RESOURCE CENTER

Bitwarden and the System for Cross-domain Identity Management (SCIM)

How SCIM is implemented in Bitwarden and frequently asked questions

Get the full interactive view at https://bitwarden.com/resources/bitwarden-and-the-system-for-cross-domain-identity-management-scim/

bitwarden

What is SCIM?

System for Cross-domain Identity Management (SCIM) is an industry open standard protocol that enables the automation of management and exchange of user identity information across IT systems or domains. SCIM utilizes a RESTful API, another standard, to run operations and commands on the database.

This makes it easy for IT administrators to provision and manage users for their IT systems, including any SaaS products, internal tools, and more. Rather than having to manually create an account for a new employee for all the different services their company uses, the IT admin would add the new user to their Identity Management system, which will use SCIM to automatically create the accounts for them.

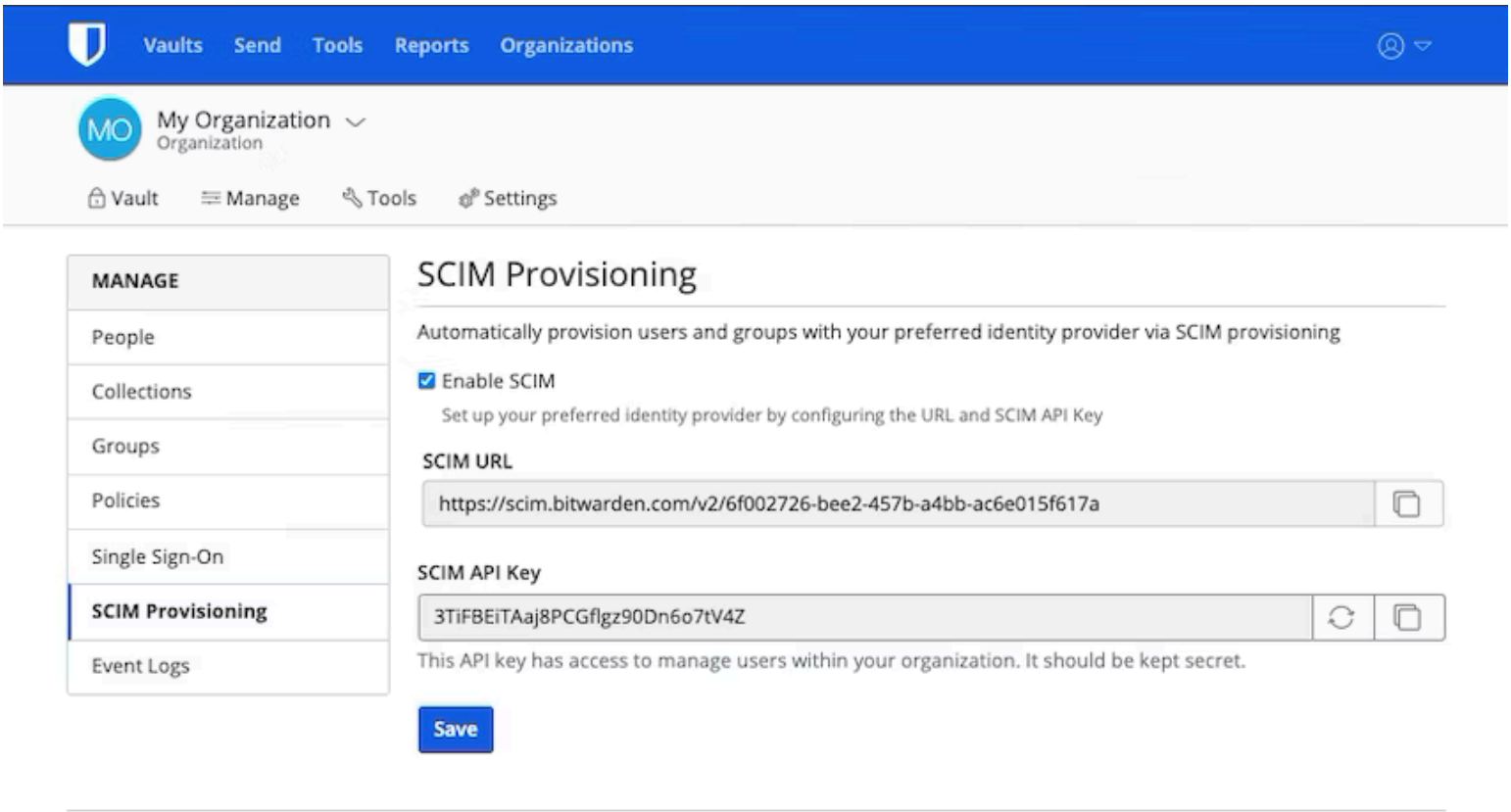
Importantly, it works in reverse when a user leaves the company it closes the accounts for that worker, reducing security risks from their departure.

Finally, SCIM can also be used to assign users to specific groups so they may be provisioned for specific tools. For example, someone joining the Human Resources team could automatically have accounts created in their SaaS Human Resources portal (e.g. any human resources tool) with the permissions needed to manage employee details.

Table of Contents

How Bitwarden implements SCIM

Bitwarden servers provide a SCIM endpoint that, with a valid SCIM API Key, will accept requests from your Identity Provider (IdP) for user and group provisioning and directory synchronization. You will input the API Key and SCIM URL provided by your Bitwarden client into your IdP installation to enable Identity Provider → Bitwarden communication. Documentation for each supported service can be found in the Help Center: Azure Active Directory; Okta; OneLogin; JumpCloud



The SCIM Provisioning page shows your SCIM URL and API key

SCIM and Single Sign-On

Using both SCIM and SSO together at your enterprise significantly eases credential management and automation while reducing overhead. They complement each other quite well. Using SSO will automate access to internal tools, including Bitwarden, while Bitwarden provides easy access to tools outside of SSO purview. With SCIM provisioning, an administrator can, with one action, provide or revoke access to all tools, including those which are not supported by either SSO or SCIM, with Bitwarden acting as an extension of those functions and gating those websites and tools.

SCIM and the Bitwarden Directory Connector

Both SCIM and the Bitwarden Directory Connector offer methods for automating the provisioning of users for a Bitwarden organization. Either solution will successfully create user accounts and permissions based on the directory.

The Bitwarden Directory Connector is a standalone application that is used to actively sync users and groups to a Bitwarden Organization from an existing directory service in a single operation. It will inquire and then automatically provision users, groups, and group associations from the source directory and close accounts for removed users. Further updates would require running the sync operation again. It also works with on-premises Identity Provider solutions.

SCIM enables Bitwarden to receive updates from the Directory or Identity Provider at any time, such as new users and modifications to groups. It will automatically provision or modify users when the Directory or Identity Provider pushes a change.

Solution	How it's run	Sync type	Sync Schedule	Partners and Compatibility
SCIM	Integrated into Bitwarden	Pushes changes to Bitwarden	Always-on	Azure AD, Okta, OneLogin, JumpCloud, Ping Identity
Bitwarden Directory Connector	Standalone on a local machine	Queries directory and pulls changes	Sync intervals are customizable	Active Directory, Azure AS, Okta, OneLogin, Google Workspace, and LDAP-based directory, self-hosted IdPs

SCIM support is available in Enterprise plans. The Bitwarden Directory Connector is available to both Teams and Enterprise plans.

FAQ:

Q: Is SCIM the same as SSO?

A: No. SSO uses the identity providers' information to authenticate logging in, whereas SCIM allows specifically for user provision and management.

Q: Can I switch from using the Bitwarden Directory Connector to SCIM?

A: Yes, with awareness of the following items:

- You should use SCIM integration with the same directory that the Directory Connector was using
- Any users or groups that are in your directory but not provisioned in Bitwarden will be provisioned
- Any user or group that already existed in Bitwarden and is not in your directory will remain.
- At this time SCIM is only able to revoke user access. The ability to remove users completely from an Organization will be added in a future release.
- Be sure that you turn off any scripts you might have created that would automate running Directory Connector.

More tools to aid in migration are in development. Additional documentation can be found in this Help Center article.

Q: Does this work for Cloud and Self-host installations?

A: Yes, SCIM is available to both types of Enterprise installations.

Q: How do I get started with SCIM?

A: Step by step documentation is available in this Help Center article.

Q: Which Identity Providers does Bitwarden support with SCIM?

A: Azure AD, Okta, OneLogin, JumpCloud, and Ping Identity are fully supported.