bitwarden | Help Center Article

ADMIN CONSOLE > MANAGE MEMBERS > SCIM

JumpCloud SCIM Integration

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

JumpCloud SCIM Integration

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

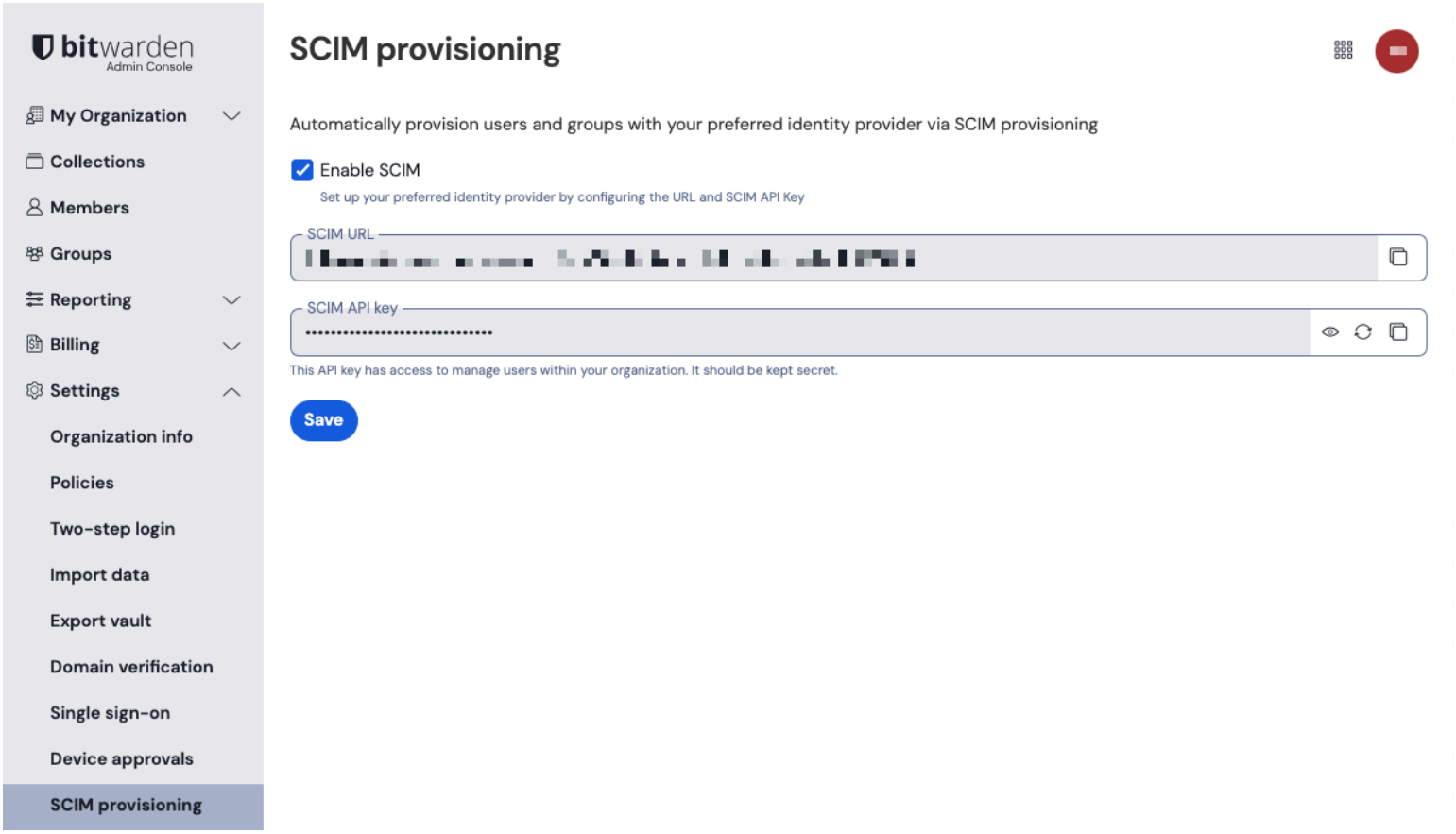
> **Note**
>
> SCIM integrations are available for **Teams and Enterprise organizations**. Customers not using a SCIM-compatible identity provider may consider using Directory Sync as an alternative means of provisioning.

This article will help you configure a SCIM integration with JumpCloud. Configuration involves working simultaneously with the Bitwarden web vault and JumpCloud Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

Enable SCIM

> **Note**
>
> **Are you self-hosting Bitwarden?** If so, complete these steps to enable SCIM for your server before proceeding.

To start your SCIM integration, open the Admin Console and navigate to **Settings → SCIM provisioning**:



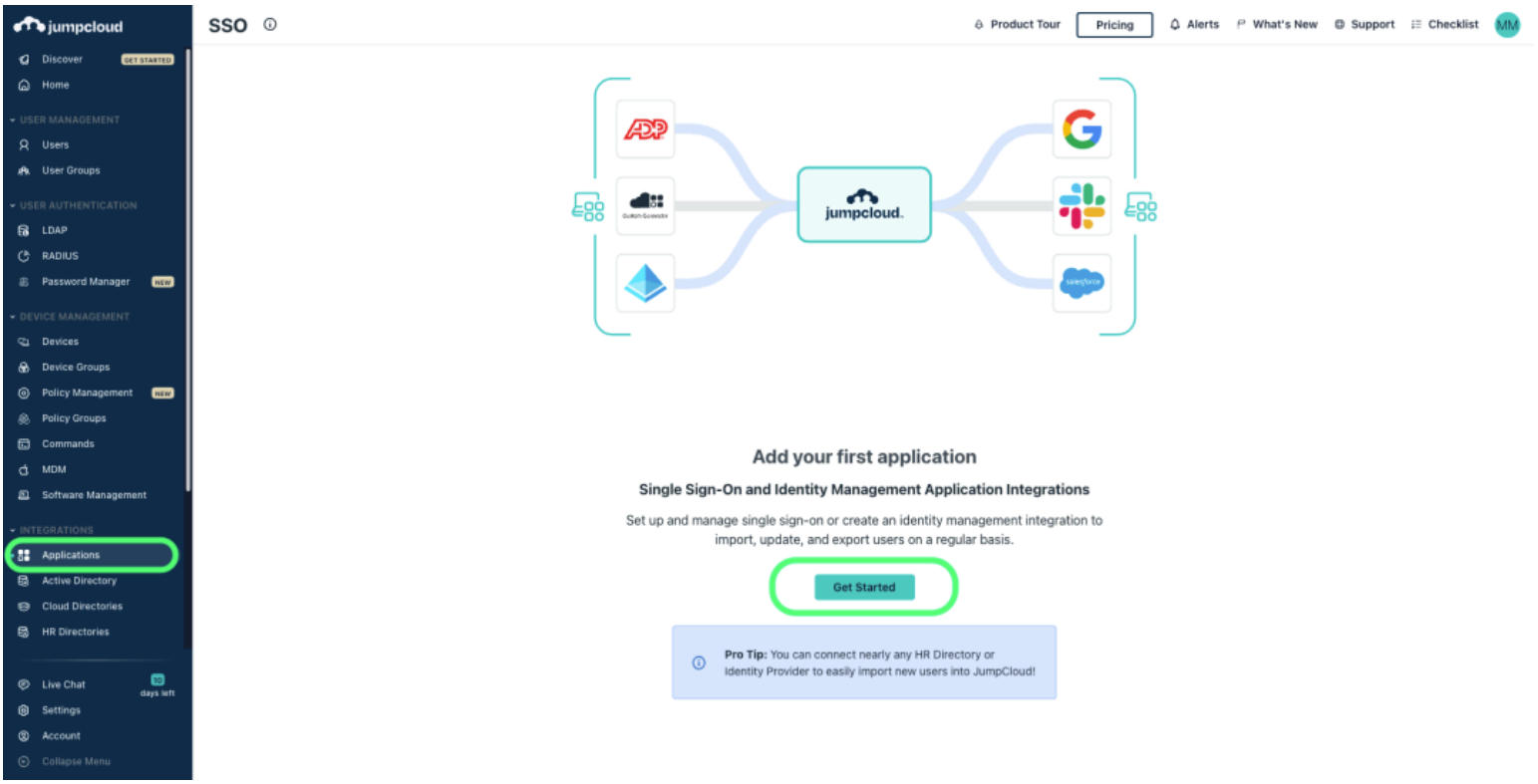
SCIM provisioning

Select the **Enable SCIM** checkbox and take note of your **SCIM URL** and **SCIM API Key**. You will need to use both values in a later step.

Create a JumpCloud app

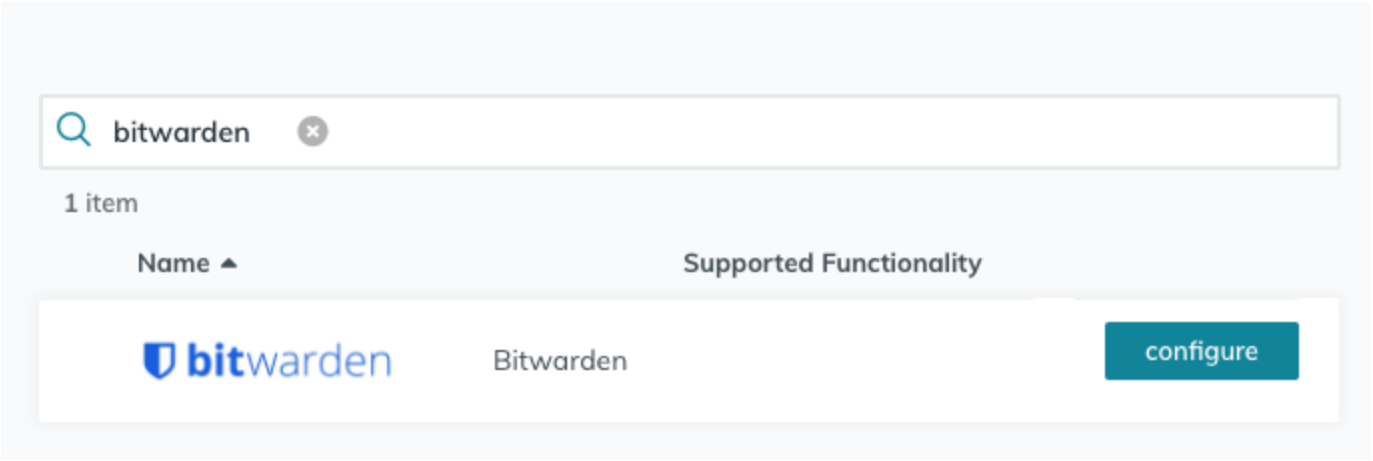
> **Tip**
>
> If you are already using this IdP for login with SSO, open that existing application and skip to this step. Otherwise, proceed with this section to create a new application.

In the JumpCloud Portal, select **Applications** from the menu and select the **Get Started** button:



Create Bitwarden app Jumpcloud

Enter `Bitwarden` in the search box and select the **configure** button:



Configure Bitwarden

General info

In the **General Info** tab, give the application a Bitwarden-specific name.

SSO

If you plan on using JumpCloud for single sign-on, select the **SSO** tab and setup SSO with these instructions. When you are done, or if you are skipping SSO for now, select the **activate** button and complete the confirmation modal.

Identity management

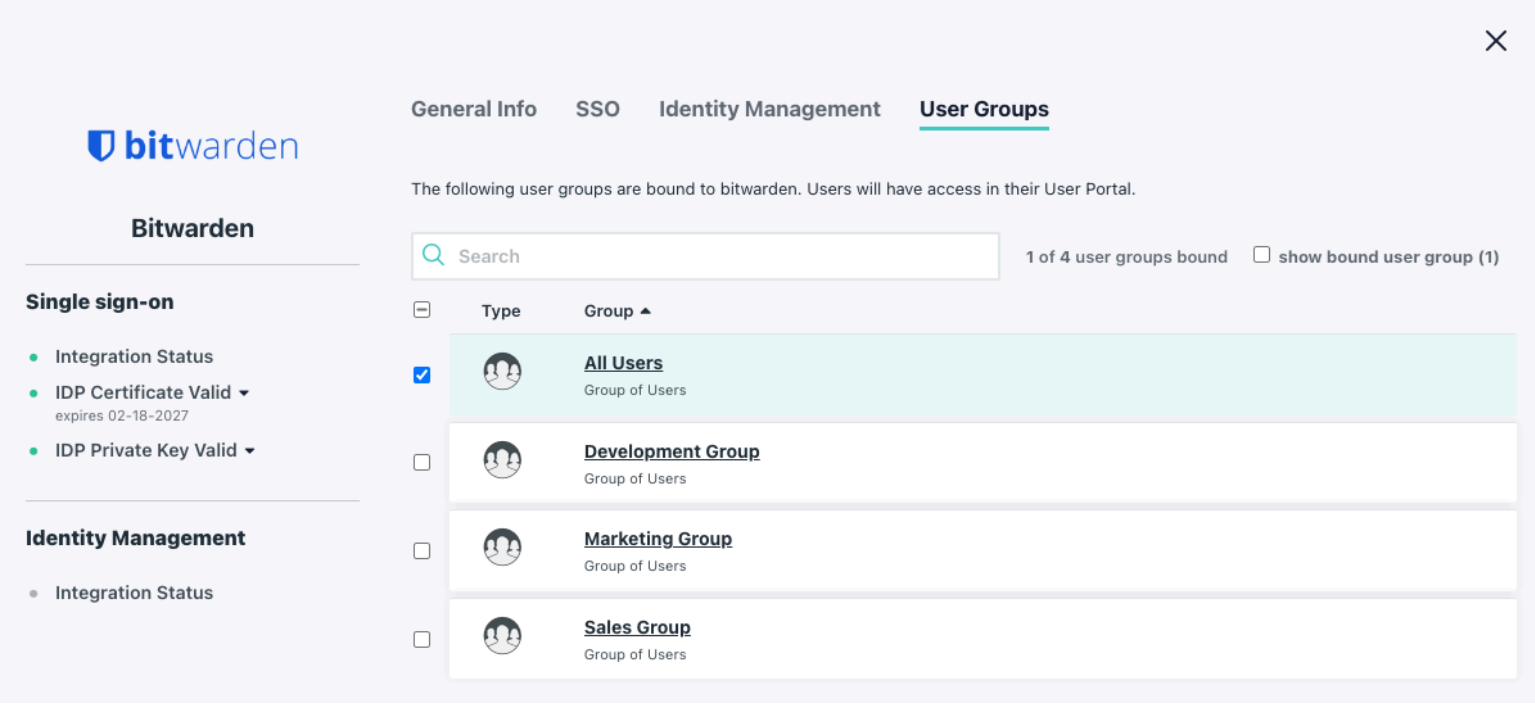
Re-open the application and navigate to the **Identity Management** tab. Expand the **Configuration Settings** box and enter the following information:

Field	Description
Base URL	Enter the SCIM URL (learn more).
Token Key	Enter the SCIM API Key (learn more).

Once you have configured these fields, select the **Activate** button. Once the test comes back successfully, select **Save**.

User groups

In the **User Groups** tab, select the Groups you would like to provision in Bitwarden. Once you select the **Save** button, provisioning according to this specification will begin immediately.



Select User Groups

Finish User Onboarding

Now that your users have been provisioned, they will receive invitations to join the organization. Instruct your users to accept the invitation and, once they have, confirm them to the organization.

> **Note**
>
> The Invite → Accept → Confirm workflow facilitates the decryption key handshake that allows users to securely access organization vault data.

Appendix

User attribute mapping

Bitwarden uses standard SCIM v2 property names, however these may differ from JumpCloud property names. Bitwarden will use the following properties for each user:

Bitwarden Attribute	JumpCloud Default Property
`active`	`!suspended && !passwordExpired`
`emails` [a]	`email`
`displayName`	`displayName`

[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 attribute mapping

Bitwarden will use the following properties for each group:

Bitwarden Attribute	JumpCloud Default Property
`displayName`	`displayName`
`members` [a]	`members`

[a] - Memberships are sent to Bitwarden as an array of objects, each of which represent a user who is a member of that group.