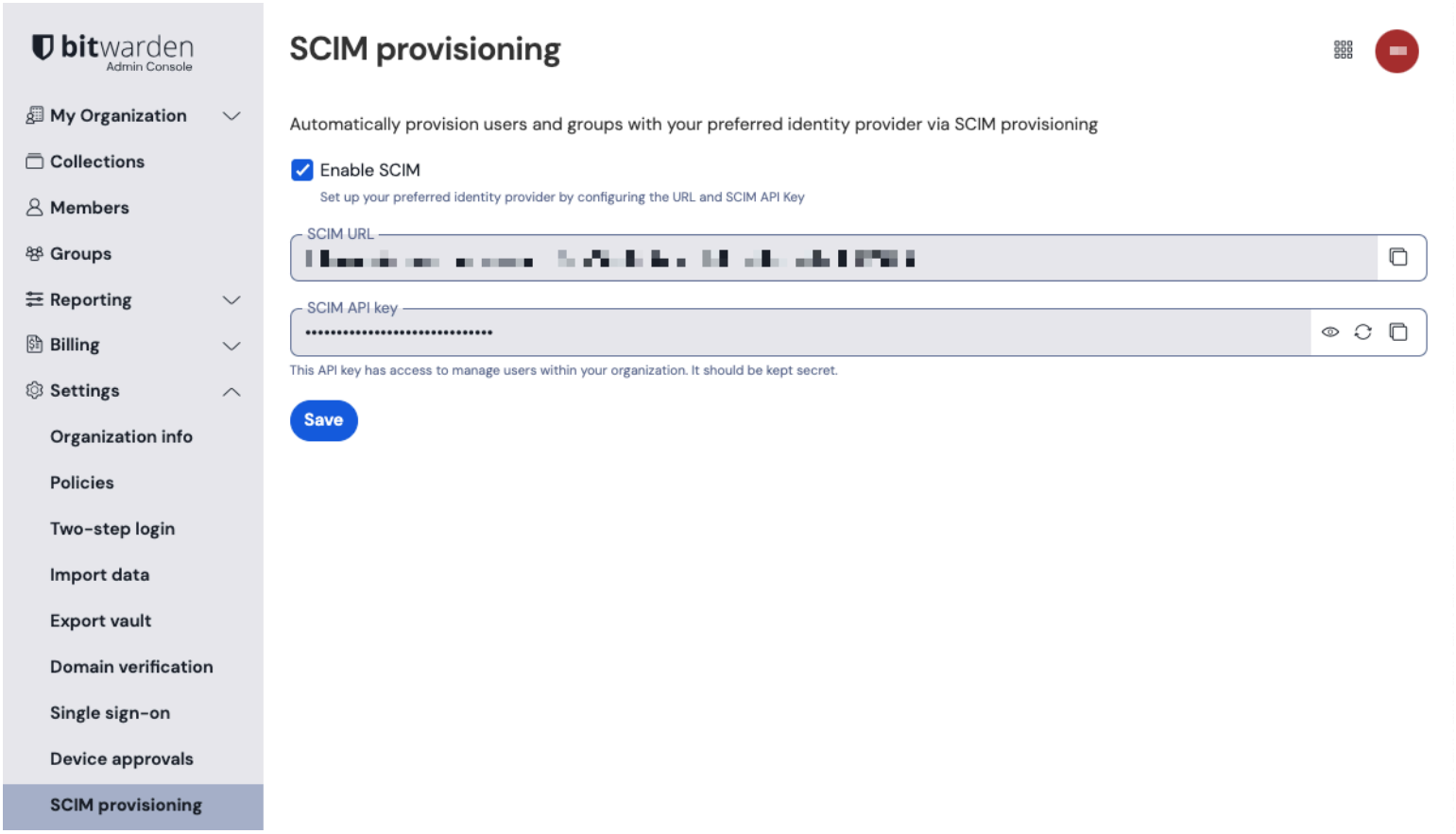
> **Note**
>
> Las integraciones SCIM están disponibles para **organizaciones de Empresa**. Las organizaciones de Equipos, o los clientes que no utilizan un proveedor de identidad compatible con SCIM, pueden considerar el uso de Conector de Directorio como un medio alternativo de aprovisionamiento.

Este artículo te ayudará a configurar una integración SCIM con Azure. La configuración implica trabajar simultáneamente con la caja fuerte web de Bitwarden y Azure Portal. A medida que avanza, recomendamos tener ambos fácilmente disponibles y completar los pasos en el orden en que están documentados.

Activar SCIM

> **Note**
>
> **¿Estás autoalojando Bitwarden?** Si es así, complete estos pasos para habilitar SCIM para su servidor antes de continuar.

Para iniciar su integración SCIM, abra la Consola de Administrador y navegue a **Ajustes** → **Provisión SCIM**:



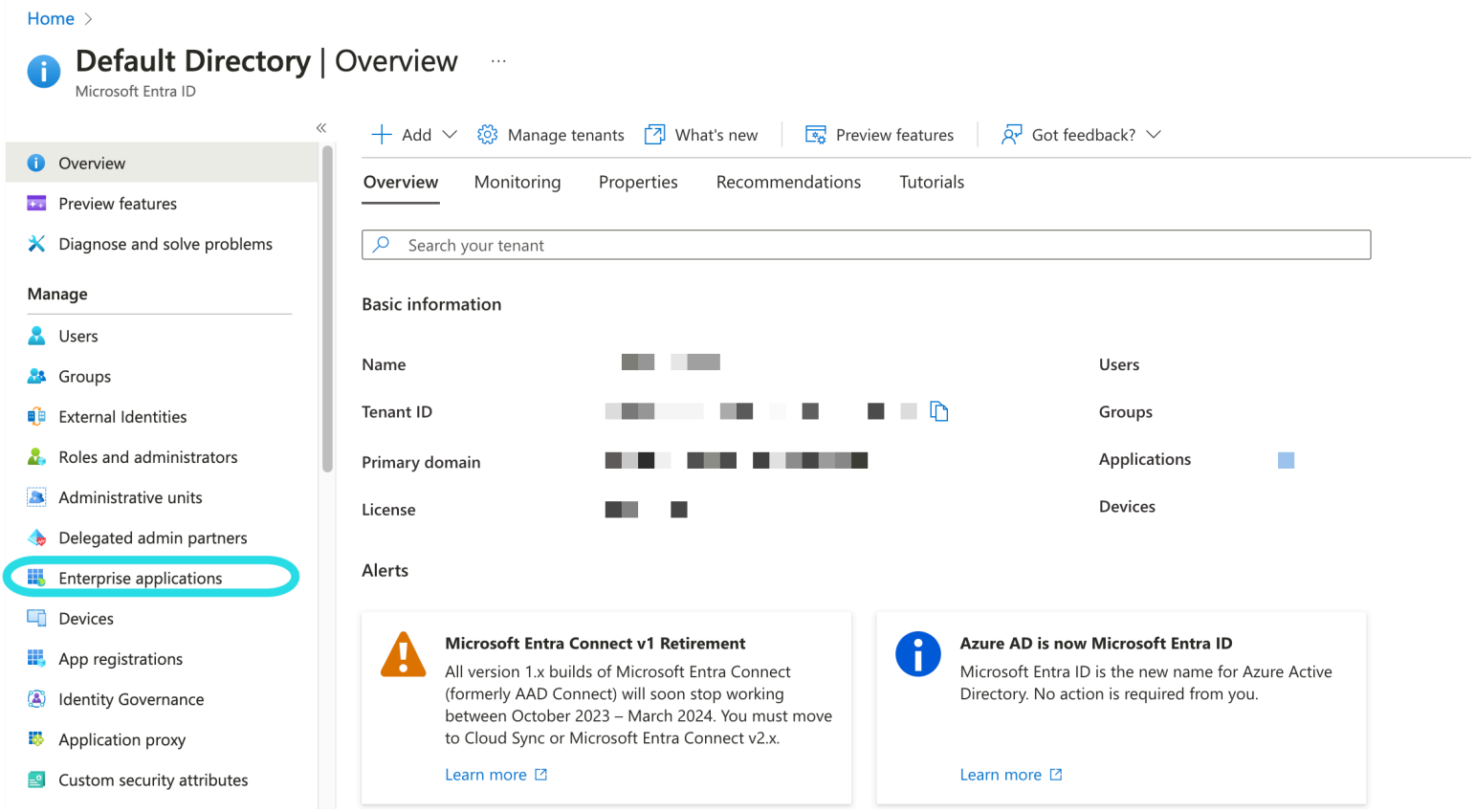
Aprovisionamiento de SCIM

Seleccione la casilla **Habilitar SCIM** y tome nota de su **URL SCIM** y **Clave API SCIM**. Necesitarás usar ambos valores en un paso posterior.

Crea una aplicación de empresa

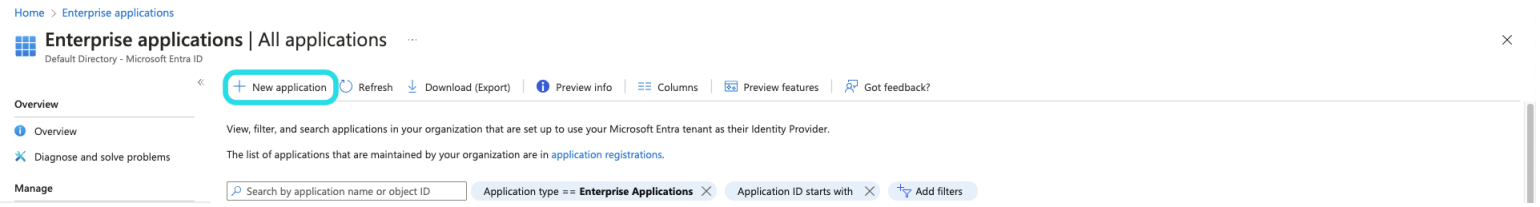
> **Tip**
>
> If you are already using this IdP for Login with SSO, open that existing enterprise application and skip to this step. Otherwise, proceed with this section to create a new application

En el Portal de Azure, navegue a **Microsoft Entra ID** y seleccione **Aplicaciones de Empresa** desde el menú de navegación:



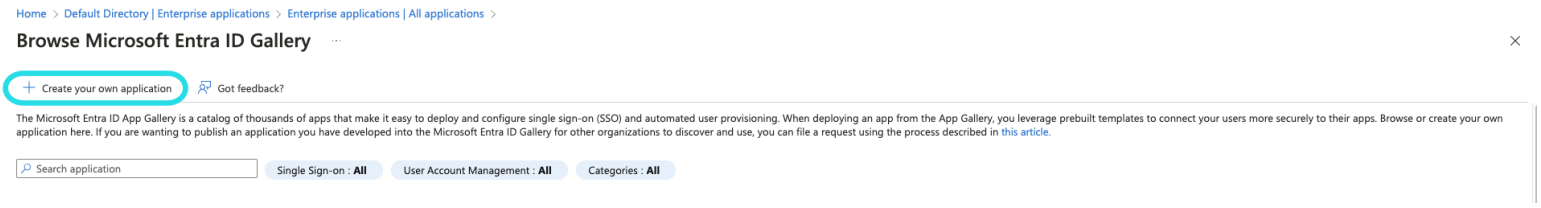
Enterprise applications

Seleccione el botón ＋ **Nueva aplicación**:



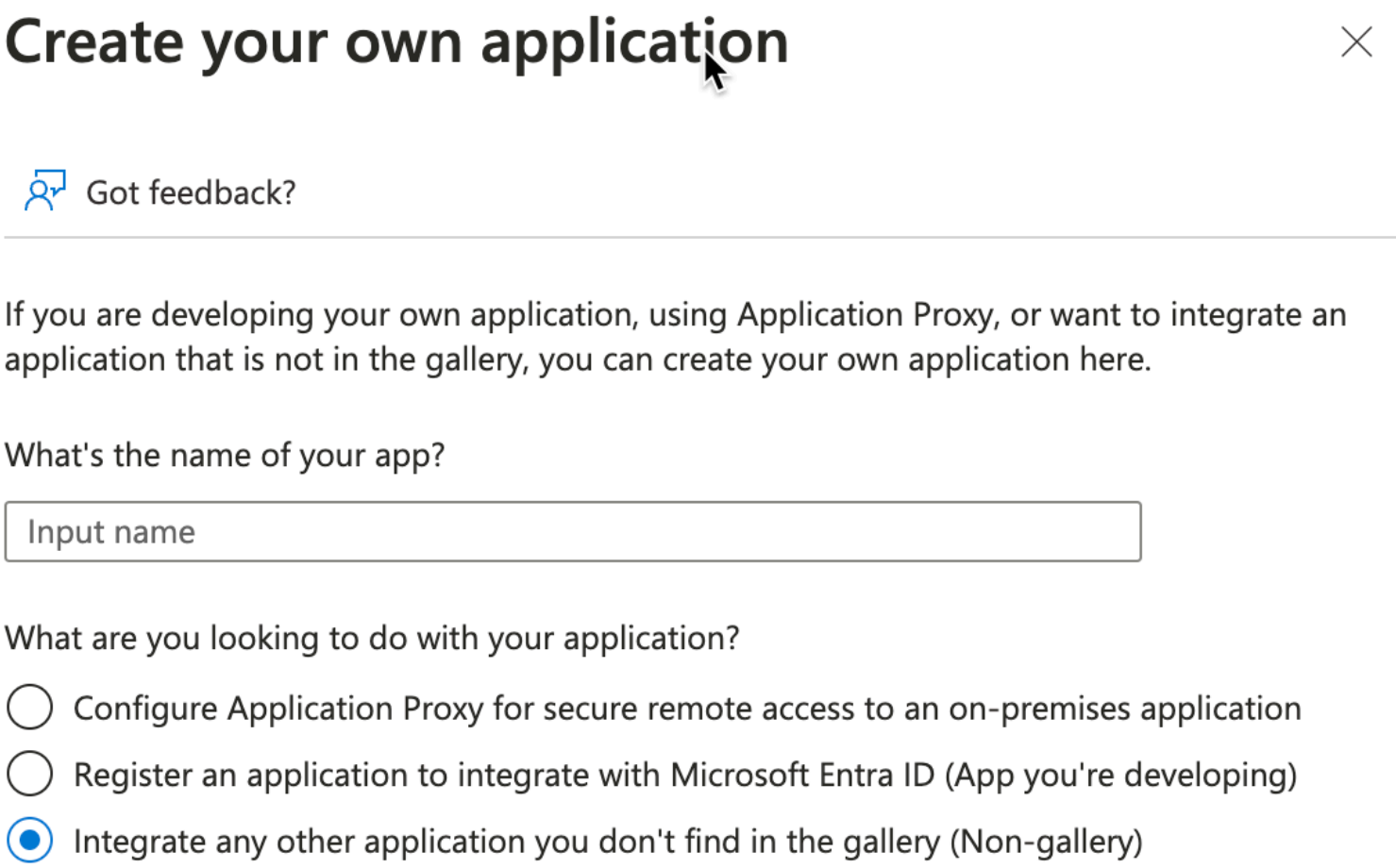
Create new application

En la pantalla de Galería de **Microsoft Entra ID**, selecciona el botón ＋ **Crea tu propia aplicación**:



Create your own application

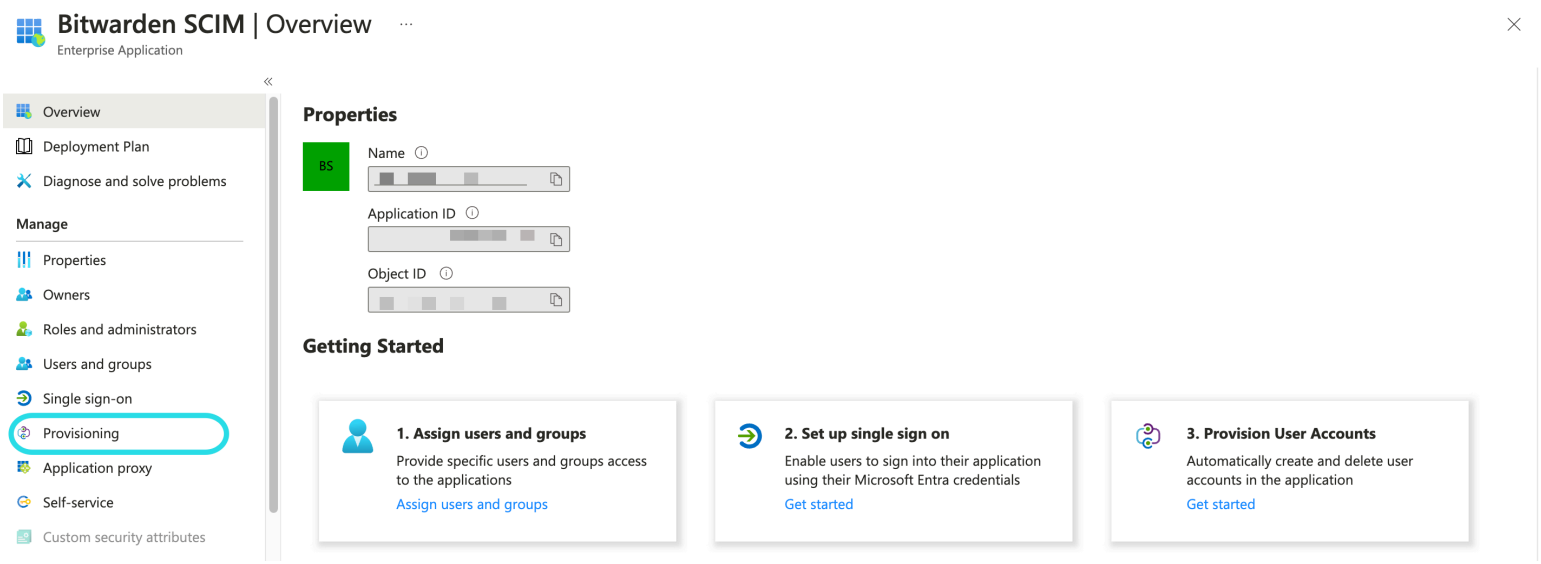
En la pantalla de Crear tu propia aplicación, dale a la aplicación un nombre único y específico de Bitwarden. Elige la opción **No galería** y luego selecciona el botón **Crear**.



Create Entra ID app

Habilitar aprovisionamiento

Seleccione **Aprovisionamiento** desde la navegación y complete los siguientes pasos:



Select Provisioning

1. Seleccione el botón **Comenzar**.
2. Seleccione **Automático** del menú desplegable **Modo de Provisionamiento**.
3. Ingrese su URL de SCIM (aprende más) en el campo de **URL del Inquilino**.
4. Ingrese su clave de API SCIM (aprende más) en el campo **Token Secreto**.
5. Seleccione el botón **Probar Conexión** .
6. Si tu prueba de conexión es exitosa, selecciona el botón **Guardar** .

Mapeos

Bitwarden utiliza nombres de atributos estándar SCIM v2, aunque estos pueden diferir de los nombres de atributos de Microsoft Entra ID. Las asignaciones predeterminadas funcionarán, pero puedes usar esta sección para hacer cambios si lo deseas. Bitwarden utilizará las siguientes propiedades para usuarios y grupos:

Mapeo de usuario

Atributo de Bitwarden	Atributo AAD predeterminado
`activo`	`Switch([IsSoftDeleted], , "Falso", "Verdadero", "Verdadero", "Falso")`
`correos electrónicos` o `nombre de usuario`	`correo` o `nombrePrincipalDeUsuario`

Atributo de Bitwarden	Atributo AAD predeterminado
`nombre para mostrar`	`nombre para mostrar`
`externalId`	`apodoDeCorreo`

- Debido a que SCIM permite que los usuarios tengan múltiples direcciones de correo electrónico expresadas como un conjunto de objetos, Bitwarden utilizará el `valor` del objeto que contiene `"primary": true`.

Mapeo de grupo

Atributo de Bitwarden	Atributo AAD predeterminado
`nombre para mostrar`	`nombre para mostrar`
`miembros`	`miembros`
`externalId`	`identificador de objeto`

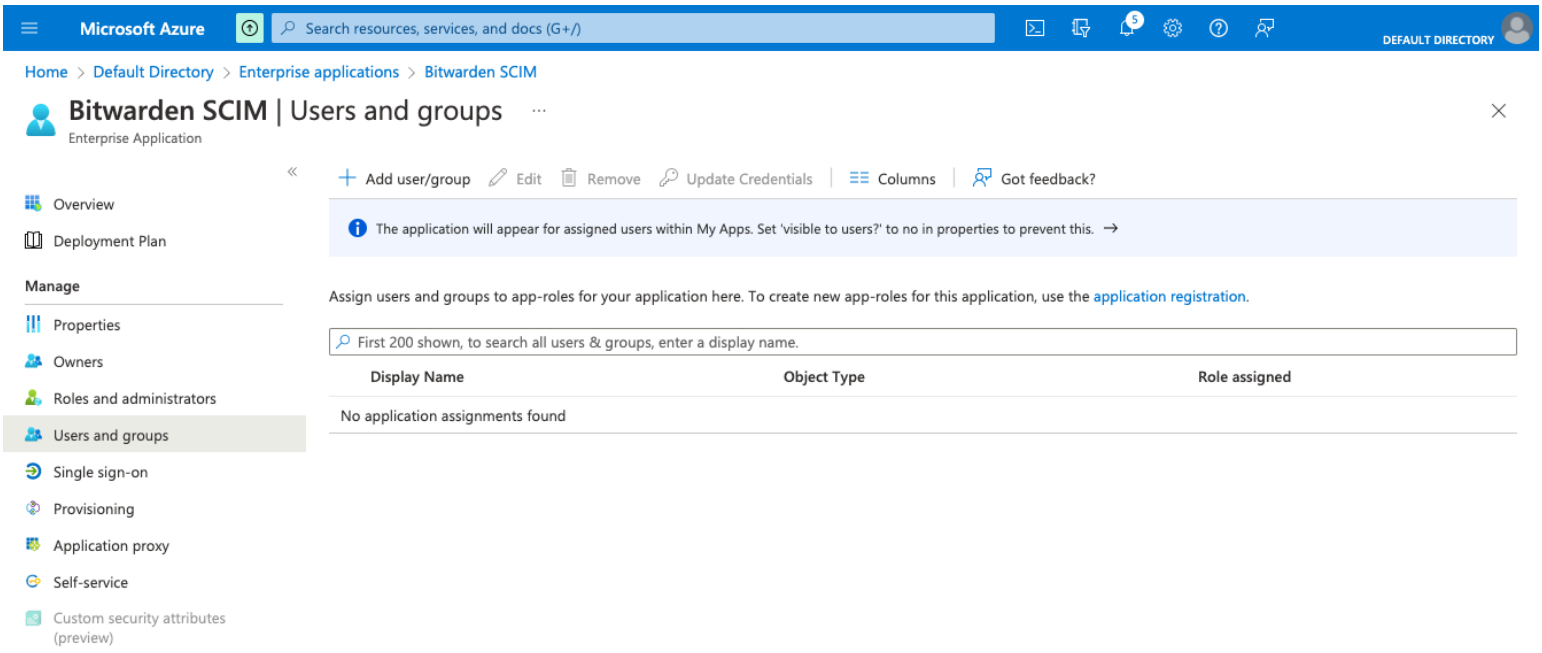
Configuración

Bajo el menú desplegable de **Ajustes** , elige:

- Si se debe enviar una notificación por correo electrónico cuando ocurre un fallo, y si es así, a qué dirección enviarla (recomendado).
- Si **sincronizar solo a los usuarios y grupos asignados** o **sincronizar a todos los usuarios y grupos**. Si eliges la sincronización de todos los usuarios y grupos, omite el siguiente paso.

Asignar usuarios y grupos

Complete este paso si ha seleccionado **sincronizar solo usuarios y grupos asignados** desde los ajustes de aprovisionamiento. Seleccione **Usuarios y grupos** del menú de navegación:



Enterprise application users and groups

Seleccione el botón ＋ **Agregar usuario/grupo** para asignar acceso a la aplicación SCIM en un nivel de usuario o grupo. Las siguientes secciones describen cómo modificar usuarios y grupos en Azure afectará a sus contrapartes en Bitwarden:

Usuarios

- Cuando se asigna un nuevo usuario en Azure, se invita al usuario a su organización Bitwarden.
- Cuando un usuario que ya es miembro de su organización es asignado en Azure, el usuario de Bitwarden se vincula al usuario de Azure a través de su valor de `nombre de usuario`.
  - Los usuarios vinculados de esta manera aún están sujetos a los otros flujos de trabajo en esta lista, sin embargo, valores como `displayName` y `externalId/mailNickname` no se cambian automáticamente en Bitwarden.
- Cuando un usuario asignado es suspendido en Azure, al usuario se le revoca su acceso a la organización.
- Cuando un usuario asignado es eliminado en Azure, el usuario es removido de la organización.
- Cuando se elimina a un usuario asignado de un grupo en Azure, el usuario se elimina de ese grupo en Bitwarden pero sigue siendo un miembro de la organización.

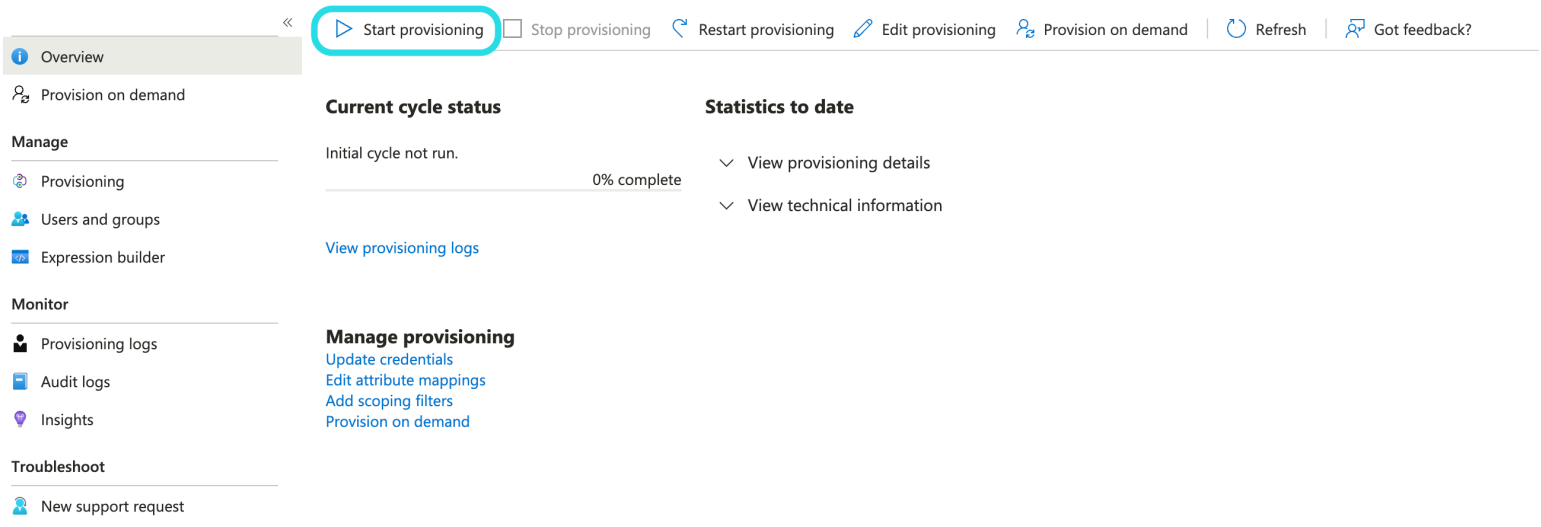
Grupos

- Cuando se asigna un nuevo grupo en Azure, el grupo se crea en Bitwarden.
  - Los miembros del grupo que ya son miembros de tu organización Bitwarden se añaden al grupo.
  - Los miembros del grupo que aún no son miembros de tu organización Bitwarden están invitados a unirse.
- Cuando un grupo que ya existe en tu organización Bitwarden se asigna en Azure, el grupo Bitwarden se vincula a Azure a través de los valores `displayName` y `externalId`/`objectId`.
  - Los grupos vinculados de esta manera tendrán la sincronización de sus miembros desde Azure.

- Cuando un grupo se renombra en Azure, se actualizará en Bitwarden siempre que se haya realizado la sincronización inicial.
    - Cuando un grupo se renombra en Bitwarden, se cambiará de nuevo a como se llama en Azure. Siempre cambia los nombres de grupo del lado de Azure.

Comienza la provisión

Una vez que la aplicación esté completamente configurada, comienza la provisión seleccionando el botón ▷ **Iniciar provisión** en la página de **Provisión** de la aplicación de la empresa:



Start provisioning

Finalizar la incorporación de usuarios

Ahora que sus usuarios han sido provistos, recibirán invitaciones para unirse a la organización. Instruya a sus usuarios para aceptar la invitación y, una vez que lo hayan hecho, confírmelos a la organización.

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