

ADMIN CONSOLE > MANAGE MEMBERS

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 [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 your 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:

The screenshot shows the Bitwarden interface. On the left, a sidebar contains navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. The 'Password Manager' option is highlighted with a red box, and an arrow points to the 'Secrets Manager' option below it. The main content area is titled 'All vaults' and features a 'New' button and a user profile icon. Below this is a table of vaults with columns for 'All', 'Name', and 'Owner'. The table lists four vaults: 'Company Credit Card' (owned by 'My Organiz...'), 'Personal Login' (owned by 'Me'), 'Secure Note' (owned by 'Me'), and 'Shared Login' (owned by 'My Organiz...'). A 'FILTERS' sidebar is also visible, showing options like 'All vaults', 'My vault', 'My Organiz...', 'Teams Org...', 'New organization', 'All items', 'Favorites', 'Login', 'Card', 'Identity', 'Secure note', 'Folders', 'No folder', 'Collections', 'Default colle...', and 'Trash'.

Product switcher

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

The screenshot shows the Bitwarden Admin Console interface. The left sidebar contains navigation options: My Organization, Collections, Members, Groups, Reporting, Billing, Subscription, Payment method, Billing history, and Settings. The 'Billing' option is highlighted. The main content area is titled 'Manage subscription' and includes a note about prorated charges. Below this is the 'Password Manager' section, which contains a 'Subscription seats' input field set to 50, a 'Total' calculation of 50 x \$72.00 = \$3,600.00 / year, a checked 'Limit subscription (optional)' checkbox, a 'Seat Limit (optional)' input field set to 100, and a 'Max potential seat cost' calculation of 100 x \$72.00 = \$7,200.00 / year. A 'Save' button is located at the bottom of this section. The 'Storage' section below shows a total of 1 GB of encrypted file storage.

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 your 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:

Product switcher

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

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

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:

Product switcher

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

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**:

Members

Search members [+ Invite member](#)

All 4 **Invited** 2 Needs confirmation Revoked

☐	Name	Groups	Role	Policies
☐	JA		User	- Activate Secrets Manager Resend invitations - Restore access - Revoke access - Remove
☐	FR		Owner	
☒	NE		User	Invited
☒	NE		User	Invited

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!



Join Organization Now

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, an administrator will need to [confirm](#) access. Once confirmed, you'll be notified that you can access the organization. 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:

The screenshot shows the Bitwarden web app interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. Below these are three product switcher buttons: Password Manager (selected), Secrets Manager, and Admin Console. A red circle highlights these three buttons, with a red arrow pointing to the Admin Console button. To the right of the sidebar is a 'FILTERS' panel with a search bar and a list of vaults and items. The main area displays 'All vaults' with a table of vaults. The table has columns for selection, name, and owner. The vaults listed are: Company Credit Card (owner: My Organiz...), Personal Login (owner: Me), Secure Note (owner: Me), and Shared Login (owner: My Organiz...). A 'New' button is in the top right corner.

	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**.

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

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.

Tip

For information on revoking, removing, or deleting members accounts, refer to:

- [Temporarily Revoke Access](#)
- [Permanently Remove Access](#)
- [Delete Member Accounts](#)

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.

bitwarden
Admin Console

My Organization

Collections

Members

Groups

Reporting

Billing

Settings

Members

Search members

+ Invite member

All 2

Invited

Needs confirmation

Revoked

☐ All	Name	Groups	Role	Policies	
☐	FR		Owner		
☐	JA		User		

2FA indicator