bitwarden | Help Center Article

ADMIN CONSOLE > USER MANAGEMENT >

About SCIM

View in the help center:
https://bitwarden.com/help/about-scim/

About SCIM

System for cross-domain identity management (SCIM) can be used to automatically provision members and groups in your Bitwarden organization.

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 de-provisioning.

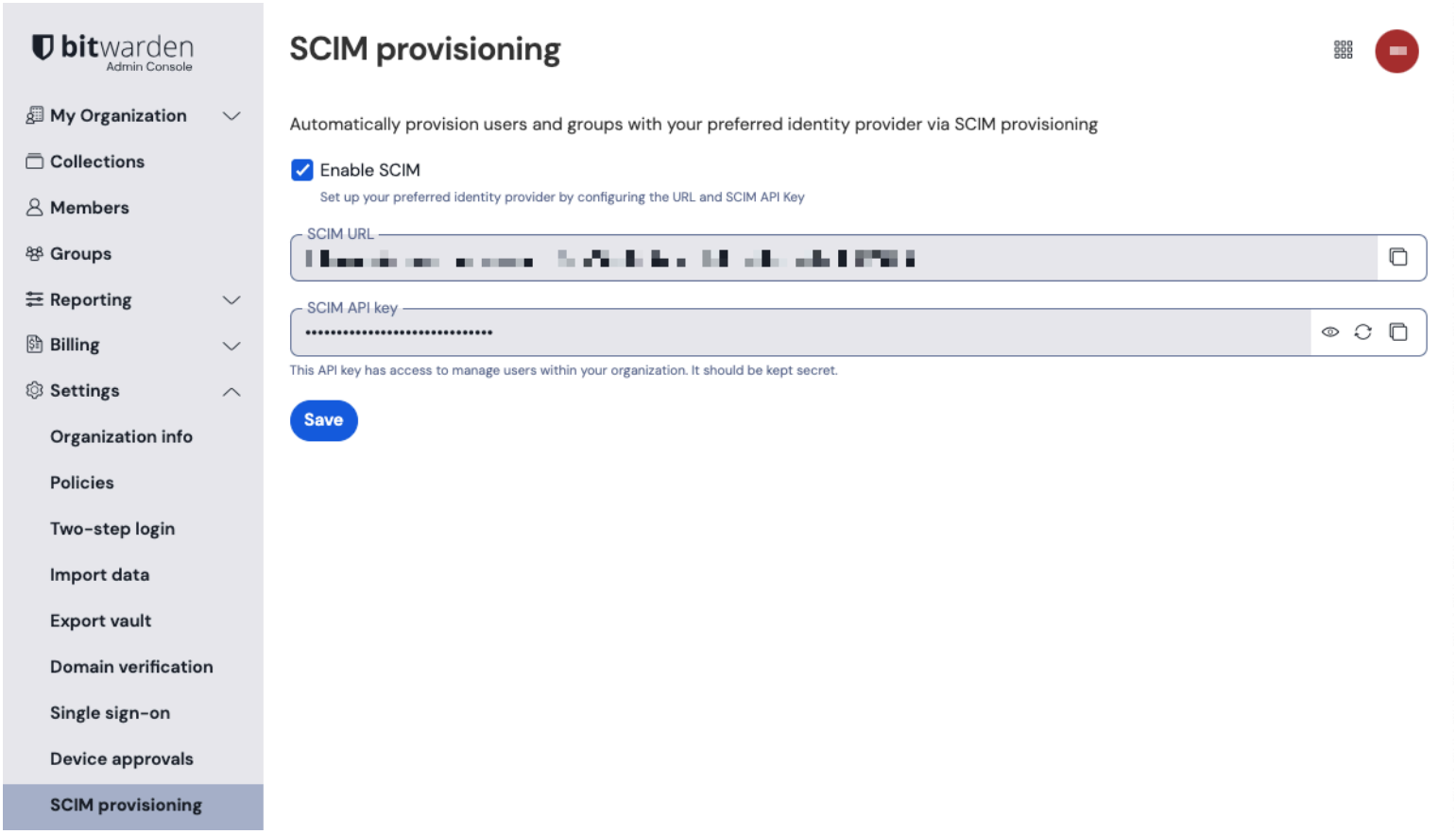
> **Note**
>
> SCIM Integrations are available for **Teams and Enterprise organizations**. Customers not using a SCIM-compatible identity provider may consider using Directory Connector as an alternative means of provisioning.

Bitwarden supports SCIM v2 using standard attribute mappings and offers official SCIM integrations for:

- Azure Active Directory
- Okta
- OneLogin
- JumpCloud
- Ping Identity

Setting up SCIM

To set up SCIM, your IdP will need a SCIM URL and API key to make authorized requests to the Bitwarden server. These values are available from the Admin Console by navigating to **Settings** → **SCIM provisioning**:



SCIM provisioning

> **Tip**
>
> We recommend using one of our dedicated guides for setting up a SCIM integration between Bitwarden and Azure AD, Okta, OneLogin, or JumpCloud.

Required attributes

Bitwarden uses standard SCIM v2 attribute names, listed here, however each IdP may use alternate names which are mapped to Bitwarden during provisioning.

User attributes

For each user, Bitwarden will use the following attributes:

- An indication that the user is `active` (**required**)
- `email`[a] or `userName` (**required**)
- `displayName`
- `externalId`

[a] – Because SCIM allows users to have multiple email addresses expressed as an array of objects, Bitwarden will use the `value` of the object which contains `"primary": true`.

Group attributes

For each group, Bitwarden will use the following attributes:

- `displayName` (**required**)
- `members`[a]
- `externalId`

[a] – `members` is an array of objects, each object representing a user in that group.

Revoking & restoring access

Once users are provisioned in Bitwarden using SCIM, you can temporarily revoke their access to your organization and its vault items. When a user is temporarily suspended/de-activated in your IdP, their access to your organization will automatically be revoked.

> **Tip**
>
> Only owners can revoke and restore access to other owners.

Users with revoked access are listed in the **Revoked** tab of the organization's **Members** screen and will:

- Not have access to any organization vault items, collections.
- Not have the ability to use SSO to login, or organizational Duo for two-step login.
- Not be subject to your organization's policies.
- Not occupy a license seat.

> **⚠ Warning**
>
> For those accounts that do not have master passwords as a result of SSO with trusted devices, removing them from your organization will cut off all access to their Bitwarden account unless:
>
> 1. You assign them a master password using account recovery beforehand.
> 2. The user logs in at least once post-account recovery in order to fully complete the account recovery workflow.
>
> Additionally, users will not be able to re-join your organization unless the above steps are taken before they are removed from the organization. In this scenario, the user will be required to delete their account and be issued a new invitation to create an account and join your organization.
>
> Revoking access to the organization, but not removing them from the organization, will still allow them to log in to Bitwarden and access **only** their individual vault.

Learn more about revoking and restoring access.

SCIM events

Your organization will capture event logs for actions taken by SCIM integrations, including inviting users and removing users, as well as creating or deleting groups. SCIM-derived events will register `SCIM` in the **Member** column.

Pre-existing users and groups

Organizations with users and groups that were onboarded before activating SCIM, either manually or using Directory Connector, should note the following:

	...that exists in the IdP.	...that does not exist in the IdP.
Pre-existing user	•Will not be duplicated •Will not be forced to re-join the organization •Will not be removed from groups they're already a member of	•Will not be removed from the organization •Will not have group memberships added or removed
Pre-existing group	•Will not be duplicated •Will have members added according to the IdP •Will not have pre-existing members removed	•Will not be removed from the organization •Will not have members added or removed

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

Changing Bitwarden email address

Users that belong to an organization using SCIM are able to change their email address in Bitwarden and their organization's relevant IdP. In order to change a Bitwarden email address in a SCIM organization:

1. Change the email address in Bitwarden by navigating to **Settings** → **My account** (more information here).
2. Once the email has been changed on Bitwarden, update the user value on the IdP or AD client. This could be the `externalid` or a corresponding value, depending on the organization's choice of IdP.
3. Re-sync the IdP or AD client to implement the changes.

> **Note**
> If the user email address is updated and synced on the IdP or AD prior to updating the Bitwarden email, the updated email will be interpreted as a new user.