

ADMIN CONSOLE > USER MANAGEMENT

# Account Recovery

View in the help center:  
<https://bitwarden.com/help/account-recovery/>

## Account Recovery

### Note

Account recovery is available for **Enterprise organizations**.

### What is account recovery?

Account recovery, formerly "admin password reset", allows **designated administrators** to recover enterprise organization user accounts and restore access in the event that an employee forgets their **master password**. Account recovery can be activated for an organization by **enabling the account recovery administration policy**.

Individual users must be enrolled (either through **self-enrollment** or using the **automatic enrollment policy option**) to be eligible for account recovery, as enrollment triggers the key exchange that makes recovery secure.

**Account recovery does not bypass two-step login or SSO.** If a **two-step login method** is enabled for the account or if your organization **requires SSO authentication**, you will still be required to use that method to access your vault after recovery.

### Encryption

When a member of the organization **enrolls** in account recovery, that user's **encryption key** is encrypted with the organization's public key. The result is stored as the **Account Recovery Key**.

When an recovery action is taken:

1. The organization private key is decrypted with the organization symmetric key.
2. The user's **Account Recovery Key** is decrypted with the decrypted organization private key, resulting in the users's **encryption key**.
3. The user's encryption key is encrypted with a new master key and a new master password hash is seeded from the new master password, both the master key-encrypted encryption key and master password has replace pre-existing server-side values
4. The user's encryption key is encrypted with the organization's public key, replacing the previous **Account Recovery Key** with a new one.

**At no point** will anyone, including the administrator who executes the reset, be able to see the old master password.

### Permissions

Account recovery can be executed by **owners, admins, and permitted custom users**. Account recovery uses a hierarchical permission structure to determine who can reset whose master password, meaning:

- Any owner, admin, or permitted custom user can reset a user, manager, or custom user's master password.
- Only an admin or owner can reset an admin's master password.
- Only an owner can reset another owner's master password.

### Event logging

**Events** are logged when:

- A master password is reset using account recovery.
- A user updates a password issued through account recovery.
- A user enrolls in account recovery.
- A user withdraws from account recovery.

## Activate account recovery

To activate account recovery for your enterprise organization, open the Admin Console using the product switcher:

The screenshot shows the Bitwarden Admin Console interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager (highlighted with a red circle), Secrets Manager, Admin Console, and Toggle Width. The main content area is titled 'All vaults' and features a 'New' button, a QR code icon, and a 'BW' profile icon. Below the title is a 'FILTERS' panel with a search bar and a list of categories: All vaults, All items, Folders, Collections, and Trash. The 'All vaults' list contains five entries: Company Credit Card, Personal Login, Secure Note, and Shared Login, each with a checkbox, an icon, a name, an owner, and a menu icon.

| <input type="checkbox"/> | All | Name                                      | Owner         |   |
|--------------------------|-----|---|---------------|---|
| <input type="checkbox"/> |     | <b>Company Credit Card</b><br>Visa, *4242 | My Organiz... | ⋮ |
| <input type="checkbox"/> |     | <b>Personal Login</b><br>myusername       | Me            | ⋮ |
| <input type="checkbox"/> |     | <b>Secure Note</b>                        | Me            | ⋮ |
| <input type="checkbox"/> |     | <b>Shared Login</b><br>sharedusername     | My Organiz... | ⋮ |

Product switcher

In the Admin Console, navigate to **Settings** → **Policies** and turn on the **Account recovery administration** policy. You must be at least an organization admin to activate this policy:

The screenshot shows the Bitwarden Admin Console interface. On the left is a navigation sidebar with items: My Organization, Collections, Members, Groups, Reporting, Billing, Settings, Organization info, Policies (highlighted), Two-step login, and Import data. The main content area is titled 'Policies' and lists several settings: 'Require two-step login', 'Master password requirements', 'Account recovery administration', 'Password generator', 'Single organization', and 'Require single sign-on authentication'. Each policy has a brief description. At the bottom of the main area is a 'Set policies' button.

Users will need to [self-enroll](#) or [be auto-enrolled](#) in account recovery before their master password can be reset.

## Automatic enrollment

Enabling the automatic enrollment policy option will automatically enroll new users in account recovery when their [invitation to the organization is accepted](#) and will prevent them from [withdrawing](#) from account recovery.

Users already in the organization will not be retroactively enrolled in account recovery and will be required to [self-enroll](#).

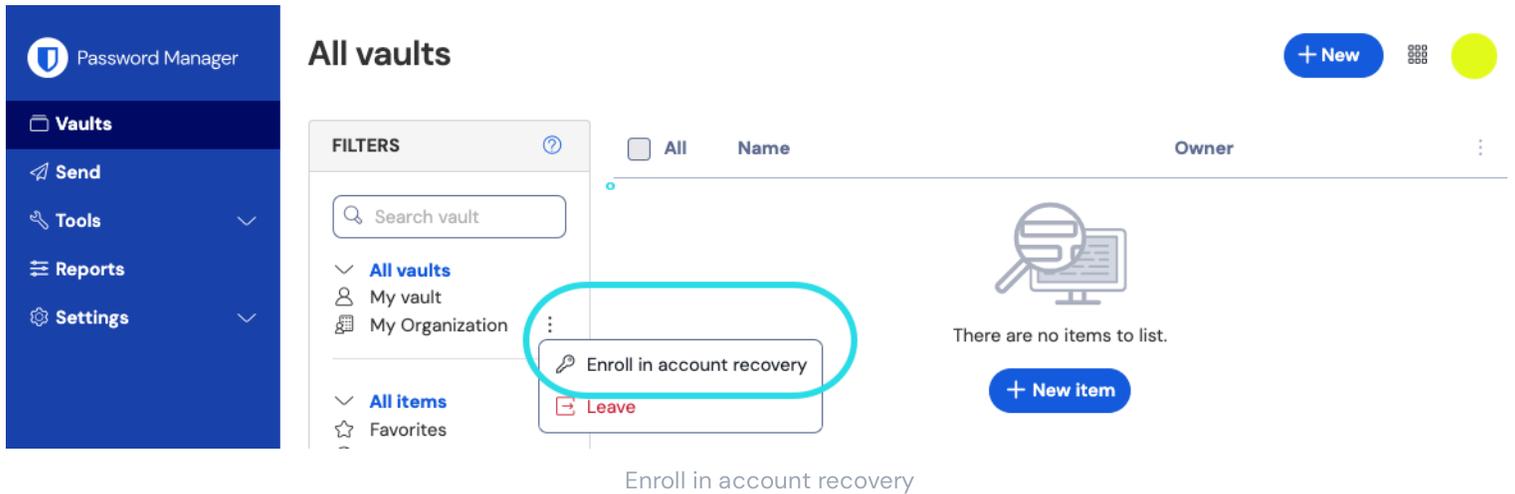


### Tip

If you are automatically enrolling organization members in account recovery, we **highly recommend notifying them of this feature**. Many Bitwarden organization users store personal credentials in their individual vault, and should be made aware that account recovery could allow an administrator to access their individual vault data.

## Self-enroll in account recovery

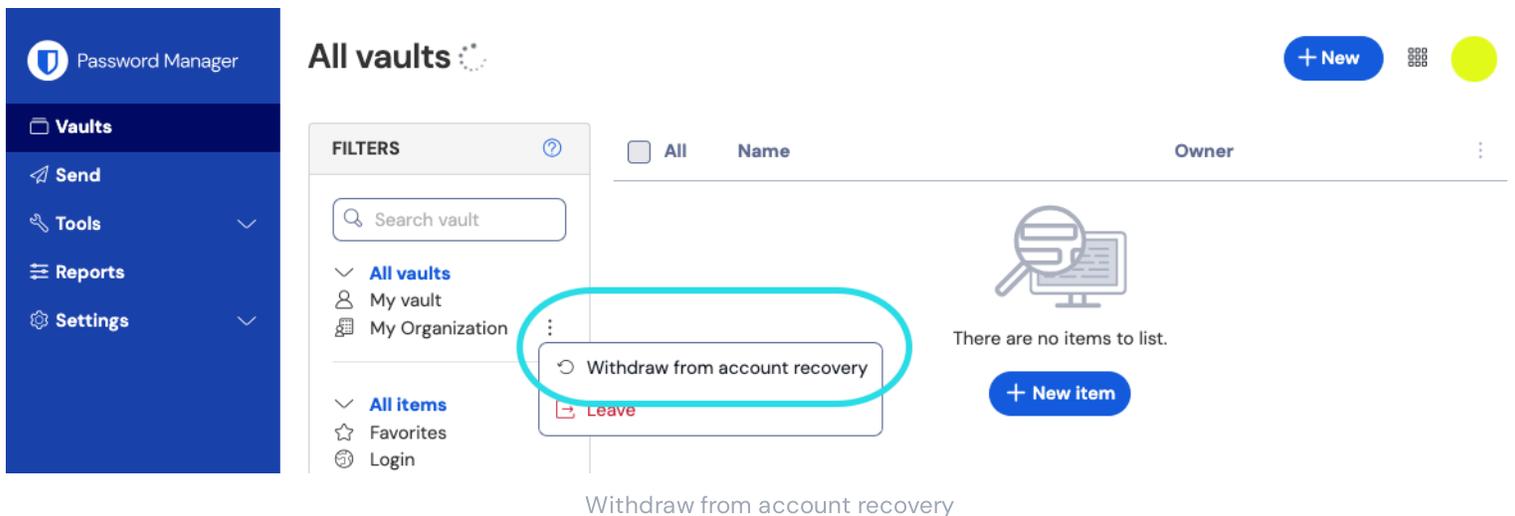
To enroll in account recovery, select the **Options** menu next to your organization in the Vaults view and select **Enroll in account recovery**:



You can enroll in account recovery for multiple organizations, if you choose.

## Withdraw enrollment

Once enrolled, you can **Withdraw** from account recovery from the same dropdown used to enroll:



Users in organizations that have enabled the [automatic enrollment](#) policy option **will not be allowed to withdraw** from account recovery. Additionally, manually changing your master password or [rotating your encryption key](#) **will not** withdraw you from account recovery.

## Recover an account

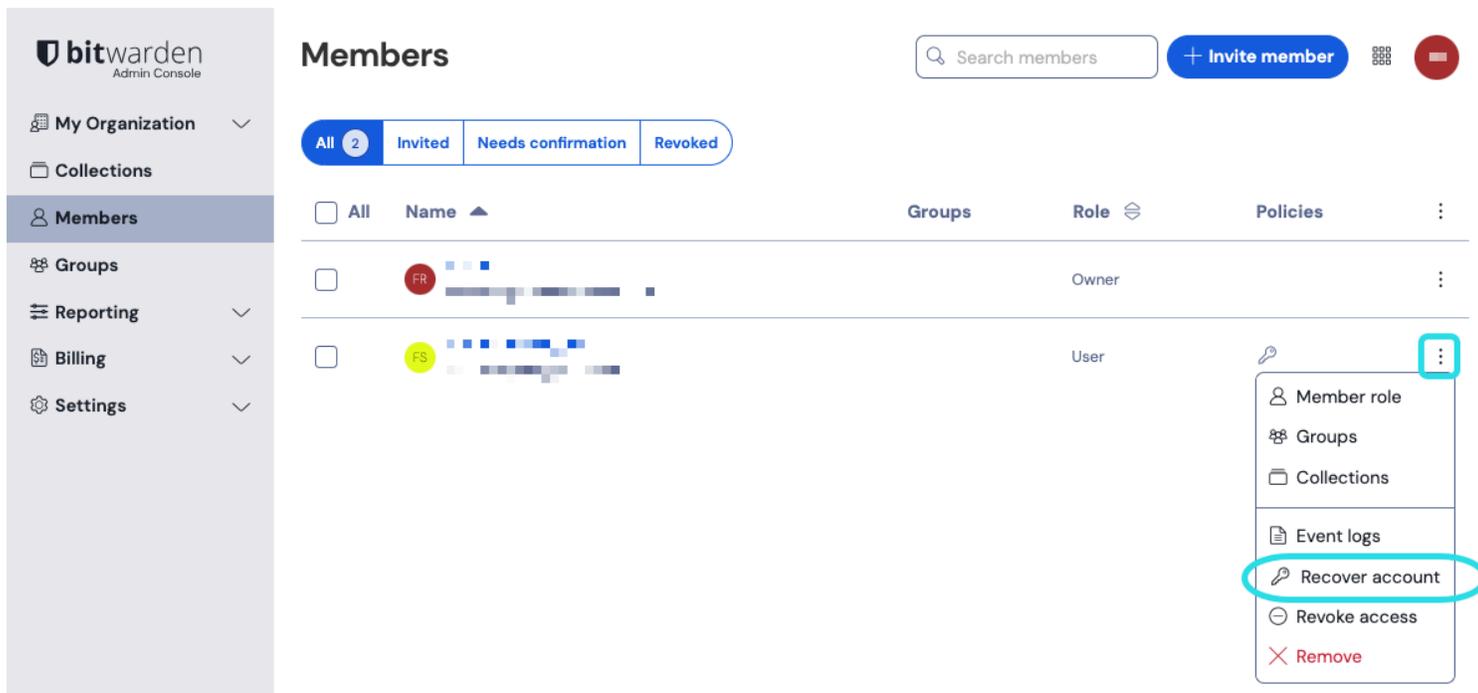
### Note

You must be an [owner](#), [admin](#), or [permitted custom user](#) to reset a master password. Check the [permissions](#) section of this article to see whose master password you are allowed to reset.

To recover the account of a member of your Enterprise organization:

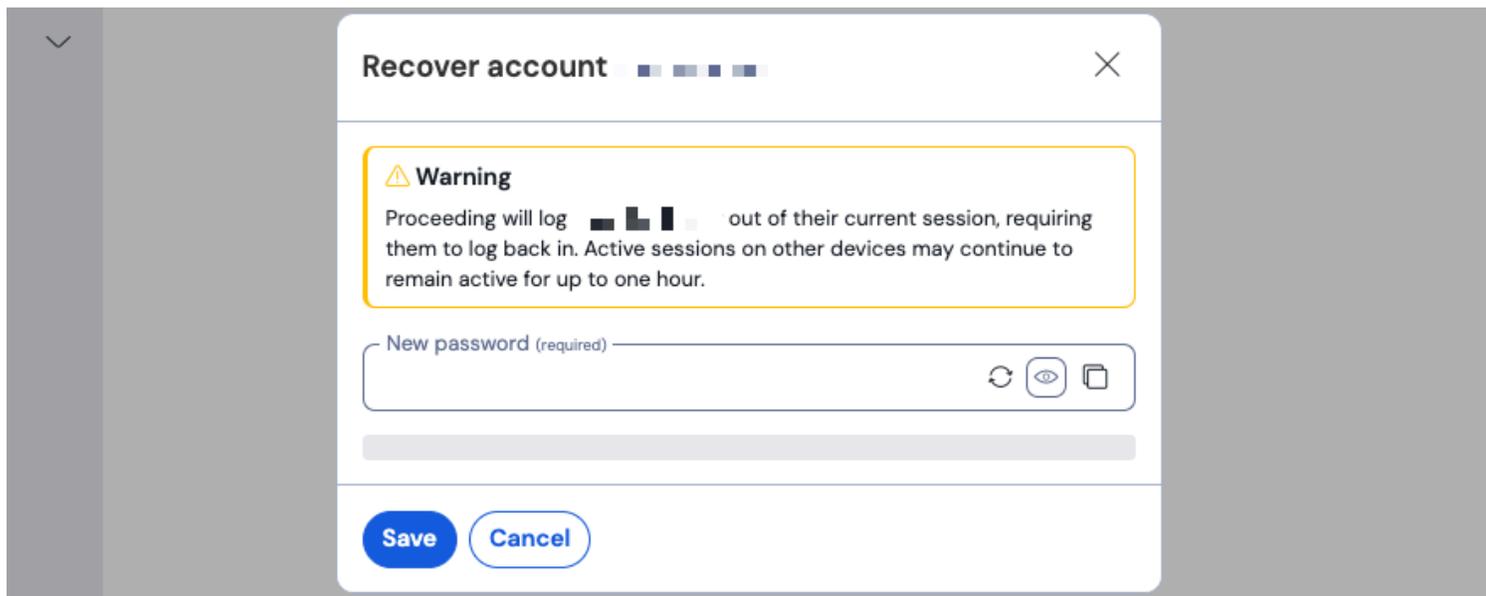
1. In the Admin Console, navigate to **Members**.

2. For the member whose master password you want to reset, use the Options menu to select **Recover account**:



Recover account

3. On the Recover Account window, create a **New password** for the user. If your organization has enabled the [master password requirements policy](#), you will need to create a password that meets the implemented requirements (for example, min. eight characters, contains numbers):



Create new password

Copy the new master password and contact the user to coordinate secure communication of it, for example by using [Bitwarden](#)

[Send](#).

4. Select **Save** to execute account recovery. Doing so will log the user out of their current sessions. Active sessions on some client applications, like mobile apps, may remain active for up to one hour.

### After a recovery

When your master password is reset, you will receive an email from Bitwarden to inform you of this. On receiving this email, contact your organization administrator to obtain your new master password through a secure channel like [Bitwarden Send](#).

Once you have regained access to your vault using the new master password, you will be prompted to update your master password again:

#### Update Master Password

**⚠ WARNING**

Your Master Password was recently changed by an administrator in your organization. In order to access the vault, you must update your Master Password now. Proceeding will log you out of your current session, requiring you to log back in. Active sessions on other devices may continue to remain active for up to one hour.

**Master Password**

.....

Strong

**Re-type Master Password**

.....

**Master Password Hint (optional)**

A master password hint can help you remember your password if you forget it.

**Submit**Log Out

Update your Master Password

You are required to update your master password after a reset because a master password should be **strong, memorable**, and something **only you** know.