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.

## (i) Note

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

### Set a seat limit

## (i) 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:

Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS		Nama	Owner	:
🖉 Send			Name	Owner	•
$\ll$ Tools $\sim$	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
æ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	🖄 My Vault 🗐 My Organiz :	0 3	myusername	Me	:
	<ul> <li>Teams Org :</li> <li>+ New organization</li> </ul>		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>④ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>		Shared Login sharedusername	My Organiz	:
<ul> <li>Password Manager</li> <li>□ Secrets Manager</li> <li>ℬ Admin Console</li> <li>Ճ Toggle Width</li> </ul>	<ul> <li>Folders</li> <li>No folder</li> <li>Collections</li> <li>Default colle</li> <li>Default colle</li> <li>Trash</li> </ul>				
		Product s	witcher		

2. Navigate to **Billing**  $\rightarrow$  **Subscription** and check the **Limit subscription** checkbox:

<b>D bit</b> warden		Manage subscription
I My Organization	$\sim$	Adjustments to your subscription will result in prorated charges on a monthly billing cycle.
Collections		Password Manager
A Members		Subscription seats
뿅 Groups		Total: 50 × \$72.00 = \$3,600.00 / year
₽ Reporting	$\sim$	🗹 Limit subscription (optional)
Billing	^	Set a seat limit for your subscription. Once this limit is reached, you will not be able to invite new members.
Subscription		100
Payment method		Max potential seat cost: 100 × \$72.00 = \$7,200.00 / year
Billing history		Save
Settings	$\sim$	-
		Storage
		Your subscription has a total of 1 GB of encrypted file storage. You are currently using O MB
		Set a seat limit

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

#### 4. Select **Save**.

#### (i) 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

### (i) 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:

Password Manager	All vaults			New 💛 💈	BW
🗇 Vaults	FILTERS		Nama	Owner	:
🗇 Send			Name	Owner	:
$\ll$ Tools $\sim$	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	:
æ Reports	<ul> <li>✓ All vaults</li> <li>○ Manuality</li> </ul>		Personal Login		
🕸 Settings 🛛 🗸 🗸	My Vault		myusername	Me	:
	+ New organization		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>④ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>		Shared Login sharedusername	My Organiz	:
<ul> <li>☐ Password Manager</li> <li>☐ Secrets Manager</li> <li>☑ Admin Console</li> <li>☆ Toggle Width</li> </ul>	<ul> <li>Folders</li> <li>No folder</li> <li>Collections</li> <li>Default colle</li> <li>Default colle</li> <li>Trash</li> </ul>				

Product switcher

### 2. Navigate to **Billing** $\rightarrow$ **Subscription**.

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

<b>D</b> bitwarden		Manage subscription
🖉 My Organization	$\sim$	Adjustments to your subscription will result in prorated charges on a monthly billing cycle.
		Password Manager
A Members		Subscription seats 50
绺 Groups		Total: 50 × \$72.00 = \$3,600.00 / year
	$\sim$	Limit subscription (optional)
Billing	$\sim$	Set a seat limit for your subscription. Once this limit is reached, you will not be able to invite new members.
Subscription		Save
Payment method		Storage
		Add or remove seats

4. Select Save.

### (i) 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  $\rightarrow$  accept  $\rightarrow$  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 onentrance to your organization.

To invite users to your organization:

Password Manager	All vaults			New 🗸	BW
🗇 Vaults			Nome	0	
🖉 Send			Name	Owner	:
$\ll$ Tools $\sim$	Q Search vau	AZIV	Company Credit Card Visa, *4242	My Organiz	:
	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	<ul> <li>∠ My vault</li> <li>∅ My Organiz :</li> <li>∅ Toomo Org</li> </ul>		myusername	Me	:
	+ New organization		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>۞ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>	0 Ø	Shared Login sharedusername	My Organiz	÷
<ul> <li>Password Manager</li> <li>Secrets Manager</li> <li>ℬ Admin Console</li> <li>Ճ Toggle Width</li> </ul>	<ul> <li>Folders</li> <li>No folder</li> <li>Collections</li> <li>Default colle</li> <li>Default colle</li> <li>Trash</li> </ul>				

Product switcher

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

<b>D bit</b> warden	Members	Q Search members +	Invite member	BW
🕮 My Free Organizat $\checkmark$ $\hfill \frown$ Collections	All 1 Invited Needs confirmation	Revoked		
A Members	🗌 All Name 📥	Collections	Role 🔤 Policies	÷
♣ Reports ∨	BW BW	(Household Finances) (Streaming Services)	Owner	:
🗄 Billing $\checkmark$				
$\otimes$ Settings $\checkmark$				
	Invite member t	o 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.

#### (i) 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**:

<b>D bit</b> warden		Members	Q Search members	+	Invite member 🗱 🧲
My Organization Collections	$\sim$	All 4 Invited 2 Needs confirmation Revoked			
A Members		All Name 📥	Groups	Role 😂	Policies
뿅 Groups				User	Activate Secrets Manager
	$\sim$			(	🖂 Resend invitations
🛱 Billing	$\sim$			Owner	Restore access
Settings	~			User	<ul> <li>○ Revoke access</li> <li>→ Remove</li> </ul>
				User	i
		Bulk re-invite			
If you're self-hosting	g Bit	warden, you can configure the invitation expiration per	iod using an envir	onment v	ariable.

### 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:



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  $\rightarrow$  accept  $\rightarrow$  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:

Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS			Owner	
🖉 Send			10	Owner	:
$\ll$ Tools $\sim$	Q Search vau	VISA Visa,	npany Credit Card *4242	My Organiz	:
₩ Reports	✓ All vaults	Por	enel Login		
🕸 Settings 🛛 🗸 🗸	My vault My Organiz		sername	Me	:
	<ul> <li>Heams Org</li> <li>Hew organization</li> </ul>	Sec	ure Note	Me	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>④ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>	Shar	r <b>ed Login</b> edusername	My Organiz	:
	<ul> <li>✓ Folders</li> <li>☐ No folder</li> </ul>				
🔒 Password Manager	$\checkmark$ Collections				
🗔 Secrets Manager	Default colle				
🖉 Admin Console	⊡ Deradit cone ⊡ Trash				
🛱 Toggle Width					
		Product switch	er		

#### 2. Navigate to **Members**.

3. Select any Accepted users and use the  $\vdots$  options menu to  $\checkmark$  Confirm selected:

## Säker och pålitlig lösenordshanterare med öppen källkod för företag

<b>D bit</b> warden	Members	Q Search members	+ Invite member 🗱 BW
$ otin \operatorname{My} $ Free Organizat $\vee$	All 2 Invited Needs confirmation 1 Revoked		
A Members	Confirm members	and to be confirmed. Members will not have access	to the organization until those are
₩ Reports	confirmed.	need to be confirmed. Members will not have access	s to the organization until they are
🕅 Billing $\checkmark$	🗌 All Name 📥	Collections	Role 😔 Policies :
Settings	Brett Warden Betty Warden Needs confirmation	Household Finances Streaming Services Household Finances Streaming Services	<ul> <li>✓ Confirm selected</li> <li>Owner</li> <li>⊕ Restore access</li> <li>⊖ Revoke access</li> <li>User</li> <li>✓ Remove</li> </ul>

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: ⑦
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**.

#### (i) 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:

Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS		Nama	Owner	:
🖉 Send			Name	Owner	•
$\ll$ Tools $\sim$	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
켩 Reports ◎ Settings	All vaults     My vault     My Organiz :	0 9	Personal Login myusername	Me	:
	<ul> <li>Bill Teams Org :</li> <li>+ New organization</li> </ul>		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>۞ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>	0 Ø	Shared Login sharedusername	My Organiz	:
Password Manager	<ul> <li>Folders</li> <li>No folder</li> <li>Collections</li> </ul>				
<ul> <li>Secrets Manager</li> <li>Admin Console</li> <li>Toggle Width</li> </ul>	<ul> <li>Default colle</li> <li>Default colle</li> <li>Trash</li> </ul>				

Product switcher

#### 2. Navigate to Members.

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

<b>D</b> bit warden Admin Console		Members	Q Search me	mbers +	Invite member 🎆 🕅
My Organization Collections	$\sim$	All 2 Invited Needs confirmation Revoked			
A Members		All Name 🔻	Groups	Role 🔤	Policies :
뿅 Groups				Owner	Activate Secrets Manager
Reporting	$\sim$	• In the dest and			+ Restore access
🖺 Billing	$\sim$			User	<ul> <li>Revoke access</li> </ul>
③ Settings	$\sim$			(	X 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 have a claimed domain, any users with account email addresses that have a matching domain (e.g. jdoe@mycompany.com) can be outright deleted by organization administrators, instead of only being able to be removed from the organization:

### Säker och pålitlig lösenordshanterare med öppen källkod för företag

<b>D bit</b> warden	Members		+ Invite r	member 🚟 💼
☐ Claimed Org Ente ∨ ☐ Collections	All 1 Invited 2 Needs confirmation 1	Revoked 1		
A Members	🗌 All Name 📥	Groups	Role 🔤	Policies :
왕 Groups			User	C Revoke access     Delete
Billing V			User	:
☆ Integrations			User	:
ŵ Settings →	Delete claimed accou	inte		

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

3. 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**:

<b>D bit</b> warden Admin Console	Members	Q Search m	embers +	- Invite member 🗱 🕞
<ul> <li>My Organization </li> <li>Collections</li> </ul>	All 2 Invited Needs confirmation Revoked			_
△ Members	All Name 🔻	Groups	Role 😂	Policies
뿅 Groups			Owner	Activate Secrets Manager
$ arrow  ext{Reporting}  imes  imes  imes$				Restore access
🗄 Billing 🗸 🗸			User	⊖ Revoke access
$\otimes$ Settings $\checkmark$				× Remove

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.
  - If the member does not have a master password, they'll still be able to use trusted devices to login but only be able to access their individual vault.
- 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**:

### Säker och pålitlig lösenordshanterare med öppen källkod för företag

<b>D bit</b> warden	Members	Q Search m	embers	Invite member
∄ My Organization ∨	All 1 Invited Needs confirmation Revoked 1			
A Members	All Name 🔻	Groups	Role 🔤	Policies
왕 Groups			User	Activate Secrets Manager
$ agreen =  end{tabular} $ Reporting $ end{tabular} $	a the first second			Restore access
🗄 Billing 🗸 🗸				<ul> <li>Revoke access</li> </ul>
$\otimes$ Settings $\checkmark$				× Remove
	- Restore access			

Users who are not compliant with certain policies will not be able to have their access restored until they take steps to become compliant. When you restore access to a user, they don't need to go through the invite  $\rightarrow$  accept  $\rightarrow$  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.

<b>D bit</b> warden		Members	Q Search mer	mbers	+ Invite member	
My Organization Ollections	$\sim$	All 2 Invited Needs confirmation Revoked				
A Members		All Name 🔻	Groups	Role 🔤	Policies	:
뿅 Groups				Owner		:
₽ Reporting	$\sim$					
Billing	$\sim$			User	ĉ	:
Settings	$\sim$					

2FA indicator