CONSOLA DE ADMINISTRADOR > GESTIÓN DE USUARIOS >

Acerca de SCIM

Acerca de SCIM

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

Los servidores de Bitwarden proporcionan un punto final de SCIM que, con una válida Clave API SCIM, aceptará solicitudes de su proveedor de identidad (IdP) para la provisión y desactivación de usuarios y grupos.

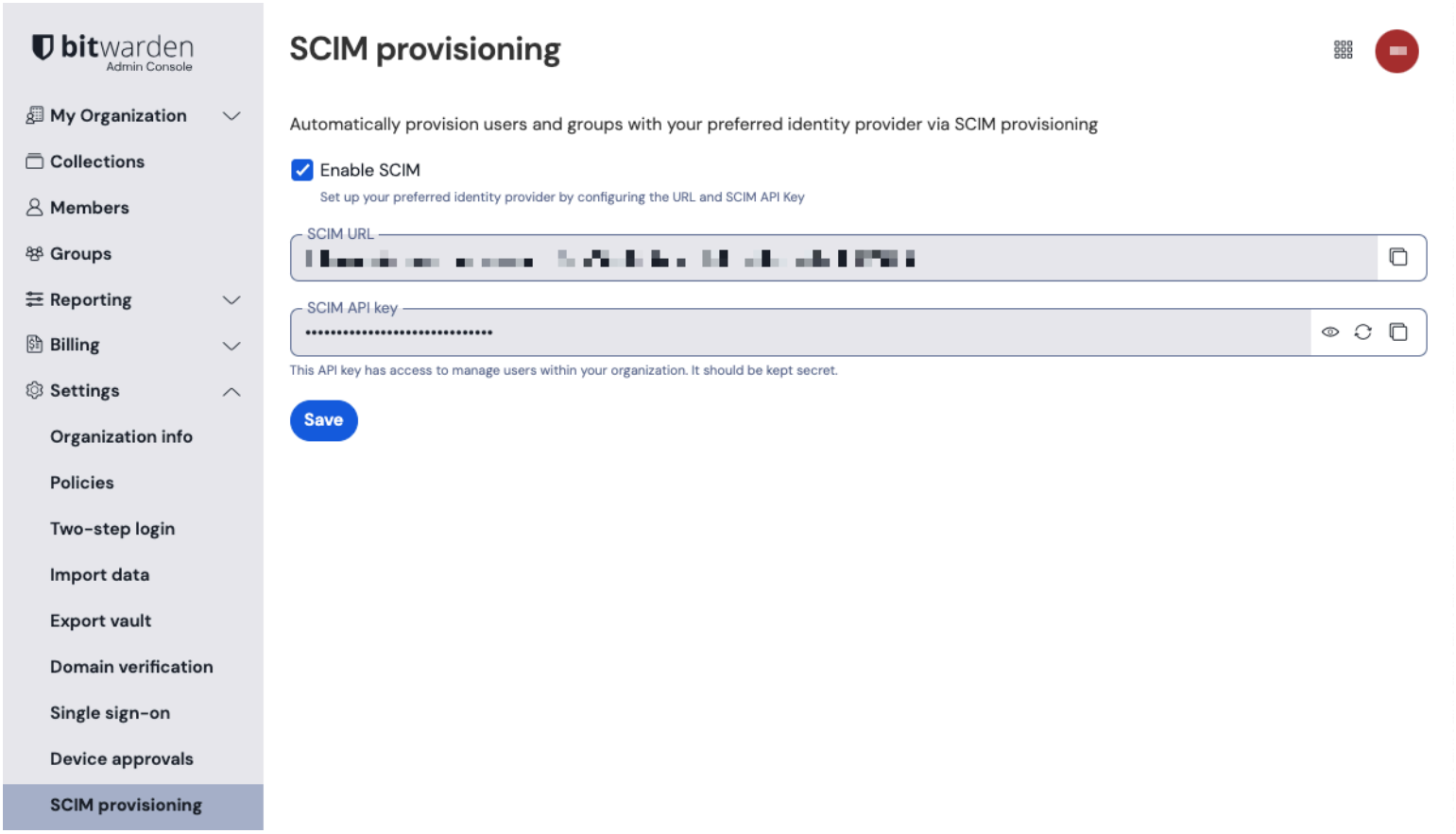
> **Note**
>
> Las integraciones SCIM están disponibles para **organizaciones de Empresa**. Las organizaciones de Equipos, o los clientes que no utilizan un proveedor de identidad compatible con SCIM, pueden considerar el uso de Conector de Directorio como un medio alternativo de aprovisionamiento.

Bitwarden admite SCIM v2 utilizando mapeos de atributos estándar y ofrece integraciones SCIM oficiales para:

- Directorio Activo Azure
- Okta
- OneLogin
- JumpCloud

Configurando SCIM

Para configurar SCIM, tu IdP necesitará una URL SCIM y una clave API para hacer solicitudes autorizadas al servidor de Bitwarden. Estos valores están disponibles desde la Consola de Administrador navegando a **Ajustes** → **Provisión SCIM**:



Aprovisionamiento de SCIM

> **Tip**
>
> Recomendamos usar una de nuestras guías dedicadas para configurar una integración SCIM entre Bitwarden y Azure AD, Okta, OneLogin, o JumpCloud.

Atributos requeridos

Bitwarden utiliza nombres de atributos estándar SCIM v2, enumerados aquí, sin embargo, cada IdP puede usar nombres alternativos que se mapean a Bitwarden durante la provisión.

Atributos del usuario

Para cada usuario, Bitwarden utilizará los siguientes atributos:

- Una indicación de que el usuario está `activo` (**requerido**)
- `correo electrónico`[a] o `nombre de usuario` (**requerido**)
- `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`.

Atributos del grupo

Para cada grupo, Bitwarden utilizará los siguientes atributos:

- `nombreParaMostrar` (**requerido**)
- `miembros`[a]
- `externalId`

[a] – `miembros` es un conjunto de objetos, cada objeto representa a un usuario en ese grupo.

Revocando y restaurando acceso

Una vez que los usuarios son provistos en Bitwarden usando SCIM, puedes revocar temporalmente su acceso a tu organización y a los elementos de su caja fuerte. Cuando un usuario está temporalmente suspendido/desactivado en su IdP, su acceso a su organización será revocado automáticamente.

> **Tip**
>
> Sólo propietarios puede revocar y restaurar el acceso a otros propietarios.

Los usuarios con acceso revocado se enumeran en la pestaña **Revocado** de la pantalla de **Miembros** de la organización y lo harán:

- No tener acceso a ningún elemento de la caja fuerte de la organización, colecciones.
- No tener la capacidad de usar SSO para inicio de sesión, o Duo organizacional para inicio de sesión de dos pasos.
- No estar sujeto a las políticas de su organización.
- No ocupar un asiento de licencia.

> **⚠ Warning**
>
> Para aquellas cuentas que no tienen una contraseña maestra como resultado de SSO con dispositivos de confianza, eliminarlos de su organización o revocar su acceso cortará todo acceso a su cuenta de Bitwarden a menos que:
>
> 1. Les asignas una contraseña maestra usando recuperación de cuenta de antemano.
> 2. El usuario inicia sesión al menos una vez después de la recuperación de la cuenta para completar completamente el flujo de trabajo de recuperación de la cuenta.

Aprende más sobre revocar y restaurar el acceso.

Eventos SCIM

Su organización capturará registros de eventos para las acciones realizadas por las integraciones SCIM, incluyendo invitar a usuarios y eliminar usuarios, así como crear o eliminar grupos. Los eventos derivados de SCIM registrarán `SCIM` en la columna de **Miembro**.

Usuarios preexistentes y grupos

Las organizaciones con usuarios y grupos que se incorporaron antes de activar SCIM, ya sea manualmente o utilizando el Conector de Directorio, deben tomar nota de lo siguiente:

	...que existe en el IdP.	...eso no existe en el IdP.
Usuario preexistente	•No será duplicado •No será obligado a unirse de nuevo a la organización. •No será eliminado de los grupos de los que ya es miembro.	•No será eliminado de la organización •No se agregarán ni se eliminarán membresías de grupo
Grupo preexistente	•No será duplicado •Tendrá miembros agregados de acuerdo con el IdP •No se eliminarán miembros preexistentes	•No será eliminado de la organización •No se agregarán ni se eliminarán miembros

ⓘ Note

If you are using Directory Connector, make sure to turn syncing off before activating SCIM.