ADMIN CONSOLE > MANAGE MEMBERS > SCIM

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.

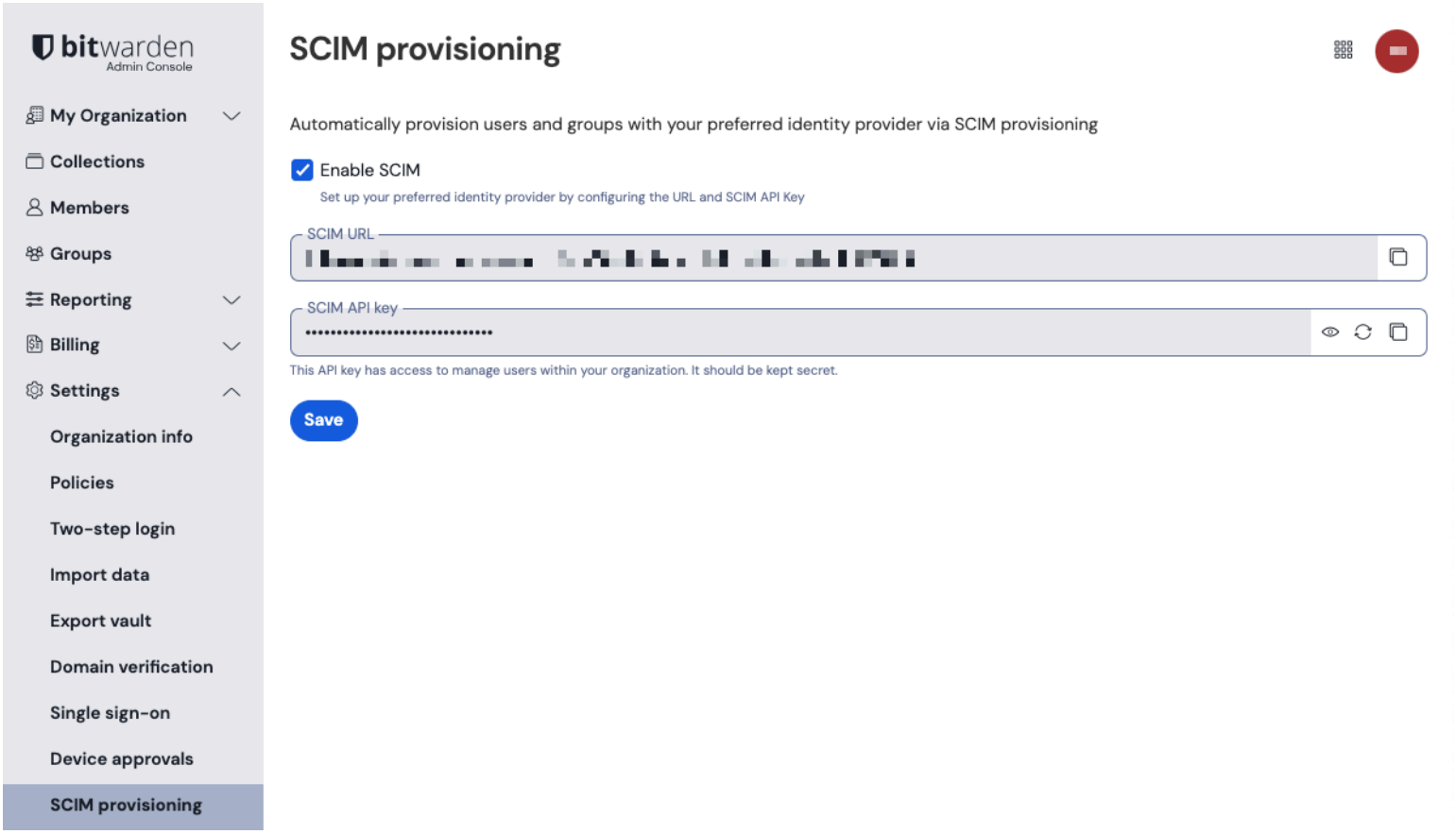
> **ⓘ Note**
>
> SCIM integrations are available for **Teams and Enterprise organizations**. Customers not using a SCIM-compatible identity provider may consider using Directory Sync as an alternative means of provisioning.

Bitwarden supports SCIM v2 using standard attribute mappings and offers integration documentation for:

- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping Identity

Set 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

The following section covers some generic information that can be used to set up SCIM, however Bitwarden recommends using one of the integration documents for:

- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping Identity

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`

> **Note**
>
> [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`

> **Note**
>
> [a] - `members` is an array of objects, each object representing a user in that group. **Group provisioning must be used in order to assign synced users to groups**, however the SCIM API cannot be used to query members in a group. To query group membership, use the Public API.

SCIM event logs

Organizations using SCIM 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.

Updates to existing objects

The following sections describe the changes that SCIM provisioning will sync to your organization for members and groups **when a change occurs in the IdP**:

Member status

When a user is temporarily suspended or de-activated in your IdP, as opposed to being outright removed, their access to your organization will automatically be revoked. 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 member accounts that do not have master passwords as a result of SSO with trusted devices:
>
> - Removing them from your organization eliminates all access to their Bitwarden account unless they were previously assigned a master password using account recovery and they log in with that master password at least once before being removed.
>
> These users will not be able to re-join your organization unless the above steps are taken **before** they are removed from the organization. If they aren't, each removed 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.

Member email address

> **ⓘ Note**
>
> Members of organizations using trusted devices cannot change their email address unless issued a master password with account recovery.
>
> Members of organizations using Key Connector cannot change their email address. Members accounts will need to deleted and re-provisioned to accommodate an email address change. Remind users to export data prior to account deletion and re-import their data once provisioned with their new email address.

Members provisioned using SCIM are able to change their account email address in Bitwarden and their organization's relevant IdP, however in order to do so they must:

1. First change the email address in Bitwarden by navigating to **Settings** → **My account** (learn more).
2. Once the email has been changed in 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.

Member display name

While requests to the SCIM API can be configured to include member display names, this data is not currently synced to Bitwarden on initial provision or when changes occur in the IdP.

Member external ID

While SCIM provisioning will assign an external ID to a user when they're initially provisioned, it will not currently sync changes to the external ID from the IdP to Bitwarden.

Updates to pre-SCIM objects

> **⚠ Warning**
>
> If you used Directory Connector prior to implementing SCIM, make sure to turn Directory Connector off before turning SCIM provisioning on.

The following sections describe the changes that SCIM provisioning will sync to your organization for members and groups **that existed in your organization prior to the implementation of SCIM**:

Members added prior to SCIM

SCIM provisioning will treat members that **joined your organization before SCIM was implemented** differently depending on whether they do or do not exist in the IdP:

- Members that **exist in the IdP** and joined before SCIM will not be duplicated, required to re-join the organization, or removed from any groups.
- Members that **do not exist in the IdP** and joined before SCIM will not be removed, or added to or removed from any groups.

Groups created prior to SCIM

SCIM provisioning will treat groups that **were created in your organization before SCIM was implemented** differently depending on whether they do or do not exist in the IdP:

- Groups that **exist in the IdP** and were created before SCIM will not be duplicated or have any member removed, but will have new members added according to membership assigned in the IdP.
- Groups that **do not exist in the IdP** and were created before SCIM will not be removed or have any members added or removed.