ADMIN CONSOLE > USER MANAGEMENT

User Management

View in the help center:
https://bitwarden.com/help/managing-users/

User Management

User seats

A "user seat" refers to a license for a single user within an organization. A user seat, while occupied by a member of your organization, grants that member access to Bitwarden services under your specific plan. A user seat is not permanently attached to that member; when they leave the organization that user seat is made available for use by a new member.

Bitwarden cloud Teams and Enterprise organizations will **automatically scale up** user seats as you invite new users. You can set a seat limit on scaling to prevent your seat count from exceeding a specified number, or manually add seats as desired. Regardless of how you choose to add seats, you will need to manually remove seats you're no longer using.

Adding and removing user seats will adjust your future billing totals. Adding seats will immediately charge your payment method on file at an adjusted rate so that **you will only pay for the remainder of the billing cycle** (month/year). Removing seats will cause your next charge to be adjusted so that you are **credited for time not used** by the already-paid-for seat.

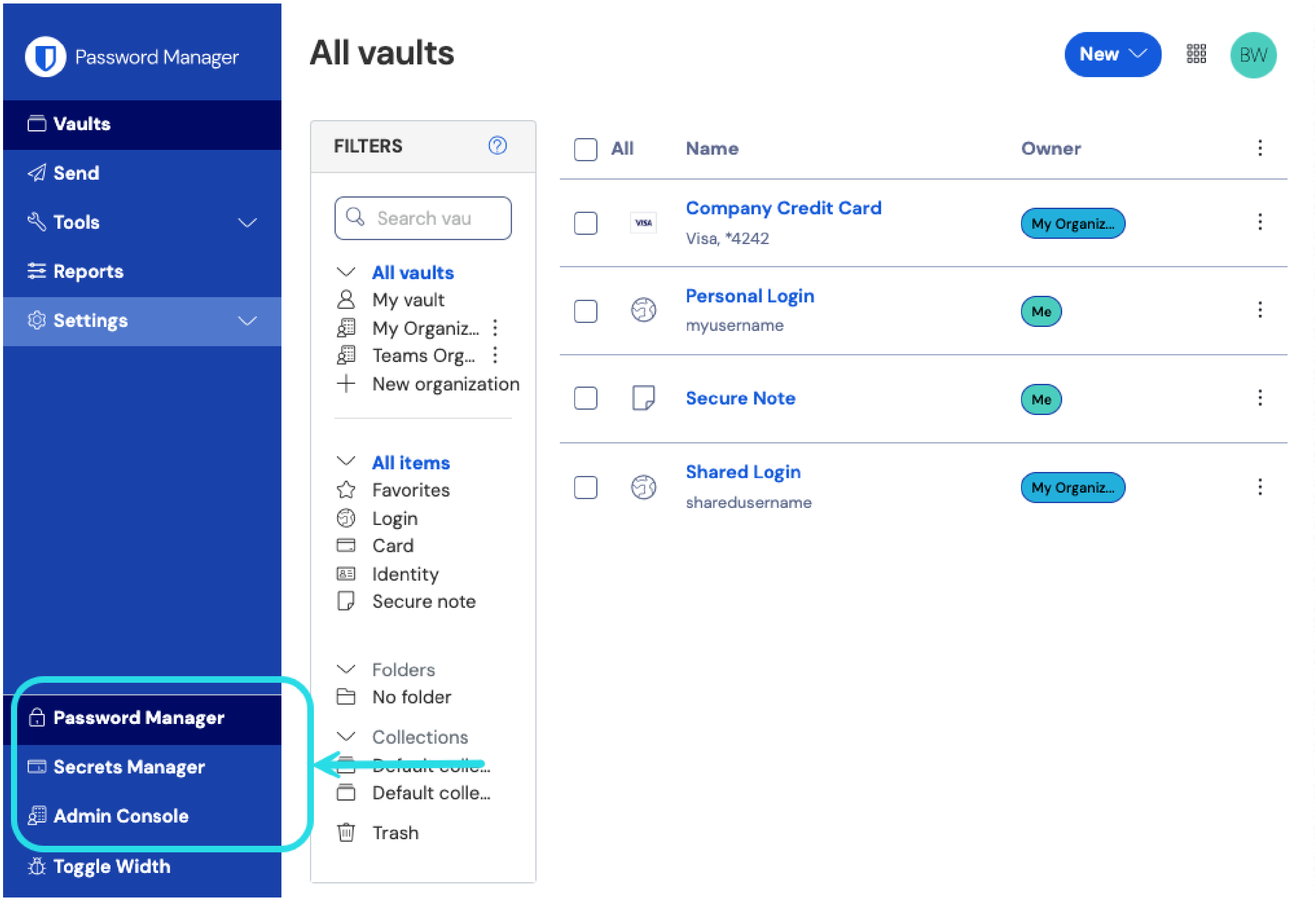
> ⓘ **Note**
>
> Only an an organization owner or provider service user can add or remove seats, as this directly affects billing.

Set a seat limit

> ⓘ **Note**
>
> The number of seats a self-hosted organization has will always mirror its counterpart cloud-organization. You will be required to manage your seat count through the cloud Admin Console, however billing sync can be setup to make these changes reflect for your self-hosted organization without requiring you to re-upload you license.

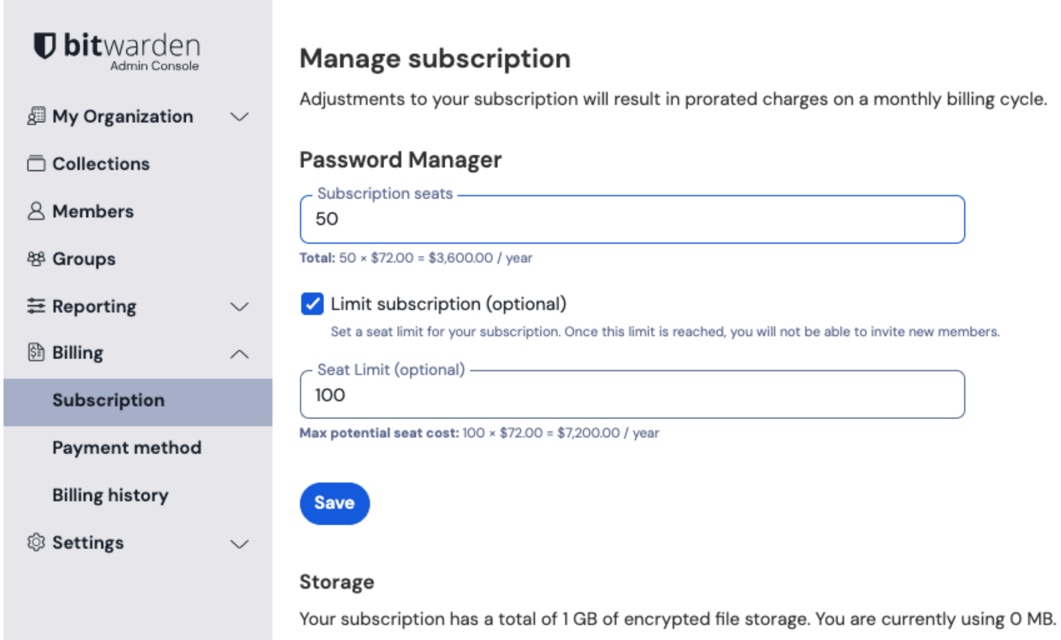
To set a limit on the number of seats your organization can scale up to:

1. Log in to the Bitwarden web app and open the Admin Console using the product switcher:



Product switcher

2. Navigate to **Billing → Subscription** and check the **Limit subscription** checkbox:



Manage subscription

Adjustments to your subscription will result in prorated charges on a monthly billing cycle.

Password Manager

Subscription seats: 50

Total: 50 × $72.00 = $3,600.00 / year

☑ Limit subscription (optional)

Set a seat limit for your subscription. Once this limit is reached, you will not be able to invite new members.

Seat Limit (optional): 100

Max potential seat cost: 100 × $72.00 = $7,200.00 / year

Storage

Your subscription has a total of 1 GB of encrypted file storage. You are currently using 0 MB.

Set a seat limit

3. In the **Seat limit** input, specify a seat limit.

4. Select **Save**.

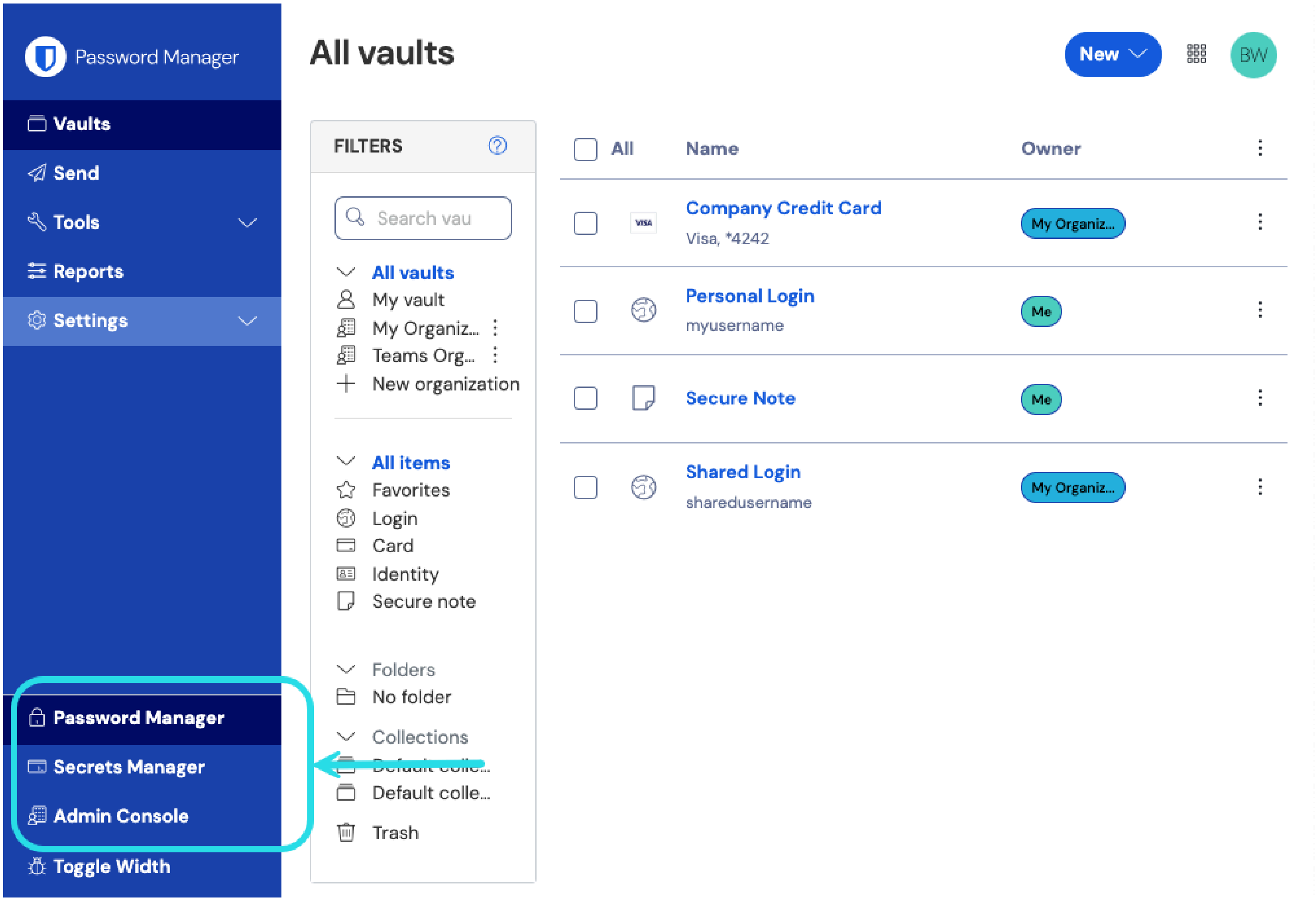
> **Note**
>
> Once the specified limit is reached, you will not be able to invite new users unless you increase the limit.

Manually add or remove seats

> **Note**
>
> The number of seats a self-hosted organization has will always mirror its counterpart cloud-organization. You will be required to manage your seat count through the cloud Admin Console, however billing sync can be setup to make these changes reflect for your self-hosted organization without requiring you to re-upload you license.

To manually add or remove seats to your organization:

1. Log in to the Bitwarden web app and open the Admin Console using the product switcher:

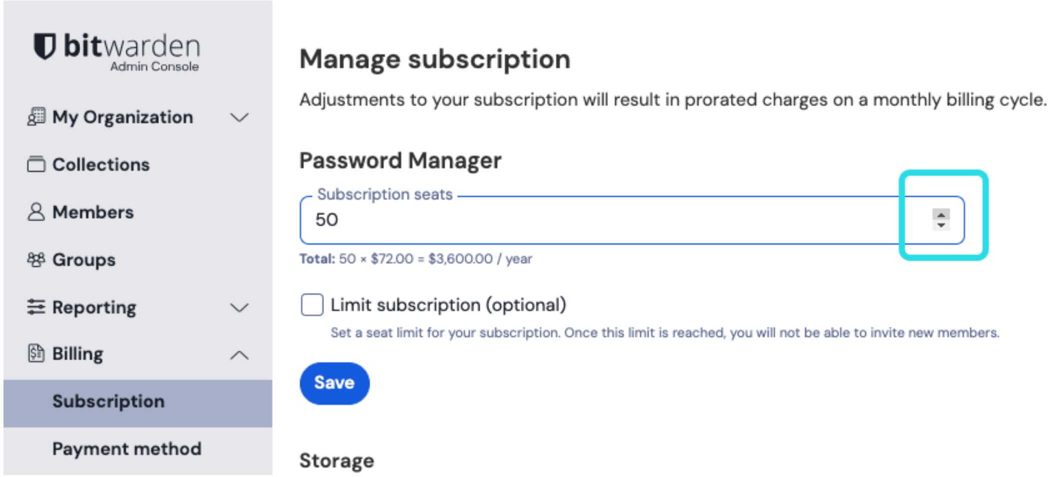


□ All	Name	Owner
□	Company Credit Card Visa, *4242	My Organiz...
□	Personal Login myusername	Me
□	Secure Note	Me
□	Shared Login sharedusername	My Organiz...

Product switcher

2. Navigate to **Billing → Subscription.**

3. In the **Subscription seats** input, add or remove seats using the hover-over arrows:



Manage subscription

Adjustments to your subscription will result in prorated charges on a monthly billing cycle.

Password Manager

Subscription seats: 50

Total: 50 × $72.00 = $3,600.00 / year

□ Limit subscription (optional)

Set a seat limit for your subscription. Once this limit is reached, you will not be able to invite new members.

Save

Storage

Add or remove seats

4. Select **Save**.

> **Note**
>
> If you are increasing your **Subscription seats** above a specified **Seat limit**, you must also increase the seat limit so that it is equal to or greater than the desired subscription seat count.

Onboard users

To ensure the security of your organization, Bitwarden applies a 3-step process for onboarding a new member, invite → accept → confirm.

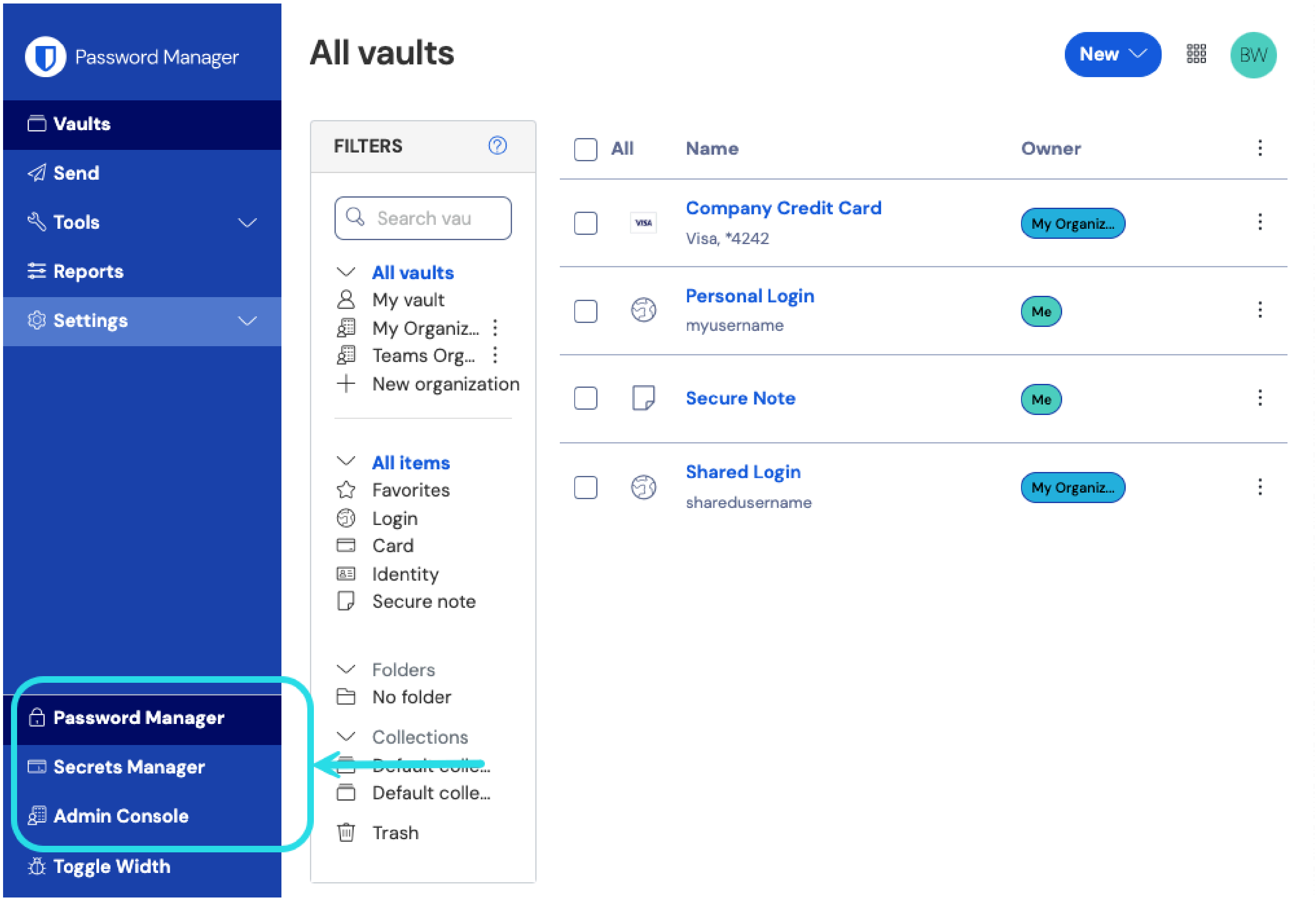
> **Tip**
>
> This document covers the manual onboarding flow for adding users to Bitwarden organizations, however Bitwarden offers two methods for automatic user and group provisioning:
>
> - Teams and Enterprise organizations can use SCIM integrations for Azure AD, Okta, OneLogin, and JumpCloud.
> - Teams and Enterprise organizations can use Directory Connector for Active Directory/LDAP, Azure AD, Google Workspace, Okta, and OneLogin.

Invite

> **Tip**
>
> For Enterprise organizations, we recommend configuring enterprise policies prior to inviting users to ensure compliance on-entrance to your organization.

To invite users to your organization:

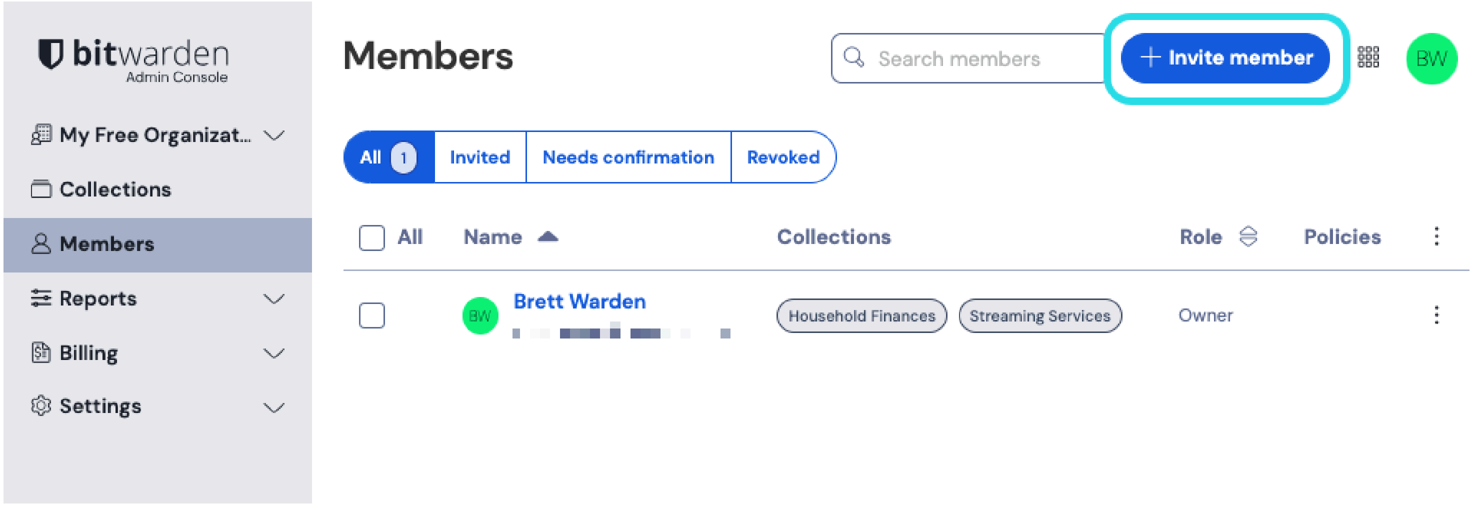
1. Log in to the Bitwarden web app and open the Admin Console using the product switcher:



□ All	Name	Owner
□	Company Credit Card Visa, *4242	My Organiz...
□	Personal Login myusername	Me
□	Secure Note	Me
□	Shared Login sharedusername	My Organiz...

Product switcher

2. Navigate to **Members** and select the + **Invite User** button:



□ All	Name	Collections	Role	Policies
□	Brett Warden [redacted]	Household Finances Streaming Services	Owner	

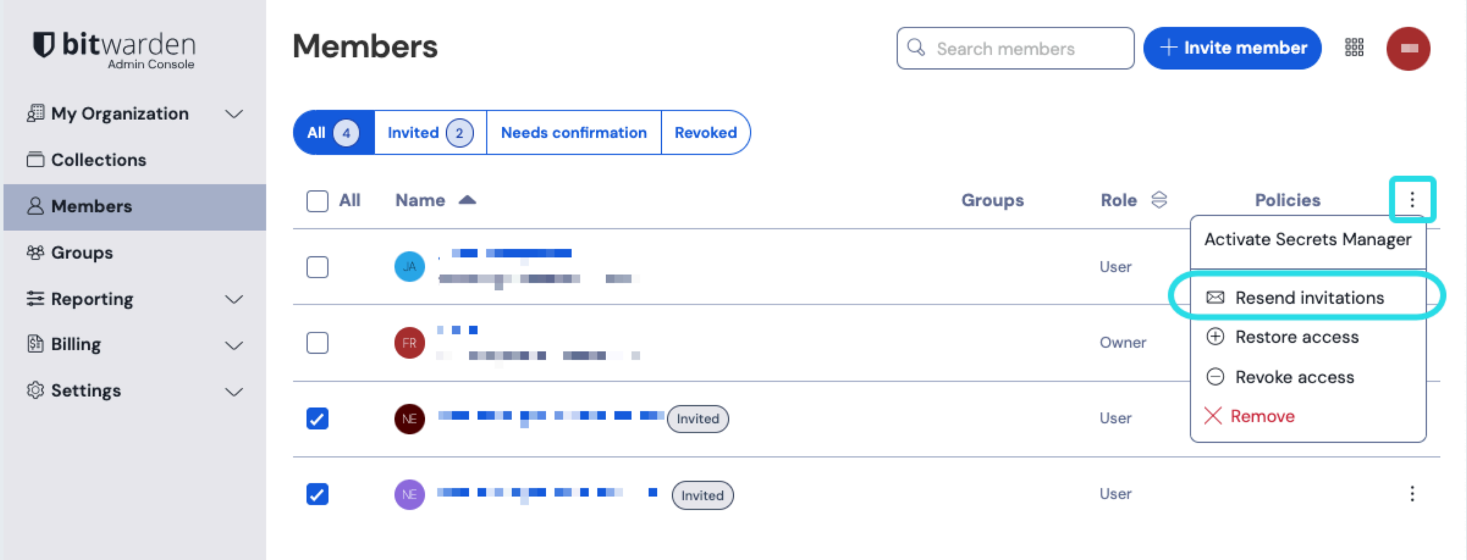
Invite member to an organization

3. On the Invite user panel:

- Enter the **Email** address where new users should receive invites. You can add up to 20 users at a time by comma-separating email addresses.
- Select the **Member role** to be applied to new users. Member role will determine what permissions these users will have at an organizational level.
- In the **Groups** tab, select which groups to add this user to.
- In the **Collections** tab, select collects to give this user access to and what permissions they should have to each collection.

4. Click **Save** to invite the designated users to your organization.

> ⓘ **Note**
>
> **Invitations expire after 5 days**, at which point the user will need to be re-invited. Re-invite users in bulk by selecting each user and using the ⋮ options menu to **Resend invitations**:



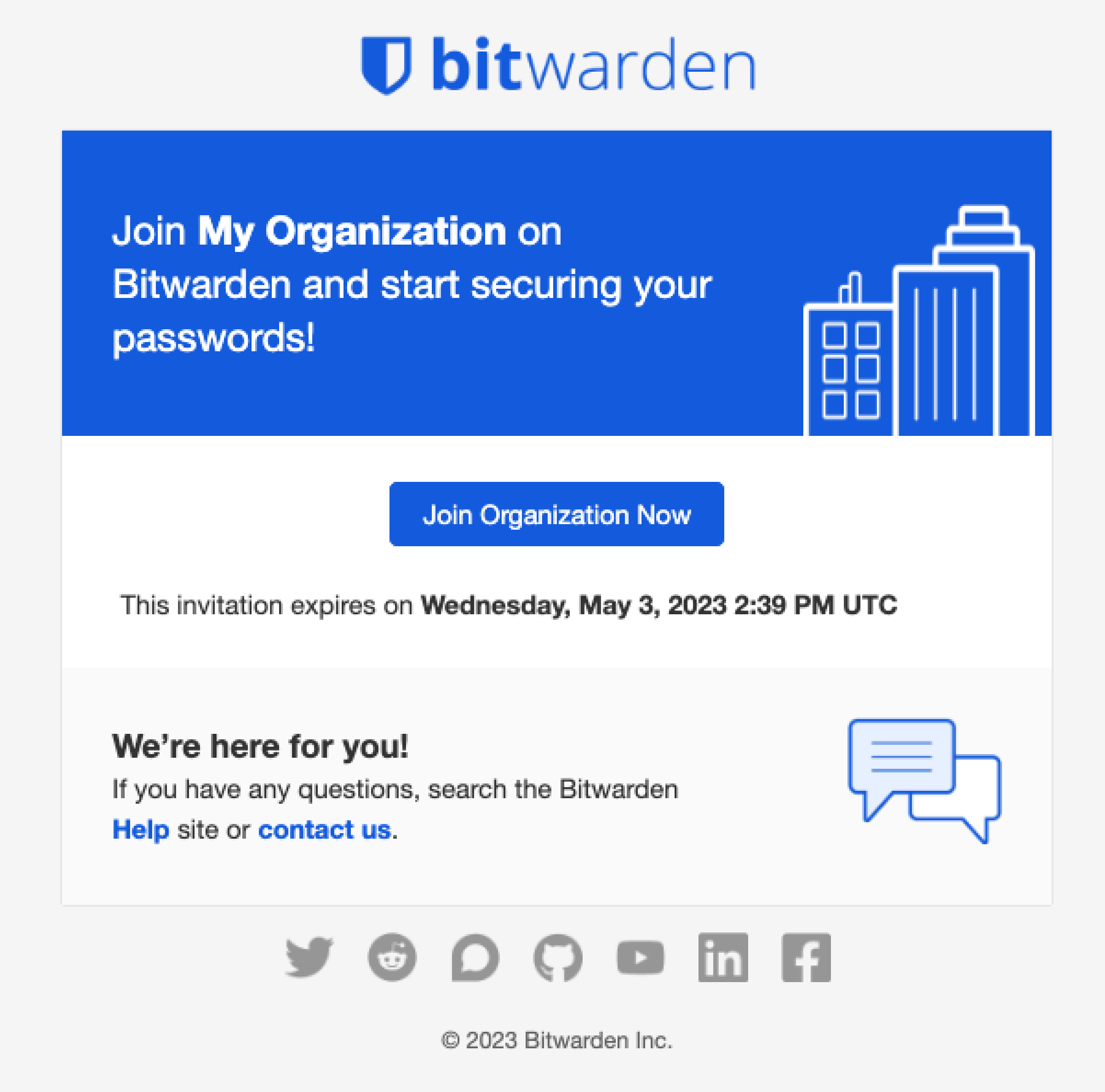
		Name	Groups	Role	Policies
□	JA	[redacted]		User	
□	FR	[redacted]		Owner	
☑	NE	[redacted] Invited		User	
☑	NE	[redacted] Invited		User	⋮

Bulk re-invite

> If you're self-hosting Bitwarden, you can configure the invitation expiration period using an environment variable.

Accept

Invited users will receive an email from Bitwarden inviting them to join the organization. Clicking the link in the email will open the Bitwarden web app, where the user can log in or create an account to accept the invitation:



Join **My Organization** on Bitwarden and start securing your passwords!

This invitation expires on **Wednesday, May 3, 2023 2:39 PM UTC**

We're here for you!

If you have any questions, search the Bitwarden **Help** site or **contact us**.

© 2023 Bitwarden Inc.

Invitation to join

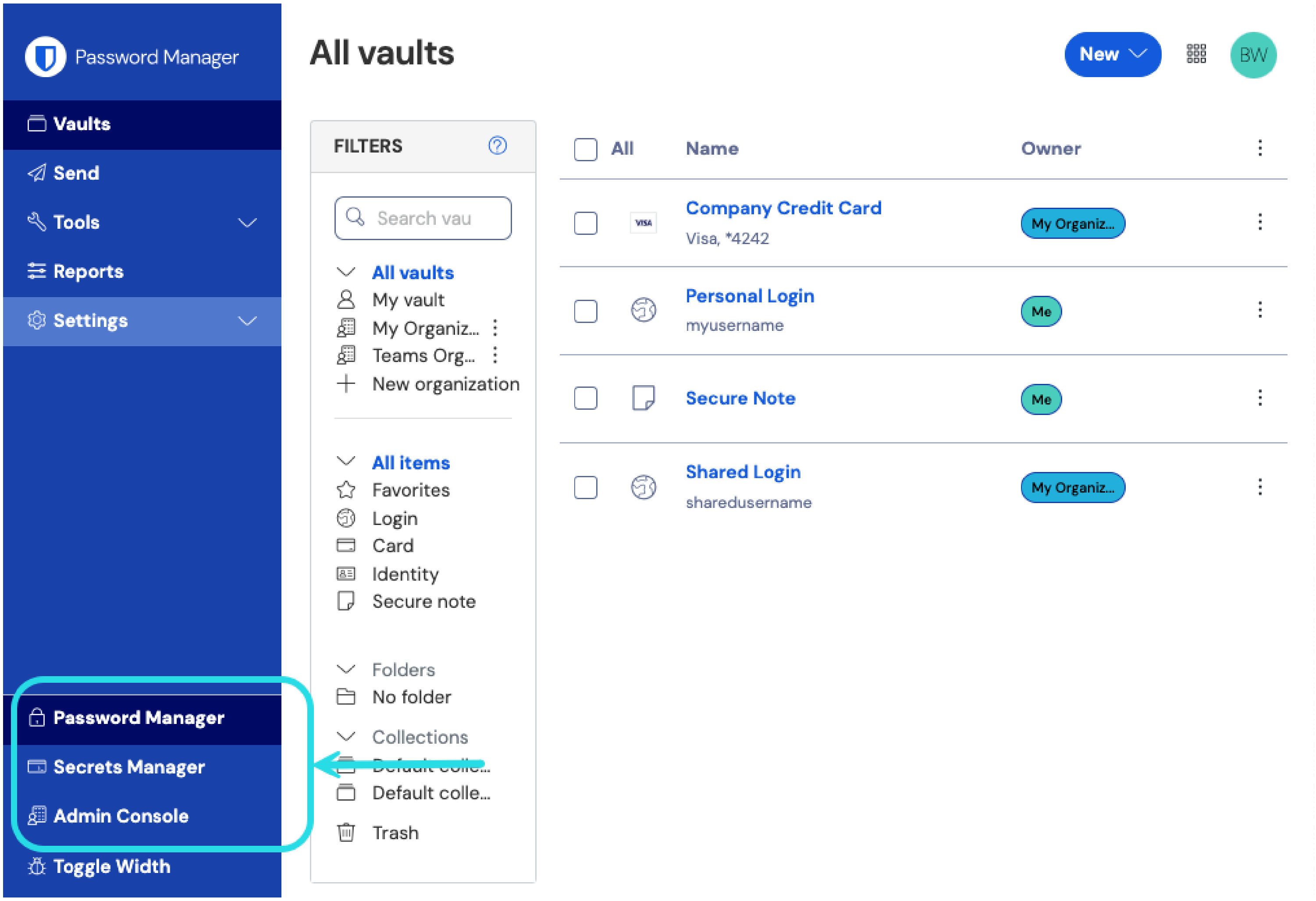
You must **fully log in to the Bitwarden web app** to accept the invitation. When you accept an invitation, you will be notified that you can access the organization once confirmed. Additionally, organization members will have their email automatically verified when they accept an invitation.

Confirm

> **Tip**
>
> The 3-step invite → accept → confirm procedure is designed to facilitate secure sharing between organizations and users by maintaining end-to-end encryption. Learn more.

To confirm accepted invitations into your organization:

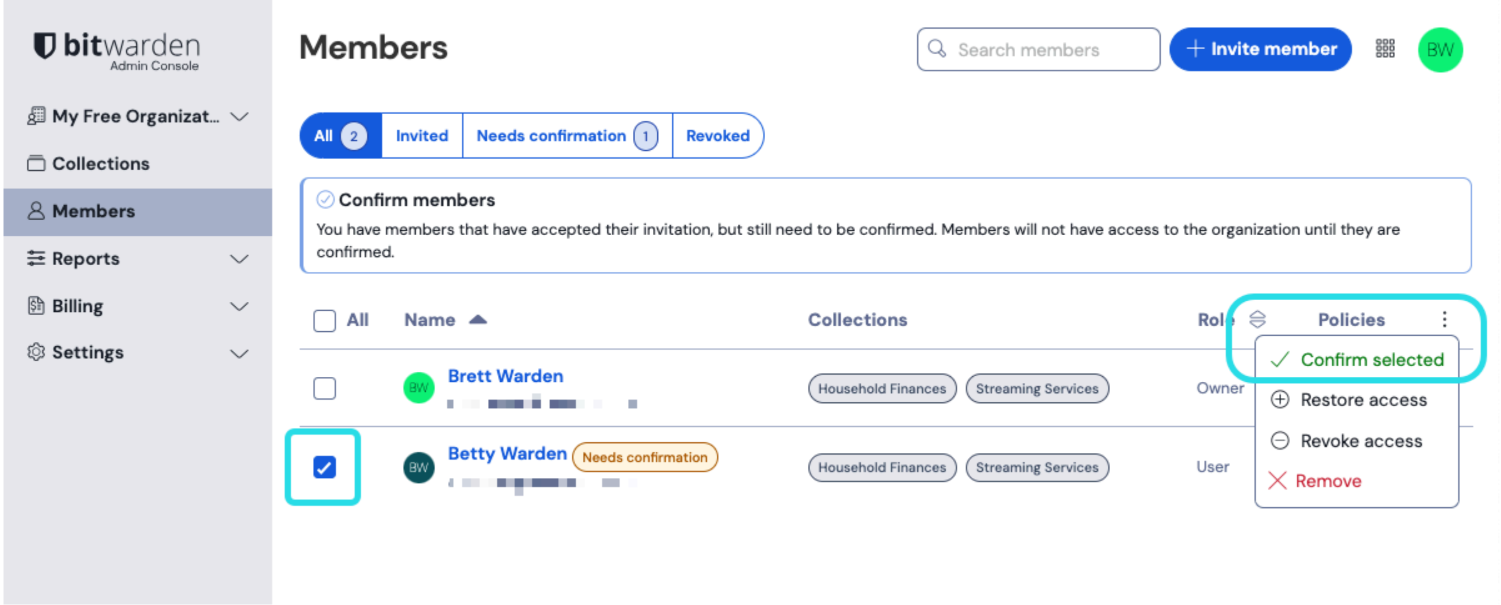
1. Log in to the Bitwarden web app and open the Admin Console using the product switcher:



Product switcher

2. Navigate to **Members**.

3. Select any `Accepted` users and use the ⋮ options menu to ✓ **Confirm selected**:

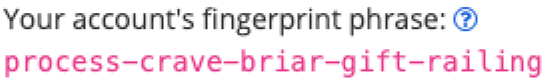


Confirm members

You have members that have accepted their invitation, but still need to be confirmed. Members will not have access to the organization until they are confirmed.

Confirm member to an organization

4. Verify that the fingerprint phrase on your screen matches the one your new member can find in **Settings → My account**:



Your account's fingerprint phrase: ?

`process-crave-briar-gift-railing`

Sample Fingerprint Phrase

Each fingerprint phrase is unique to its account, and ensures a final layer of oversight in securely adding users. If they match, select **Submit**.

> **ⓘ Note**
>
> If **Never prompt to verify fingerprint phrases** has been toggled on, fingerprint phrase verification be reactivated by clearing the browser cache and cookies.

Deprovision users

⚠ **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:

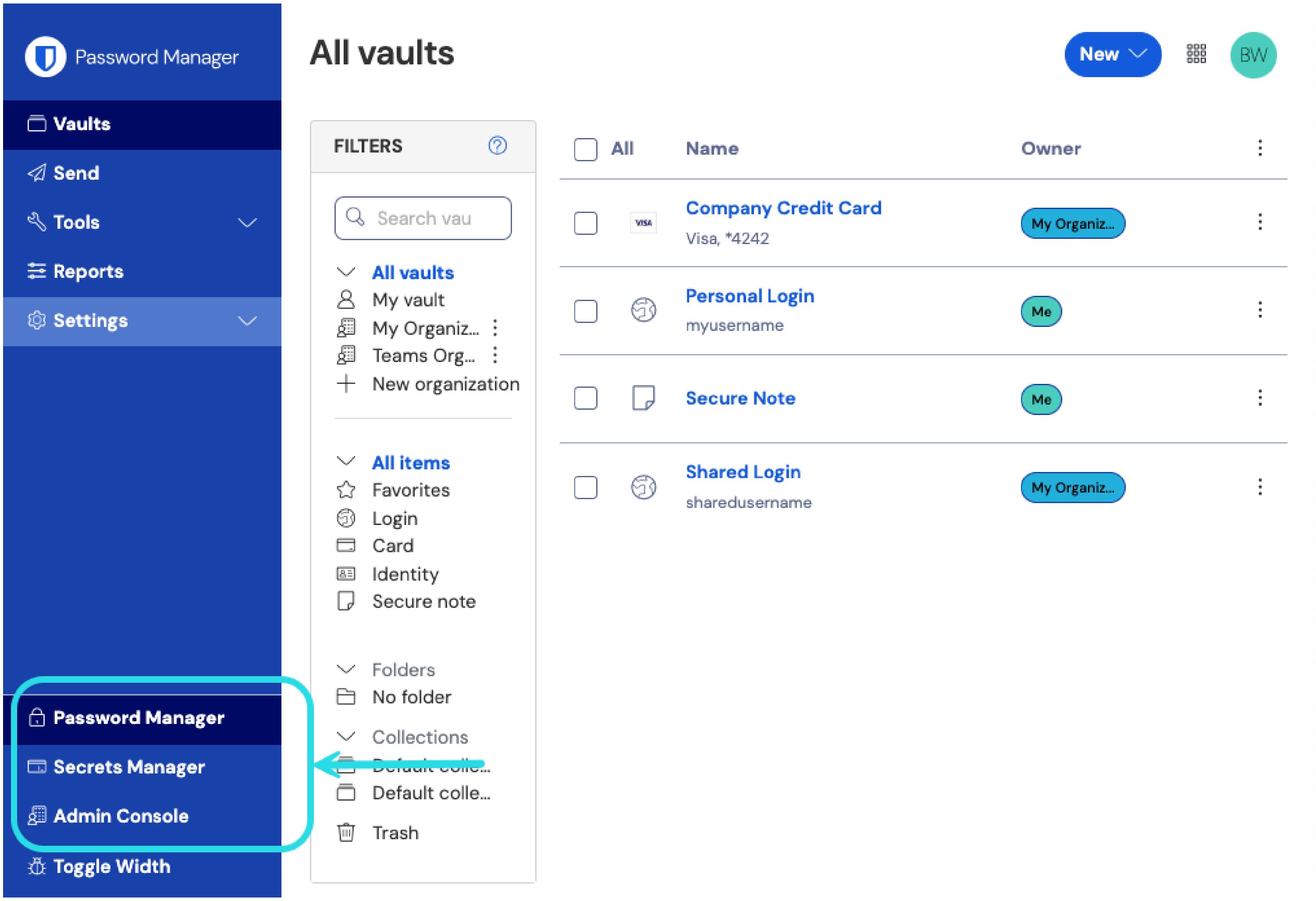
1. You assign them a master password using account recovery beforehand.
2. The user logs in at least once post-account recovery in order to fully complete the account recovery workflow.

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.

To remove users from your organization:

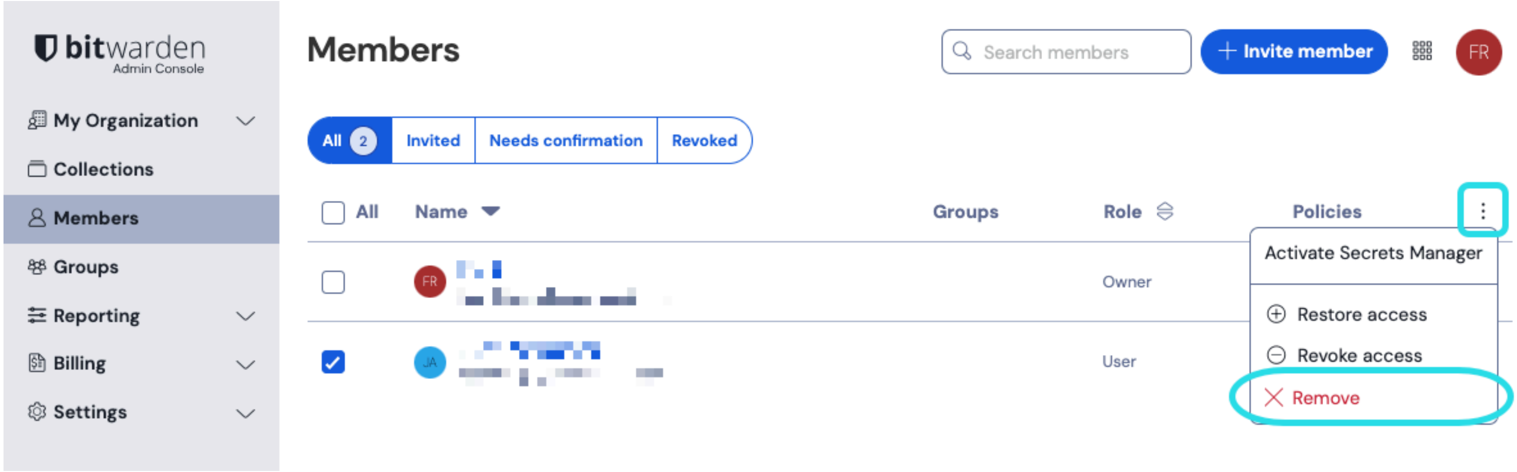
1. Log in to the Bitwarden web app and open the Admin Console using the product switcher:



Product switcher

2. Navigate to **Members**.

3. Select the users you want to remove from the organization and use the ⋮ Options menu to ✕ **Remove**:



Remove members

Tip

Offline devices cache a read-only copy of vault data, including organizational vault data. Some clients may retain access to this read-only data for a short period of time after a member is deprovisioned. If you anticipate malicious exploitation of this, credentials the member had access to should be updated when you remove them from the organization.

Deleting user accounts

Removing a user from your organization does not delete their Bitwarden account. When a user is removed they can no longer access the organization or any shared items and collections, however they will still be able to log in to Bitwarden using their existing master password and access any individual vault items.

Depending on the particulars of your implementation, you may be able to use one of the following methods to delete a Bitwarden user account that belongs to a deprovisioned user:

1. If you are self-hosting Bitwarden, an authorized admin can delete the account from the System Administrator Portal.

2. If the account has an `@yourcompany.com` email address that your company controls, you can use the delete without logging in workflow and confirm deletion within the `@yourcompany.com` inbox. For more information, see Delete an Account or Organization.

Revoke access

Tip

If your organization has an active SCIM integration, user access to your organization is automatically revoked when users are suspended or de-activated in your source directory.

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.

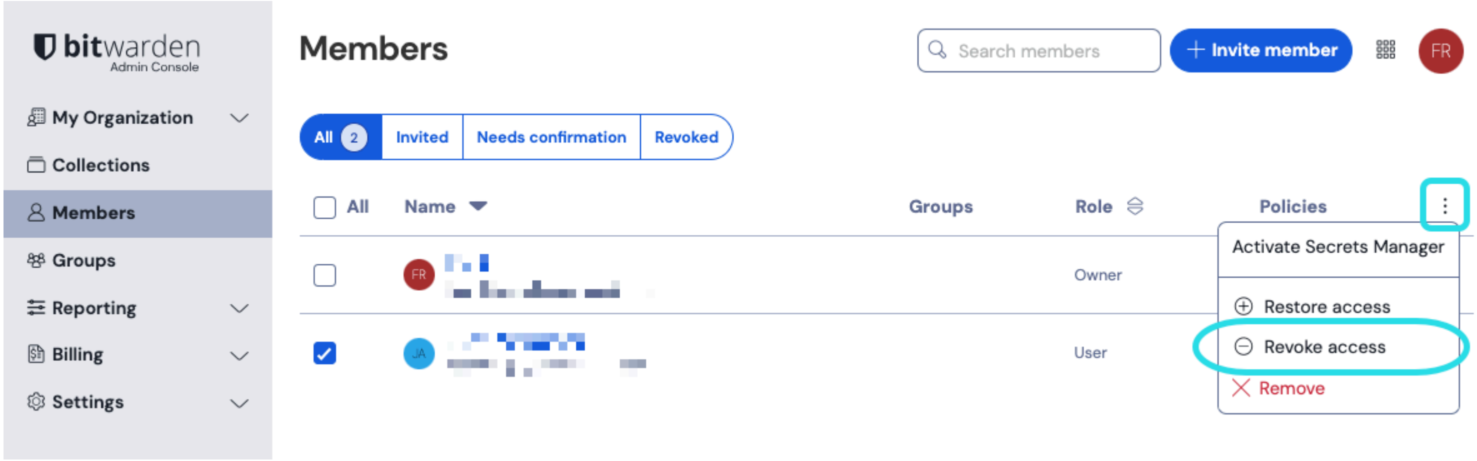
Additionally, users will not be able to re-join your organization unless the above steps are taken before they are removed from the organization. In this scenario, the user will be required to delete their account and be issued a new invitation to create an account and join your organization.

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.

Instead of completely removing members, you can also temporarily revoke access to your organization and its vault items. To revoke access:

1. In the Admin Console, navigate to **Members**.

2. Select the members you want to revoke access for and use the ⋮ Options menu to **Revoke access**:



Revoke access

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

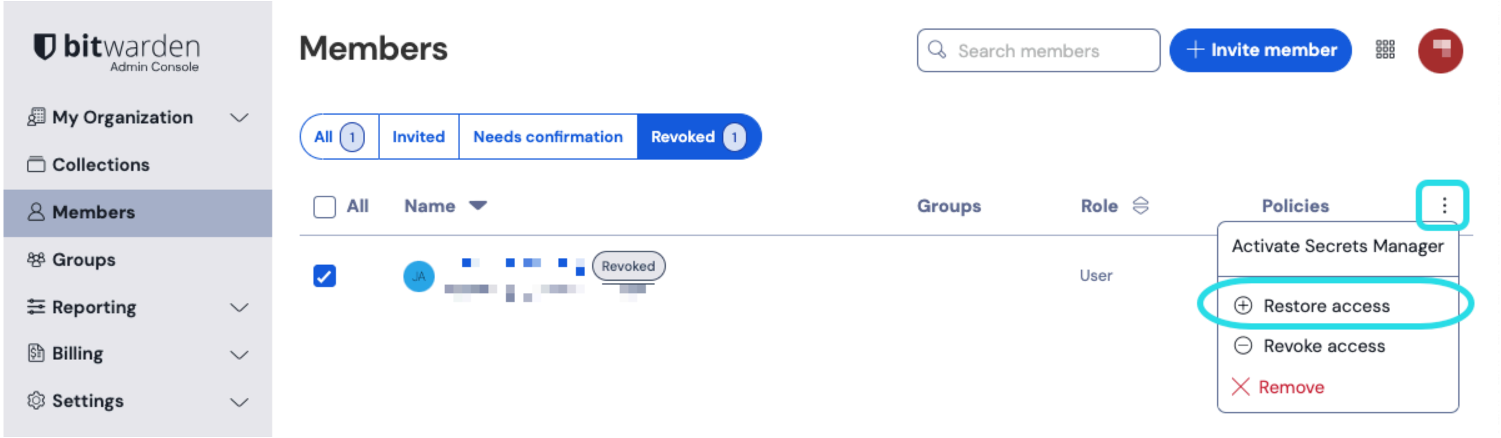
Users with revoked access are listed in the **Revoked** tab and will:

- Not have access to any organization vault items, collections, and more.
- 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.

Restore access

To restore access to a user:

1. In the Admin Console, navigate to **Members**.
2. Open the **Revoked** members tab.
3. Select the users you want to restore access for and use the ⋮ Options menu to **Restore access**:

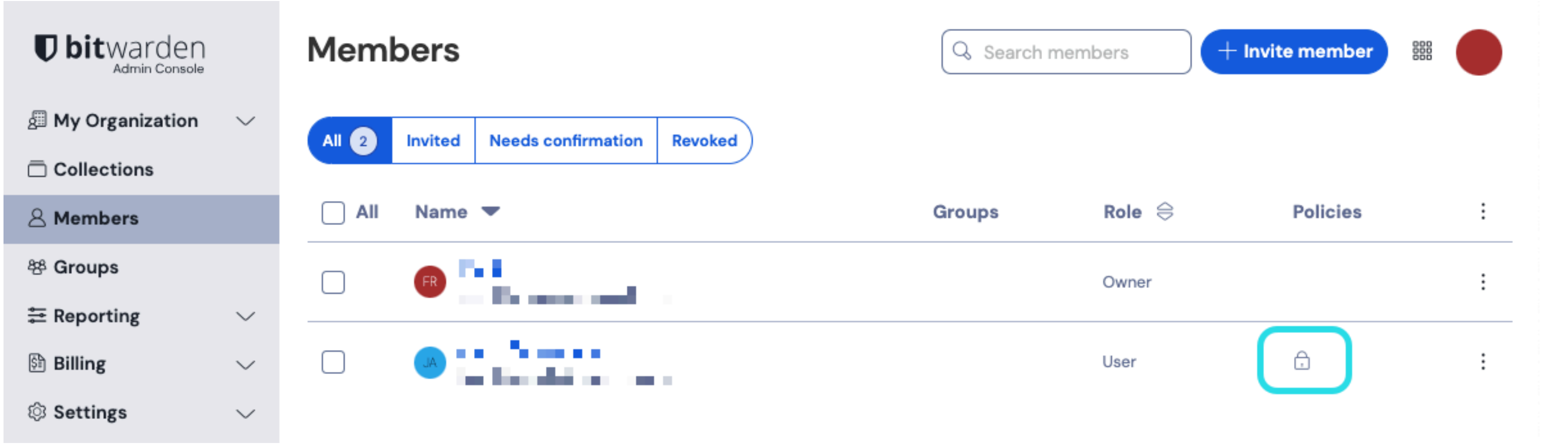


Restore access

When you restore access to a user, they don't need to go through the invite → accept → confirm workflow again.

Review user 2FA status

The 2FA status of users can be viewed from the **Members** page. If the user has a 🔒 icon, two-step login has been enabled on their Bitwarden account.



2FA indicator