CONSOLA DE ADMINISTRADOR > GESTIÓN DE USUARIOS >

Integración SCIM de OneLogin

Integración SCIM de OneLogin

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.

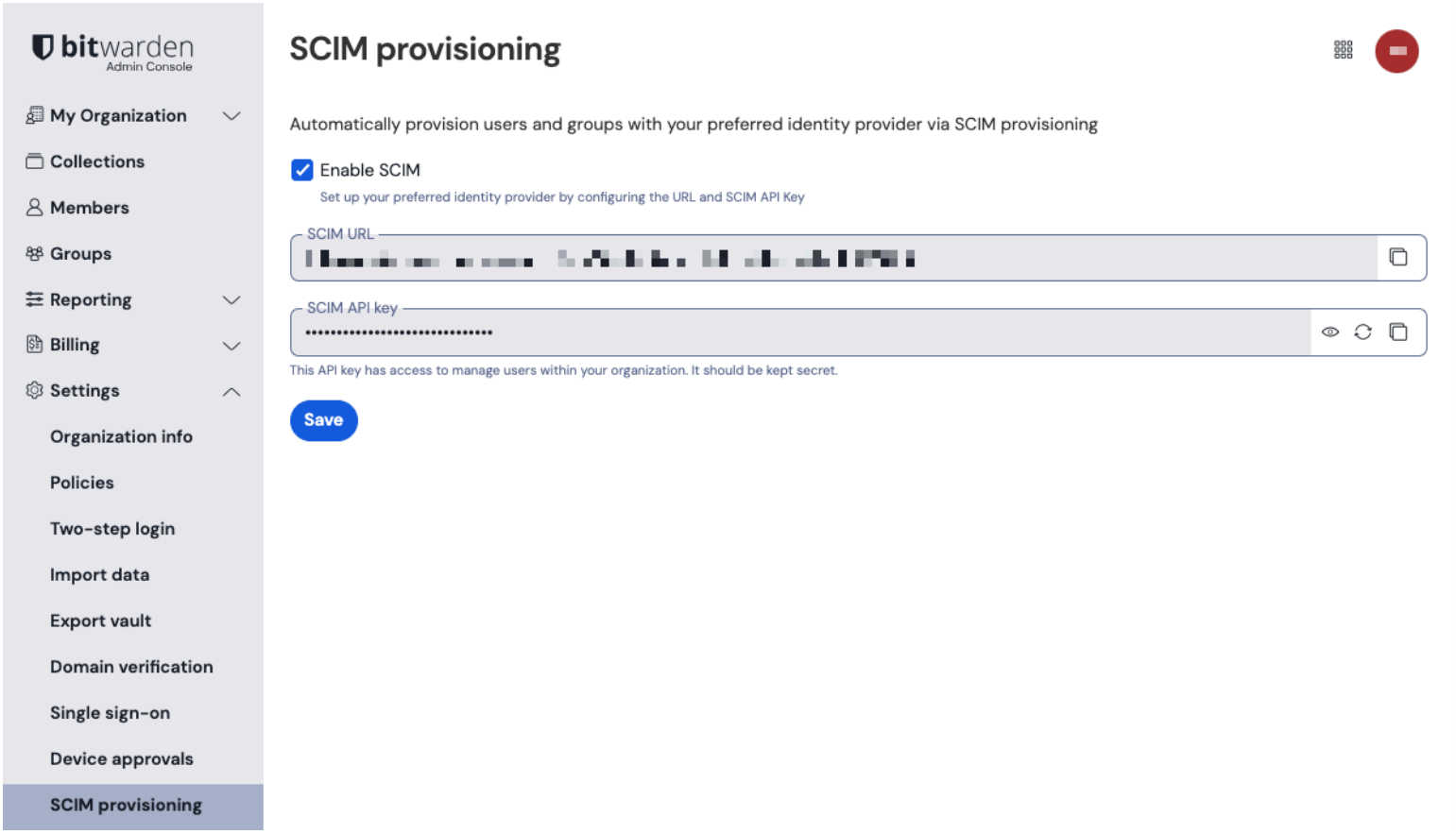
> **Note**
>
> Las integraciones SCIM están disponibles para **organizaciones de Empresa**. Las organizaciones de Equipos, o los clientes que no utilizan un proveedor de identidad compatible con SCIM, pueden considerar el uso de Conector de Directorio como un medio alternativo de aprovisionamiento.

Este artículo te ayudará a configurar una integración SCIM con OneLogin. La configuración implica trabajar simultáneamente con la caja fuerte web de Bitwarden y el Portal de Administrador de OneLogin. 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**:

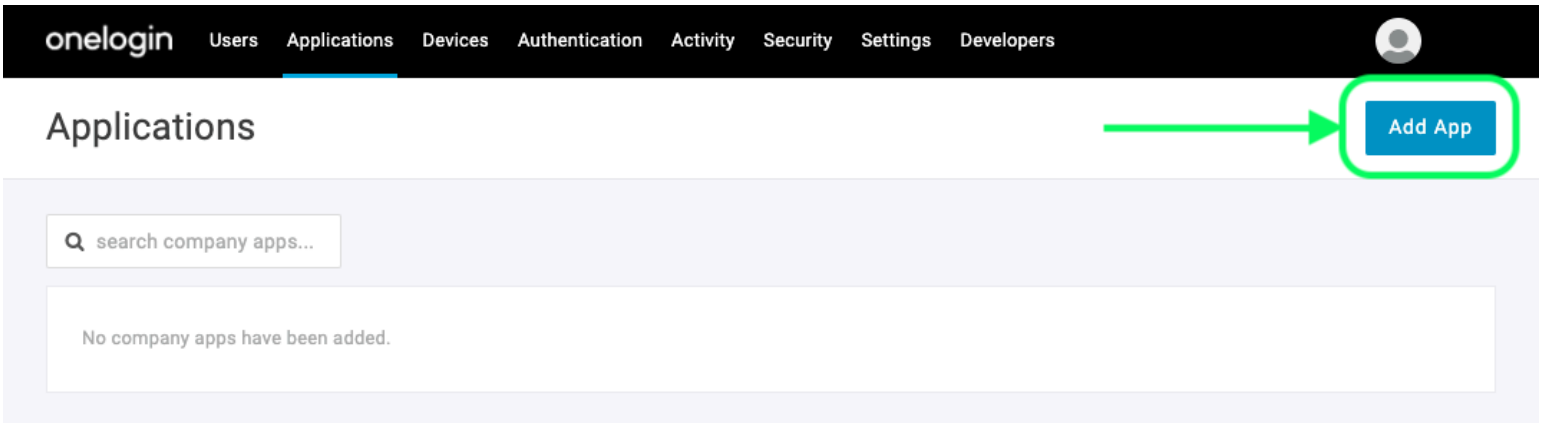


Aprovisionamiento de SCIM

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

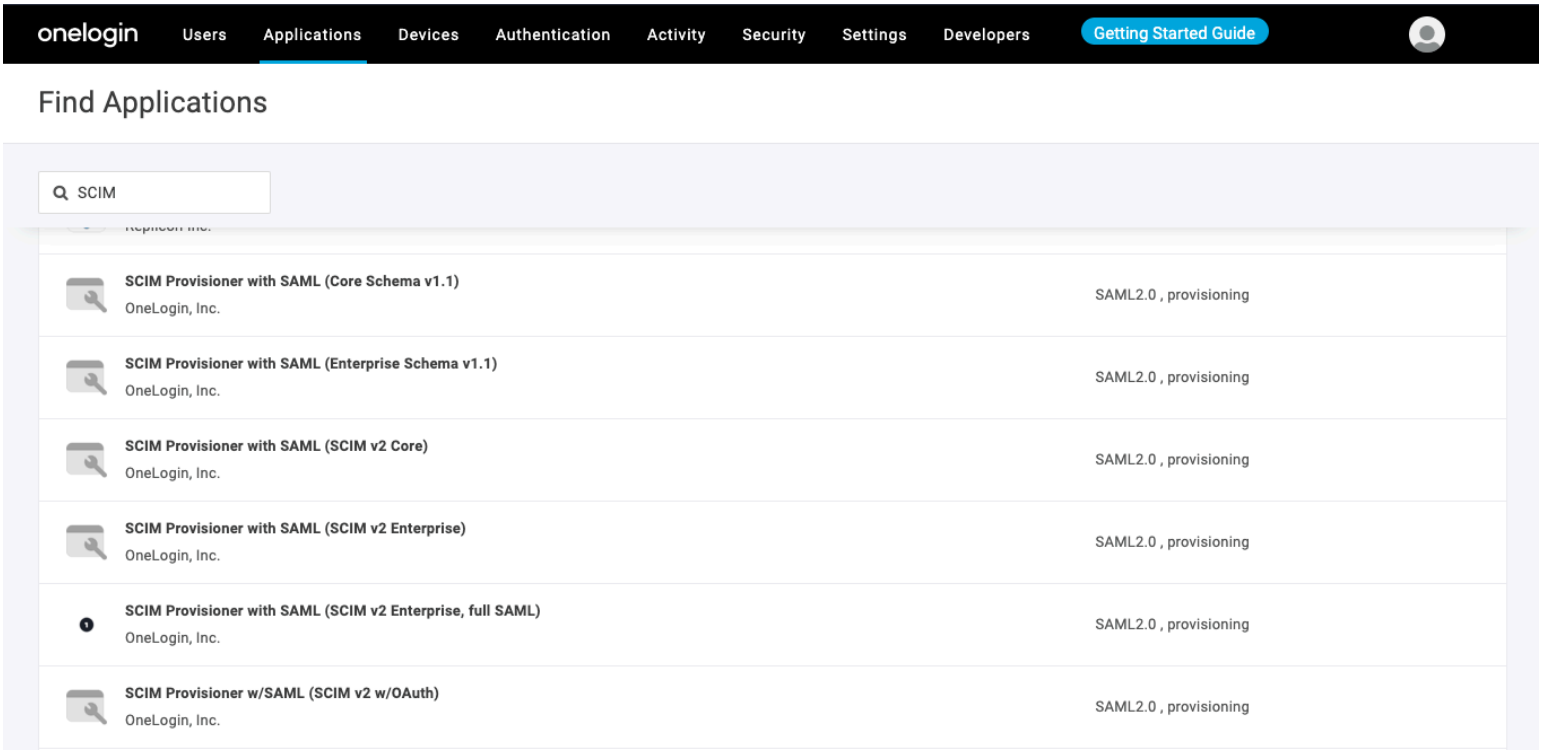
Crea una aplicación OneLogin

En el Portal de OneLogin, navegue a la pantalla de **Aplicaciones** y seleccione el botón de **Agregar App**:



Add an Application

En la barra de buscar, tipo `SCIM` y selecciona la aplicación **Provisionador SCIM con SAML (SCIM v2 Empresa)**:

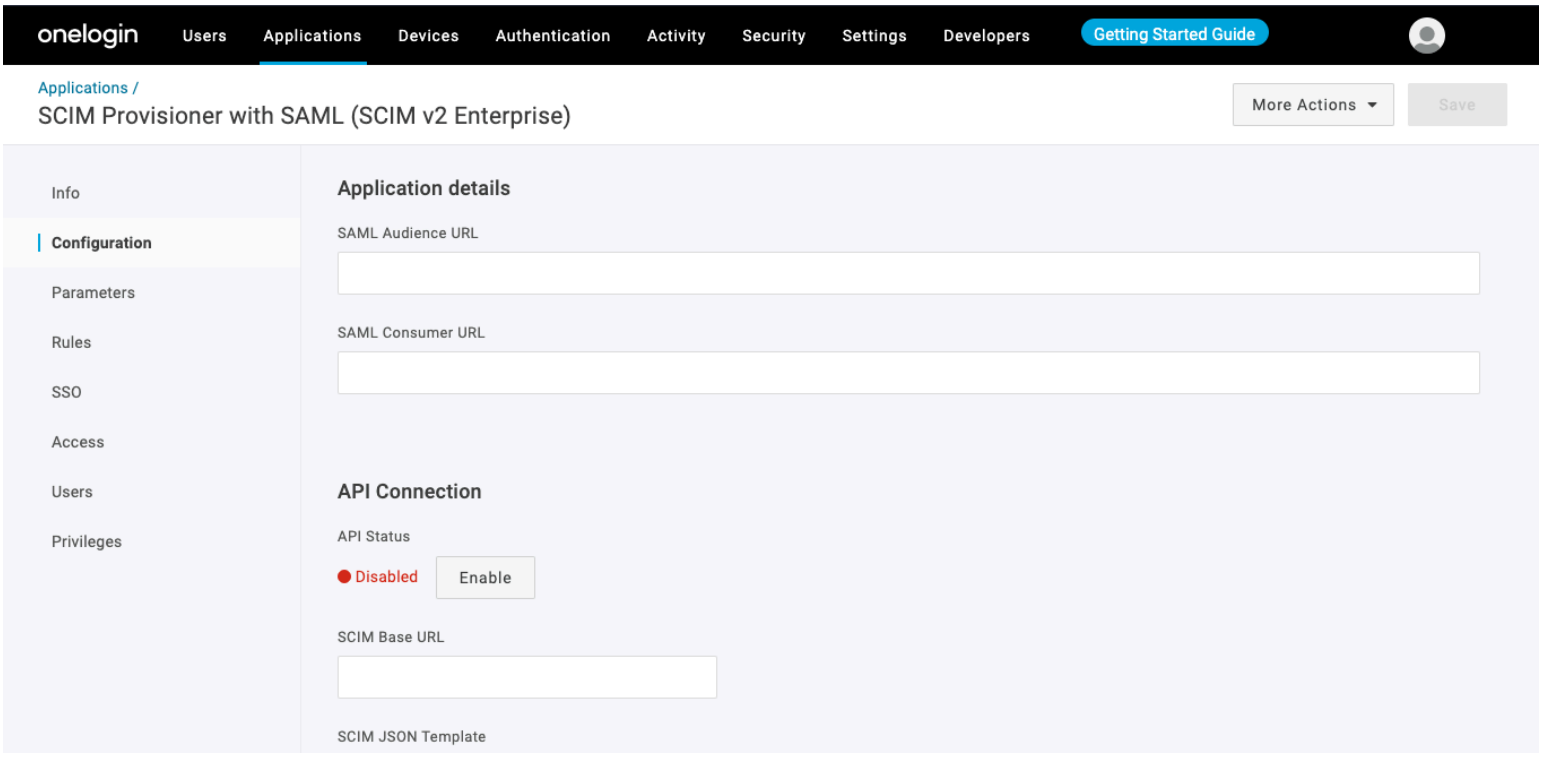


SCIM Provisioner App

Dale a tu aplicación un **Nombre de Visualización** específico de Bitwarden y selecciona el botón de **Guardar**.

Configuración

Seleccione **Configuración** del menú de navegación izquierdo y configure la siguiente información, parte de la cual deberá recuperar de las pantallas de Single Sign-On y SCIM Provisioning en Bitwarden.



SCIM App Configuration

Detalles de la aplicación

OneLogin requerirá que completes los campos de **URL del Público SAML** y **URL del Consumidor SAML** incluso si no vas a utilizar el inicio de sesión único. Aprenda qué ingresar en estos campos .

Conexión API

Ingrese los siguientes valores en la sección **Conexión API**:

Ajuste de aplicación	Descripción
URL base de SCIM	Establezca este campo en la URL de SCIM (aprende más).
Token SCIM portador	Establezca este campo en la clave API de SCIM (aprende más).

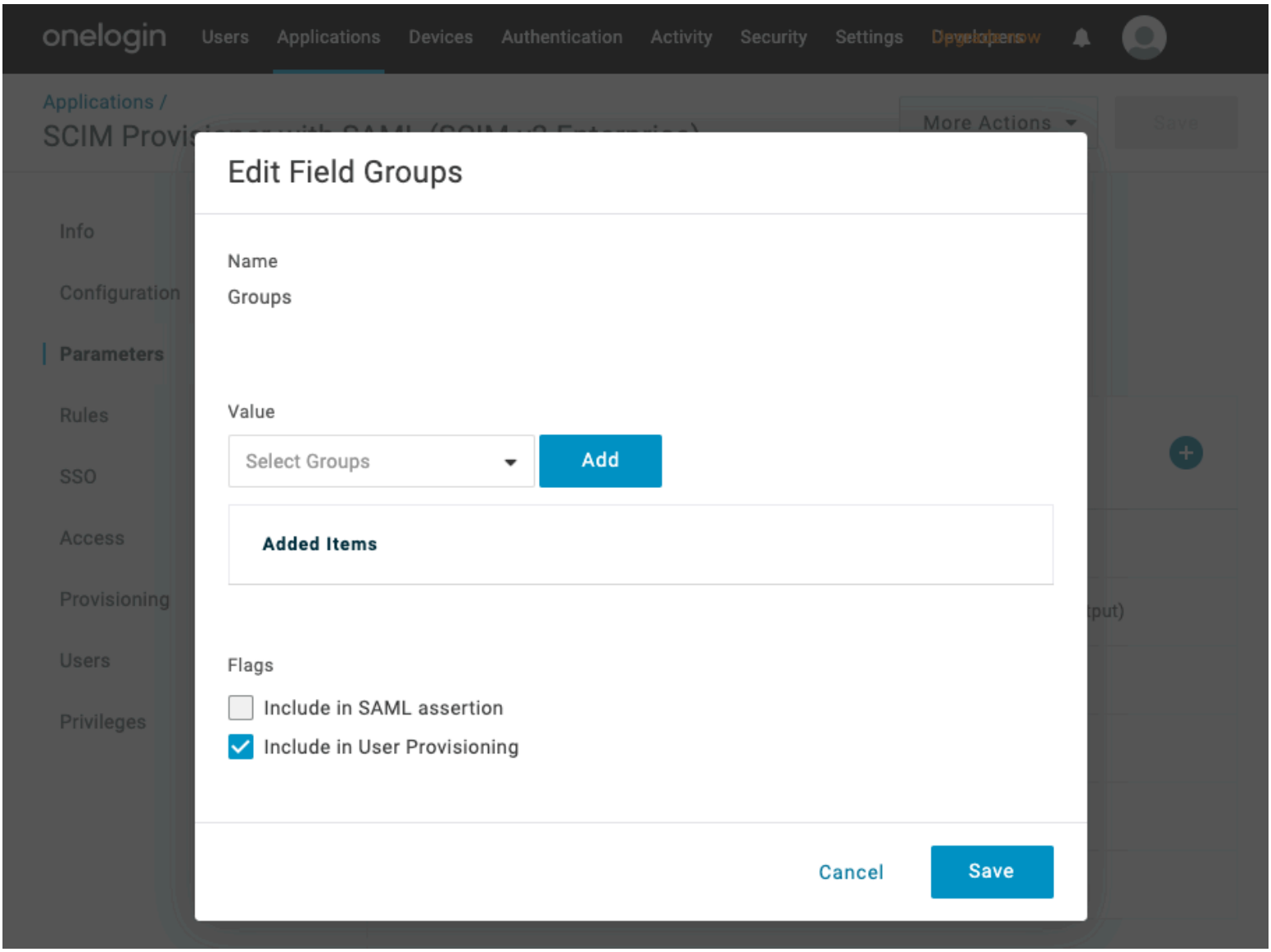
Seleccione **Guardar** una vez que haya configurado estos campos.

Acceso

Seleccione **Acceso** desde la navegación de la mano izquierda. En la sección de **Roles**, asigna el acceso a la aplicación a todos los roles que te gustaría provisionar en Bitwarden. Cada rol se trata como un grupo en su organización Bitwarden, y los usuarios asignados a cualquier rol serán incluidos en cada grupo, incluso si se les asignan múltiples roles.

Parámetros

Seleccione **Parámetros** de la navegación izquierda. Seleccione **Grupos** de la tabla, habilite la casilla **Incluir en la Provision de Usuario** , y seleccione el botón **Guardar** :

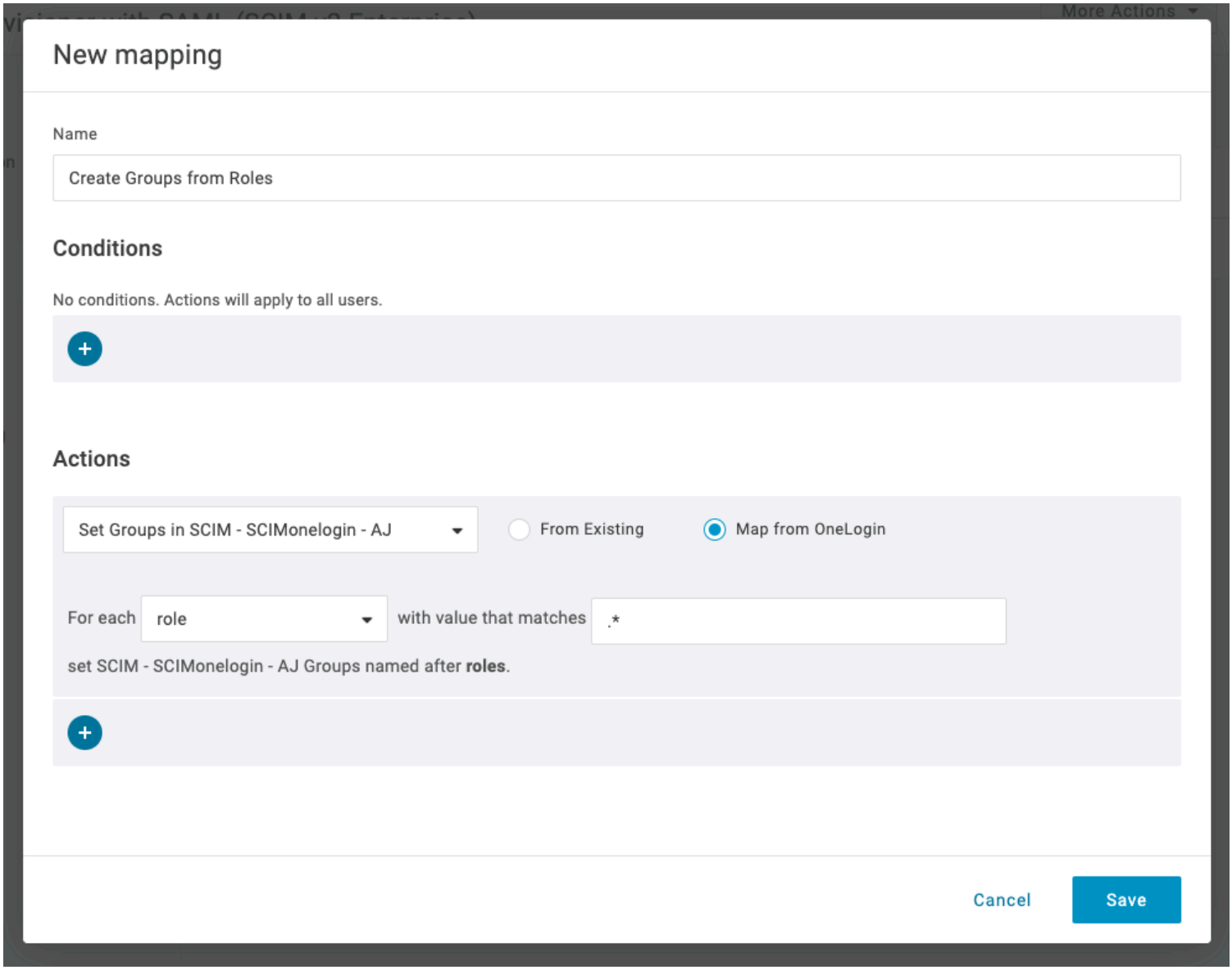


Include Groups in User Provisioning

Reglas

Crea una regla para mapear los roles de OneLogin a los grupos de Bitwarden:

1. Seleccione **Reglas** de la navegación en el lado izquierdo.
2. Seleccione el botón Agregar Regla para abrir el diálogo de **Nueva asignación** :



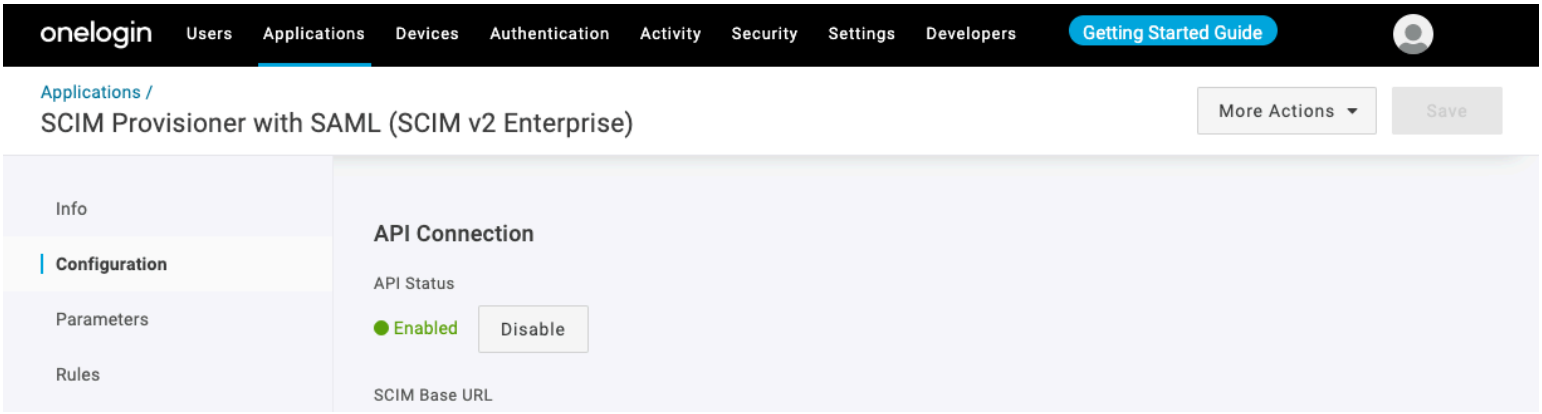
Role/Group Mapping

3. Dale a la regla un **Nombre** como Crear Grupos desde Reglas.
4. Deja **Condiciones** en blanco.
5. En la sección de **Acciones**:
    1. Seleccione **Establecer Grupos en** del primer menú desplegable.
    2. Seleccione la opción **Mapa de OneLogin**.
    3. Seleccione **rol** del menú desplegable "Para cada uno".
    4. Ingrese .* en el campo "con valor que coincide" para asignar todos los roles a grupos, o ingrese un nombre de rol específico.

6. Seleccione el botón **Guardar** para terminar de crear la regla.

Prueba de conexión

Seleccione **Configuración** del menú de navegación izquierdo, y seleccione el botón **Habilitar** debajo de **Estado de API:**

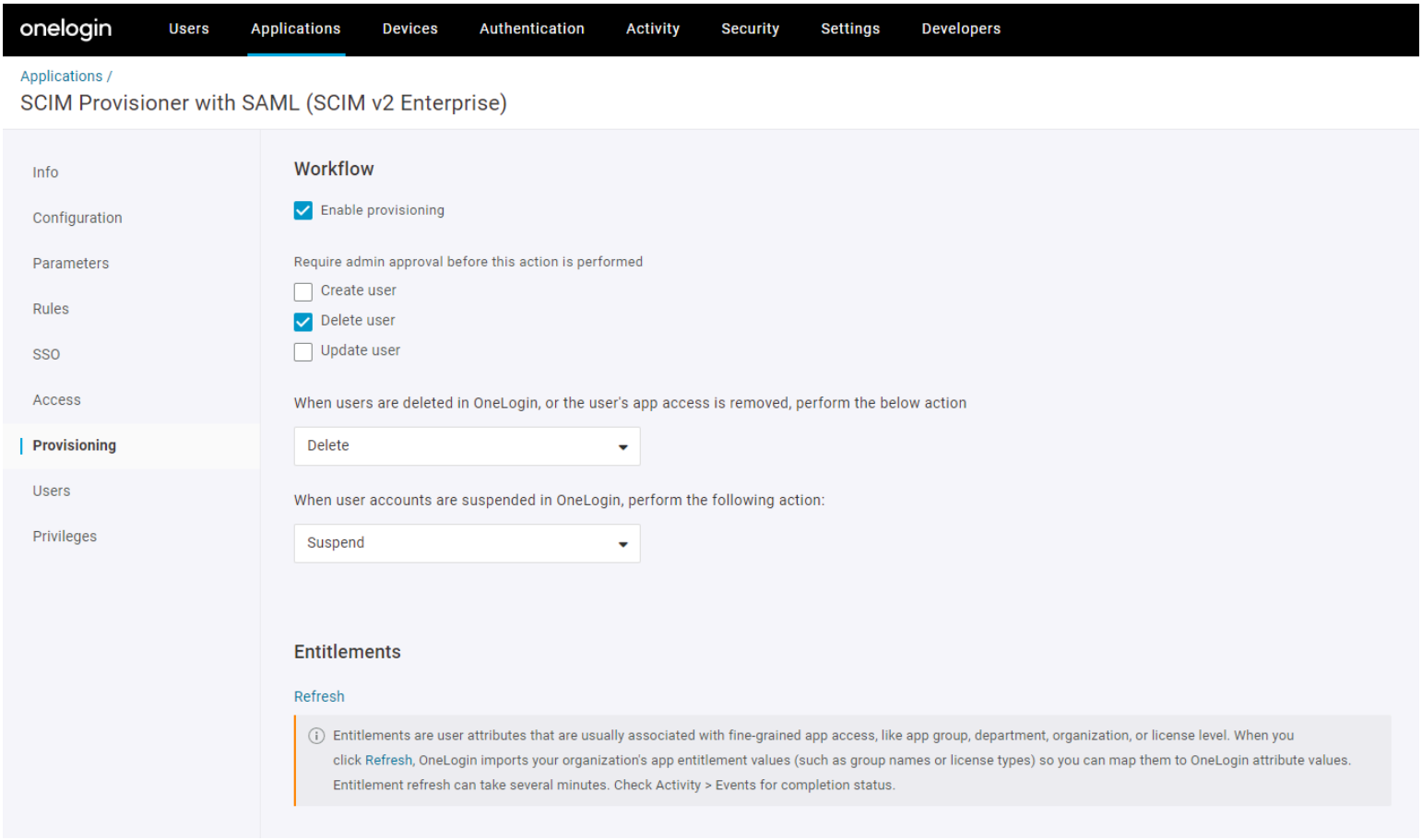


Test API Connection

Esta prueba **no** comenzará a aprovisionar, pero hará una solicitud GET a Bitwarden y mostrará **Habilitado** si la aplicación obtiene una respuesta de Bitwarden con éxito.

Habilitar aprovisionamiento

Seleccione **Aprovisionamiento** del menú de navegación izquierdo:



Provisioning Settings

En esta pantalla:

1. Seleccione la casilla **Habilitar aprovisionamiento**.
2. En el menú desplegable **Cuando los usuarios son eliminados en OneLogin...** , selecciona **Eliminar**.
3. En el menú desplegable **Cuando las cuentas de usuario están suspendidas en OneLogin...**, selecciona **Suspender**.

Cuando hayas terminado, selecciona **Guardar** para activar la provisión.

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.

Apéndice

Atributos del usuario

Tanto Bitwarden como la aplicación de OneLogin **SCIM Provisioner con SAML (SCIM v2 Empresa)** utilizan nombres de atributos estándar SCIM v2. Bitwarden utilizará los siguientes atributos:

- `activo`
- `correos electrónicos` o `nombre de usuario`
- `nombre para mostrar`
- `externalId`

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