

CONSOLA DE ADMINISTRADOR > GESTIÓN DE USUARIOS >

Integración de Okta SCIM

Ver en el centro de ayuda:
<https://bitwarden.com/help/okta-scim-integration/>

Integración de Okta SCIM

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 Okta. La configuración implica trabajar simultáneamente con la caja fuerte web de Bitwarden y el Portal de Administrador de Okta. A medida que avanza, recomendamos tener ambos fácilmente disponibles y completar los pasos en el orden en que están documentados.

Funcionalidades soportadas

Las siguientes funcionalidades de aprovisionamiento son compatibles con esta integración:

- **Usuarios de Push:** Los usuarios en Okta que están asignados a Bitwarden se agregan como usuarios en Bitwarden.
- **Desactivar Usuarios:** Cuando los usuarios se desactivan en Okta, también se desactivarán en Bitwarden.
- **Grupos de Empuje:** Los grupos y sus usuarios en Okta pueden ser empujados a Bitwarden.

Note

Please note, Bitwarden does not support changing a user's email address once provisioned. Bitwarden also does not support changing a user's email address type, or using a type other than **primary**. The values entered for email and username should be the same. [Learn more](#).

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**:

The screenshot shows the Bitwarden Admin Console interface for SCIM provisioning. On the left is a sidebar with navigation options: My Organization, Collections, Members, Groups, Reporting, Billing, and Settings. The Settings menu is expanded to show options like Organization info, Policies, Two-step login, Import data, Export vault, Domain verification, Single sign-on, Device approvals, and SCIM provisioning (which is highlighted). The main content area is titled 'SCIM provisioning' and includes a sub-header 'Automatically provision users and groups with your preferred identity provider via SCIM provisioning'. There is a checked checkbox for 'Enable SCIM' with a note to 'Set up your preferred identity provider by configuring the URL and SCIM API Key'. Below this are two input fields: 'SCIM URL' containing a masked URL and 'SCIM API key' containing a masked key. A warning note states: 'This API key has access to manage users within your organization. It should be kept secret.' A blue 'Save' button is located at the bottom left of the form area.

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.

Agrega la aplicación Bitwarden

En el Portal de Administrador de Okta, selecciona **Aplicaciones** → **Aplicaciones** desde la navegación. En la pantalla de la aplicación, seleccione el botón **Explorar Catálogo de Aplicaciones** :

Applications

[Help](#)[Create App Integration](#)[Browse App Catalog](#)[Assign Users to App](#)[More ▾](#)

STATUS

ACTIVE 0

INACTIVE 0



Okta Admin Console



Okta Browser Plugin



Okta Dashboard

[Browse App Catalog](#)

En la barra de buscar, ingrese **Bitwarden** y seleccione **Bitwarden**:

Browse App Integration Catalog

[Create New App](#)

Use Case

All Integrations 7453

Apps for Good 8

Automation 23

Centralized Logging 11

Directory and HR Sync 14

Bot or Fraud Detection 2

Identity Proofing 7

Identity Governance and Administration (IGA) 5

Lifecycle Management 534

Multi-factor Authentication 22

POPULAR SEARCHES : [Bookmark App](#) [SCIM 2.0 Test App](#) [Okta Org2Org](#) [Template App](#)



Rearden Commerce
SAML, SWA



FSRS gov Awardees
SWA



Aquacrmsoftware
SWA



FORWARD
SWA



Awardco
SAML



Bitwarden

[See All Results →](#)

[Workflow Connectors](#) [SCIM](#) [SAML](#) [SWA](#) [SCIM](#)

[Bitwarden Okta App](#)

Seleccione el botón **Agregar Integración** para proceder a la configuración.

Ajustes generales

En la pestaña de **Ajustes Generales**, dale a la aplicación una etiqueta única, específica de Bitwarden. Marque las opciones **No mostrar el ícono de la aplicación a los usuarios** y **No mostrar el ícono de la aplicación en la aplicación móvil Okta** y seleccione **Hecho**.

Configuración de aprovisionamiento

Ajustes de aprovisionamiento

Abra la pestaña **Provisioning** y seleccione el botón **Configurar Integración API**.

Una vez seleccionado, Okta enumerará algunas opciones para que configures:

The screenshot shows the Bitwarden integration configuration interface. At the top, there's a header for 'Bitwarden' with an 'Active' dropdown, two user icons, and links for 'View Logs' and 'Monitor Imports'. Below this is a navigation bar with tabs: 'General', 'Provisioning' (selected), 'Import', 'Assignments', and 'Push Groups'. On the left, a 'Settings' sidebar has 'Integration' selected. The main content area features an information box with the title 'Bitwarden: Configuration Guide', 'Provisioning Certification: Okta Verified', and a note that the integration is partner-built by Bitwarden, with a link to contact partner support. Below this is a checkbox labeled 'Enable API integration' which is checked. A text prompt asks to enter Bitwarden credentials. There are two input fields: 'Base URL' with the value 'https://scim.bitwarden.com/v2/6f012726-bff2-455b-a4ab-ac6eC' and 'API Token' which is masked with dots. A 'Test API Credentials' button is positioned below the API Token field. At the bottom right, there is a 'Save' button.

Configure API Integration

1. Marca la casilla **Habilitar Integración de API**.

2. En el campo **URL base**, ingrese su URL SCIM, que se puede encontrar en la pantalla de aprovisionamiento SCIM ([aprende más](#)).
3. En el campo **Token de API**, ingrese su clave de API SCIM ([aprende más](#)).

Una vez que haya terminado, use el botón **Probar Credenciales de API** para probar su configuración. Si pasa la prueba, seleccione el botón **Guardar**.

Establecer acciones de aprovisionamiento

En la pantalla de **Aprovisionamiento** → **A la aplicación**, seleccione el botón de **Editar** :

The screenshot shows the Bitwarden SCIM interface. At the top, there's a header for "Bitwarden SCIM" with an "Active" dropdown, two user icons, and links for "View Logs" and "Monitor Imports". Below this is a navigation bar with tabs: "General", "Mobile", "Provisioning" (selected), "Import", "Assignments", and "Push Groups". On the left, a sidebar menu includes "Settings", "To App" (selected), "To Okta", and "Integration". The main content area shows a diagram of "okta" pointing to the Bitwarden logo. Below the diagram, there are three sections: "Provisioning to App" with a "Cancel" button; "Create Users" with a checked "Enable" checkbox and a description: "Creates or links a user in Bitwarden when assigning the app to a user in Okta. The default username used to create accounts is set to Okta username."; and "Deactivate Users" with a checked "Enable" checkbox and a description: "Deactivates a user's Bitwarden account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta." At the bottom right of the main content area is a blue "Save" button.

Provisioning To App

Habilite, como mínimo, **Crear Usuarios** y **Desactivar Usuarios**. Seleccione **Guardar** cuando haya terminado.

Tareas

Abre la pestaña **Asignaciones** y usa el menú desplegable **Asignar** para asignar personas o grupos a la aplicación. Los usuarios y grupos asignados recibirán automáticamente una invitación. Dependiendo de tu flujo de trabajo, es posible que necesites usar la pestaña **Push Groups** para activar la provisión de grupo una vez que se asignan.

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.