

ADMIN CONSOLE > USER MANAGEMENT >

Ping Identity SCIM Integration

View in the help center:

<https://bitwarden.com/help/ping-identity-scim-integration/>

Ping Identity 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 Connector](#) as an alternative means of provisioning.

This article will help you configure a SCIM integration with Ping Identity. Configuration involves working simultaneously with the Bitwarden web vault and Ping Identity Administrator dashboard. 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**:

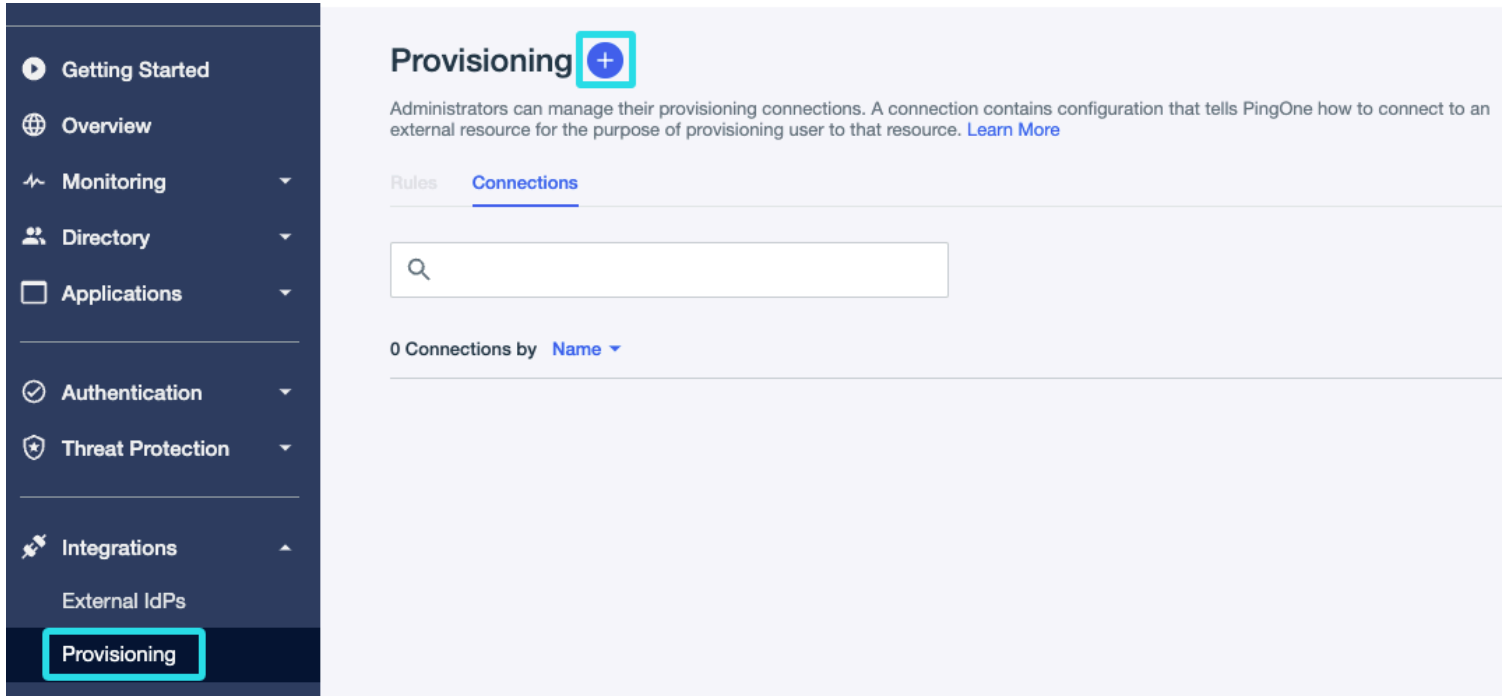
The screenshot shows the Bitwarden Admin Console interface. On the left is a navigation sidebar with the following items: My Organization, Collections, Members, Groups, Reporting, Billing, and Settings. The 'Settings' item is expanded, showing a list of settings: Organization info, Policies, Two-step 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 contains the following elements: a sub-header 'Automatically provision users and groups with your preferred identity provider via SCIM provisioning', a checked checkbox for 'Enable SCIM' with the instruction 'Set up your preferred identity provider by configuring the URL and SCIM API Key', a text input field for 'SCIM URL' containing a masked URL, a text input field for 'SCIM API key' containing a masked key, a warning note 'This API key has access to manage users within your organization. It should be kept secret.', and a blue 'Save' button.

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 SCIM app

1. Navigate to provisioning ⊕ **New Connection**.



2. In the Create a New Connection window, choose the **Select** option for **Identity Store**.

3. In the Identity Store, enter SCIM into the search box and select **SCIM Outbound**. Once this step is complete, select **Next**.

Create a New Connection



To create a new connection first select a provisioning identity store from the options below.



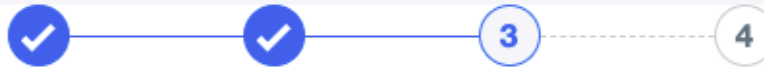
SCIM Outbound

Integrate with a SCIM compliant directory to provision users out of the PingOne Directory.

SCIM Connection

4. Input a Name and Description for the SCIM connection.
5. Next, you will be required to input the **SCIM BASE URL**. Copy the **SCIM URL** value located on the Enable SCIM page in the Bitwarden Admin Console and paste it into this field.
6. Using the **Authentication Method** dropdown menu, select **OAuth 2 Bearer Token**. A field will appear named **OAuth Access Token**, paste the **SCIM API key** value from the Bitwarden Admin Console into this field.

Create a New Connection



Specify the authentication configuration for the connection.

Configure Authentication

SCIM BASE URL *

https://vault.bitwarden.pw/scim/v2/

Users Resource

/Users

SCIM version

2.0

Groups Resource

/Groups

Authentication Method

OAuth 2 Bearer Token

OAuth Access Token *

.....

Auth Type Header

Bearer

Previous

Cancel

Test Connection

Next

Ping Identity SCIM connection test

7. Once setup is complete, you may select **Test Connection**. If successful, select **Next**.

8. On the **Configure Preferences** page, select desired preferences and actions.

Note


Setting the Remove Action setting to **Disable** will result in Bitwarden users being moved to **Revoked** status rather if the user fails to meet the filter criteria set on Ping Identity. Restoring the criteria will return the user to their **previous state**.


If the Remove Action is set to **Delete**, the same action will **deprovision the user**.

9. Select **Save** once complete. Select the newly created Connection and enable the Connection using the toggle.

Bitwarden
Created on 2024-10-09

Overview Configuration



Name	Bitwarden	
Description	Bitwarden SCIM connection	

Enable Ping Identity Connection

Create a Rule

Before syncing user groups and directories, a Rule is required to sync the user groups to Bitwarden SCIM.

1. Return to the Provisioning Screen.
2. Select the **Rules** tab and then **+ New Rule**.
3. Enter an app specific name for the Rule and select **Create Rule**.
4. Edit the new Rule in the Configuration tab. Select **Bitwarden SCIM connection** and then **Save**.

Select Source or Target to choose an available connection.



Available Connections

[+ New Connection](#)

	Bitwarden Bitwarden SCIM connection	
--	---	--

Ping Identity Rule

5. Select the Configuration tab and add a **User Filter**. For more information, see the [Ping Identity documentation](#). Select **Save** once complete.

Bitwarden Rule > Edit User Filter

User Filter
Edit the user filter to change how users are selected for provisioning.

All **Any** of the conditions are true Add +

Attribute Email Address	Operator Equals	Value @my-company.com	
Attribute Country Code	Operator Equals	Value US	

Ping Identity User Filter

6. Enable the Rule using the toggle.

Bitwarden Rule
Created on 2024-10-09



Overview Configuration

Bitwarden Rule



Ping Identity new Rule

Provision groups

1. To assign groups, return to the Provisioning screen and select the rule : **Edit Group Provisioning**.

Bitwarden Rule > Edit Group Provisioning



Select groups for outbound provisioning. Group memberships in the target are updated according to user filter criteria.



For groups with matching names on the target, group memberships (the list of users in a group) will be overwritten with PingOne members during sync. [Learn More](#)

Population

All Groups Selected Groups **1**



Bitwarden
Default



Edit group provisioning

2. Choose the group or groups to provision and select **Save**. Once saved, the directory will trigger a sync.

Appendix

Required attributes

Both the Bitwarden and Ping Identity **SCIM Provisioner with SAML (SCIM v2 Enterprise)** applications use standard SCIM v2 attribute names. Bitwarden will use the following attributes:

User attributes

- `active`
- `emails`[Ⓐ] or `userName`
- `displayName`
- `externalId`

[Ⓐ] - 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`[Ⓐ]
- `externalId`

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