

MY ACCOUNT > MORE

Emergency Access

A decorative graphic consisting of numerous thin, light blue wavy lines that create a sense of motion and depth across the middle section of the page.

Weergeven in het Helpcentrum:
<https://bitwarden.com/help/emergency-access/>

Emergency Access

Emergency access allows users to designate and manage [trusted emergency contacts](#), who can request access to their vault in cases of emergency.

Note

Only premium users, including members of paid organizations (Families, Teams, or Enterprise) can designate trusted emergency contacts, however anyone with a Bitwarden account can be designated as a trusted emergency contact.

If your premium features are cancelled or lapse due to failed payment method, your trusted emergency contacts will still be able to request and obtain access to your vault. You will, however, not be able to add new or edit existing trusted emergency contacts.

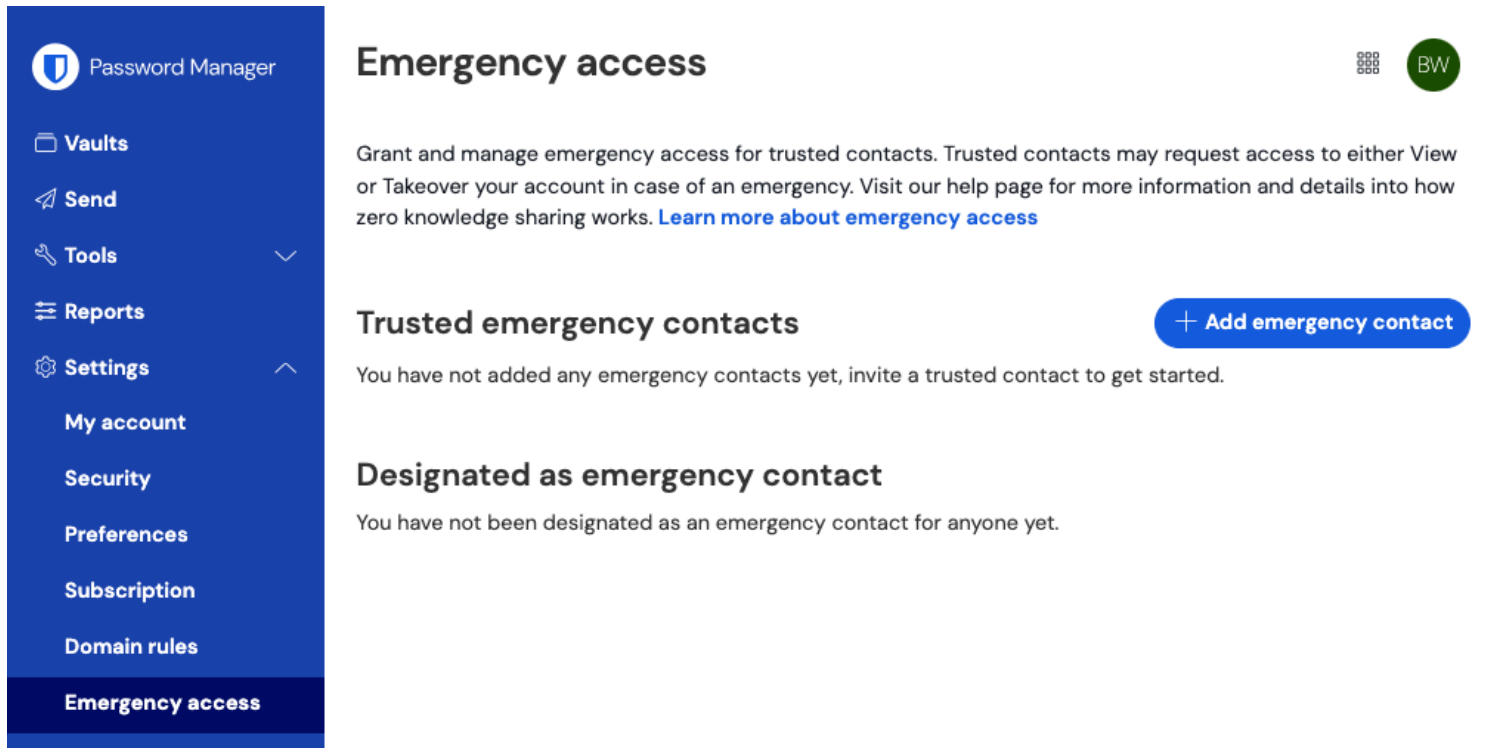
Set up emergency access

Setting up emergency access is a 3-step process in which you must **Invite** a user to become a trusted emergency contact, they must **Accept** the invitation, and finally you must **Confirm** their acceptance:

⇒Invite

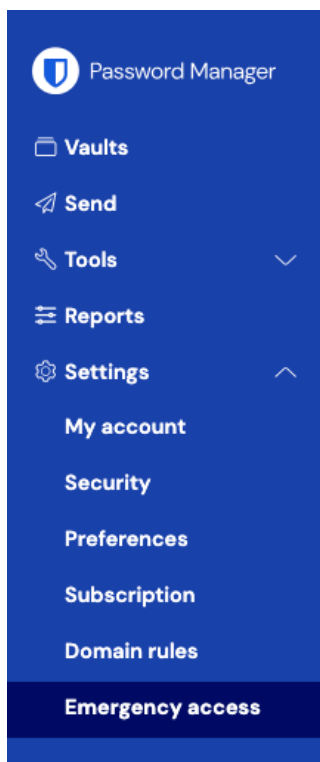
As someone who wants to grant emergency access to your vault, invite a trusted emergency contact:

1. In the Bitwarden web app, navigate to **Settings** → **Emergency access**:



Emergency access page

2. Select the **+ Add emergency contact** button:



Emergency access

Grant and manage emergency access for trusted contacts. Trusted contacts may request access to either View or Takeover your account in case of an emergency. Visit our [help page](#) for more information and details into how zero knowledge sharing works. [Learn more about emergency access](#)

Trusted emergency contacts



Name	Access level	Options
  Invited	View	⋮

Designated as emergency contact

You have not been designated as an emergency contact for anyone yet.

Add emergency contact

3. Enter the **Email** of your trusted emergency contact. Trusted emergency contacts must have Bitwarden accounts of their own, but don't need to have premium.
4. Set a **User Access** level for the trusted emergency contact ([View-only](#) or [Takeover](#)).
5. Set a **Wait time** for vault access. Wait time dictates how long your trusted emergency contact must wait to access your vault after initiating an emergency access request.
6. Select the **Save** button to send the invitation.

Your trusted emergency contact **must now accept the invitation**.

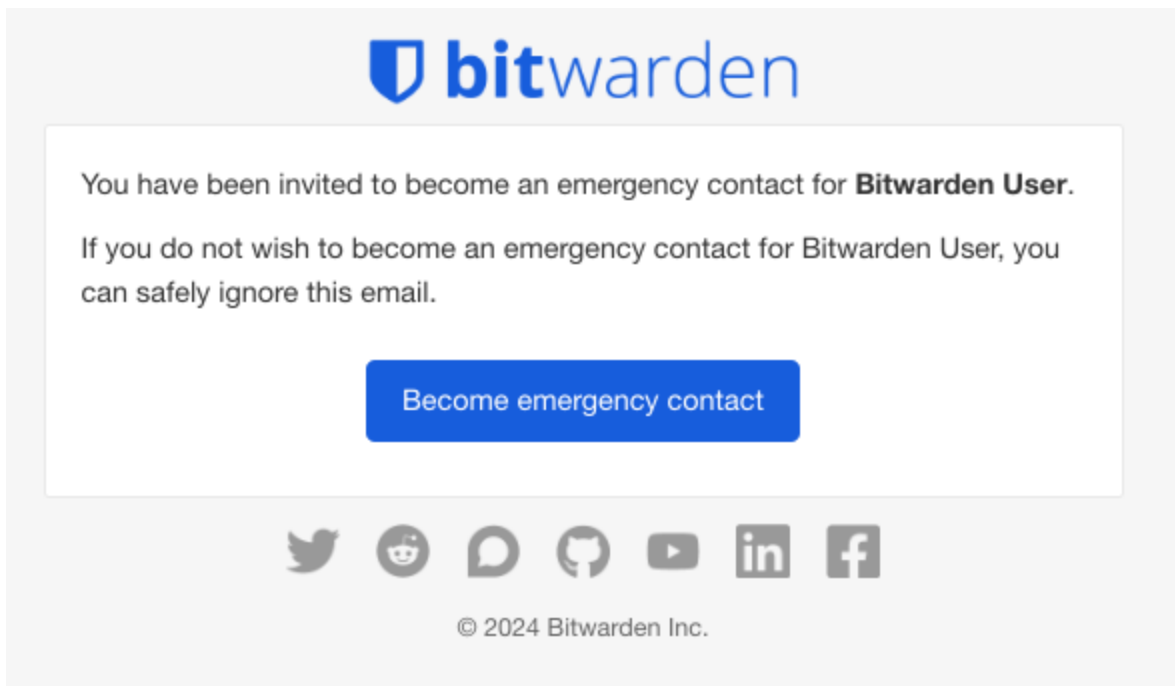
Note

Invitations to become a trusted emergency contact are only valid for five days.

⇒Accept

As someone who wants to receive emergency access to another vault, accept the issued email invitation:

1. In the received email invitation, select the **Become emergency contact** button in the email to open an emergency access page in your browser:



Emergency access invitation

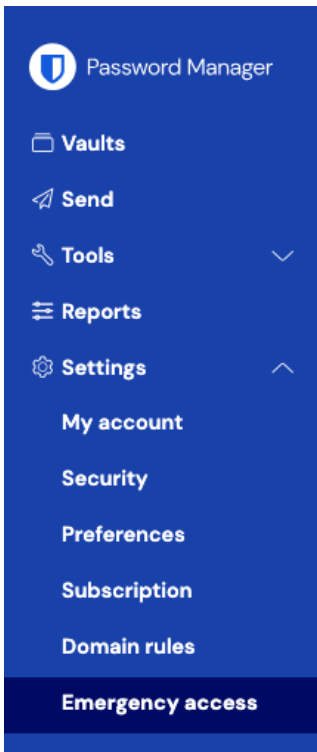
2. Log in to your Bitwarden account to accept the invitation. If you don't already have a Bitwarden account, you will need to create one.

Once you have accepted the invitation, the inviting user **must confirm your acceptance** before you can [initiate access requests](#).

⇒ **Confirm**

As someone who wants to grant emergency access to your vault, confirm your new trusted emergency contact:

1. In the Bitwarden web app, navigate to **Settings** → **Emergency access**:



Emergency access



Grant and manage emergency access for trusted contacts. Trusted contacts may request access to either View or Takeover your account in case of an emergency. Visit our [help page](#) for more information and details into how zero knowledge sharing works. [Learn more about emergency access](#)

Trusted emergency contacts

[+ Add emergency contact](#)

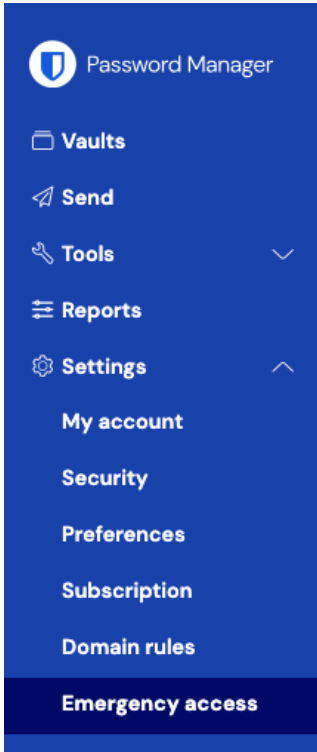
You have not added any emergency contacts yet, invite a trusted contact to get started.

Designated as emergency contact

You have not been designated as an emergency contact for anyone yet.

Emergency access page

2. In the **Trusted emergency contacts** section, the invited user should appear with a **Needs Confirmation** status card. Using the **:** menu, select **Confirm** from the dropdown menu:




Emergency access



Grant and manage emergency access for trusted contacts. Trusted contacts may request access to either View or Takeover your account in case of an emergency. Visit our [help page](#) for more information and details into how zero knowledge sharing works. [Learn more about emergency access](#)

Trusted emergency contacts

[+ Add emergency contact](#)

Name	Access level	Options
 [Redacted Name] Needs confirmation	View	<ul style="list-style-type: none">ConfirmRemove

Designated as emergency contact

You have not been designated as an emergency contact for anyone yet.

Confirm emergency contact

To ensure the integrity of your encryption keys, verify the displayed fingerprint phrase with the grantee before completing confirmation.

Use emergency access

Once [setup](#), the following sections will help you **Initiate access** as a trusted emergency contact or **Manage access** as someone who has designated a trusted emergency contact:

💡 Tip

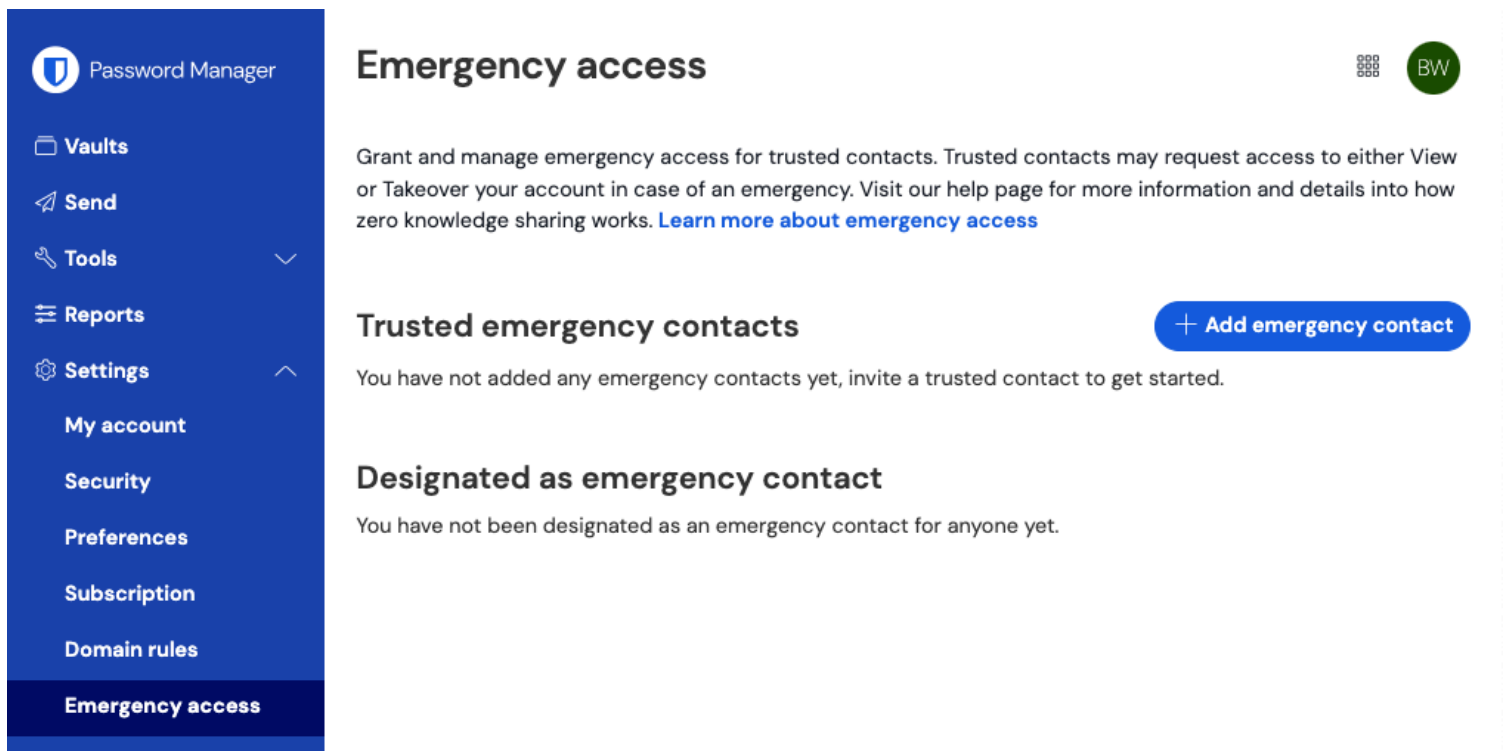
The following **Manage access** tab also contains information about what to do when you no longer want your trusted emergency contacts to have View or Takeover access to your vault.

⇒ Initiate access

Initiate emergency access

Complete the following steps to initiate an emergency access request:

1. In the Bitwarden web app, navigate to **Settings** → **Emergency access**:



Emergency access page

2. In the **Designated as emergency contact** section, select the menu icon and choose **Request Access**:

Password Manager

- Vaults
- Send
- Tools
- Reports
- Settings
- My account
- Security
- Preferences
- Subscription
- Domain rules
- Emergency access**

Emergency access




Grant and manage emergency access for trusted contacts. Trusted contacts may request access to either View or Takeover your account in case of an emergency. Visit our [help page](#) for more information and details into how zero knowledge sharing works. [Learn more about emergency access](#)

Trusted emergency contacts Premium

[+ Add emergency contact](#)

You have not added any emergency contacts yet, invite a trusted contact to get started.

Designated as emergency contact

Name	Access level	Options
 [Redacted Name]	View	Request Access Remove

Request emergency access

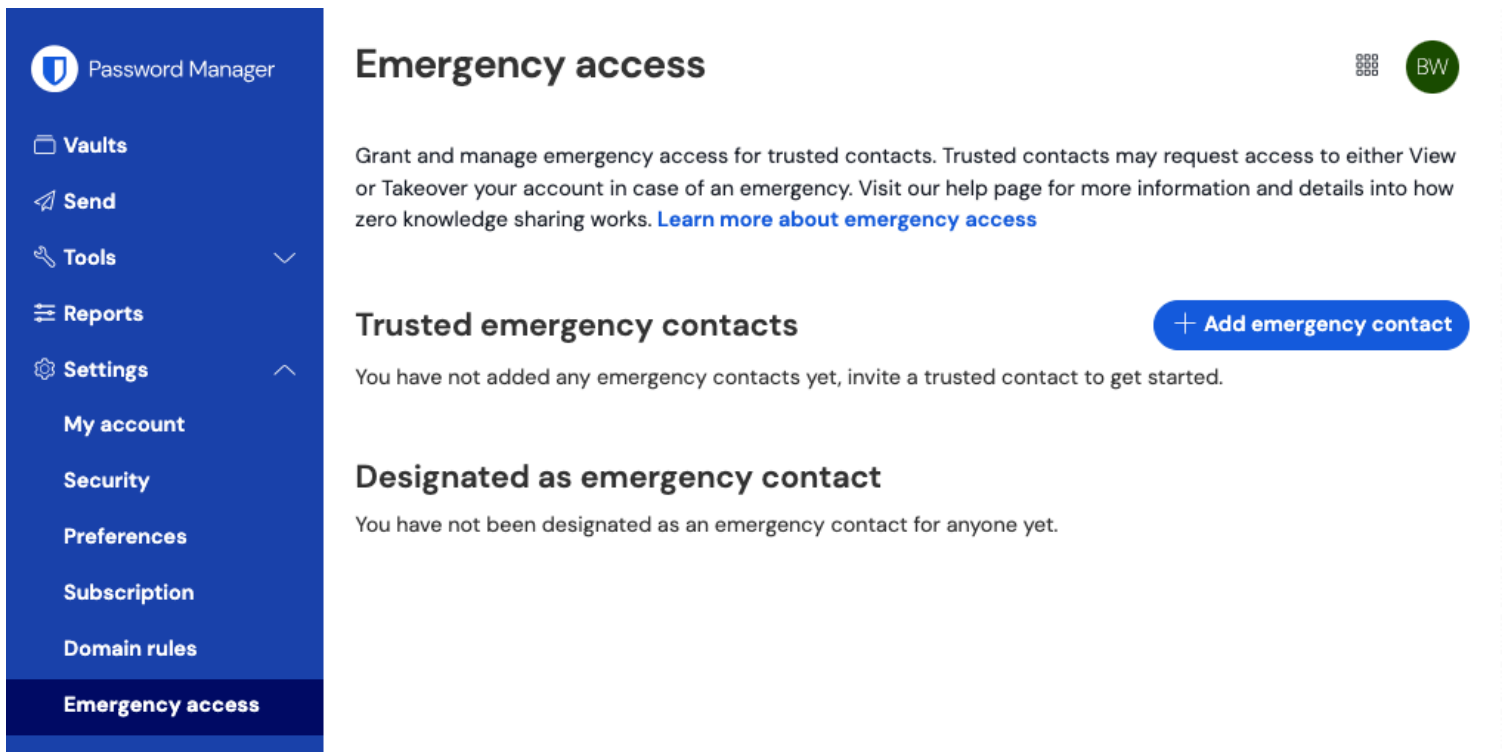
3. In the confirmation window, select the **Request Access** button.

You will be provided access to the grantor's vault after the configured wait time, or when the grantor manually approves (see **Manage access** tab) the emergency access request.


Access the vault

Complete the following steps to access the vault once your request has been approved:

1. In the Bitwarden web app, navigate to **Settings** → **Emergency access**:



Emergency access page

2. In the **Designated as emergency contact** section, select the  menu icon and choose the option from the dropdown that corresponds with your [assigned access](#):

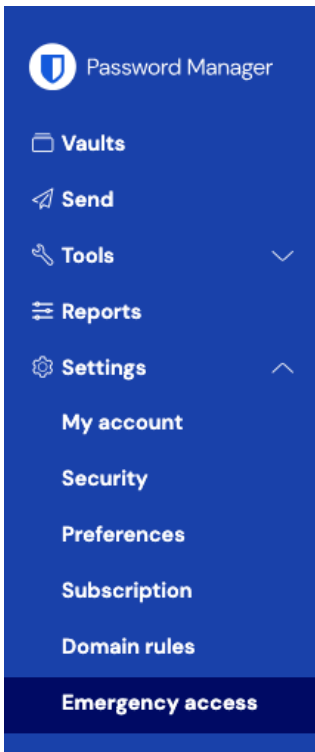
- **View** – Selecting this option will display the grantor's vault items on this screen.
- **Takeover** – Selecting this option will allow you to enter and confirm a new master password for the grantor's account. Once saved, log in to Bitwarden as normal, entering the grantor's email address and the new master password.

⇒Manage access

Approve or reject emergency access

You can manually approve or reject an emergency access request before the configured wait time lapses. Complete the following steps to approve or reject emergency access:

1. In the Bitwarden web app, navigate to **Settings** → **Emergency access**:



Emergency access



Grant and manage emergency access for trusted contacts. Trusted contacts may request access to either View or Takeover your account in case of an emergency. Visit our [help page](#) for more information and details into how zero knowledge sharing works. [Learn more about emergency access](#)

Trusted emergency contacts

[+ Add emergency contact](#)

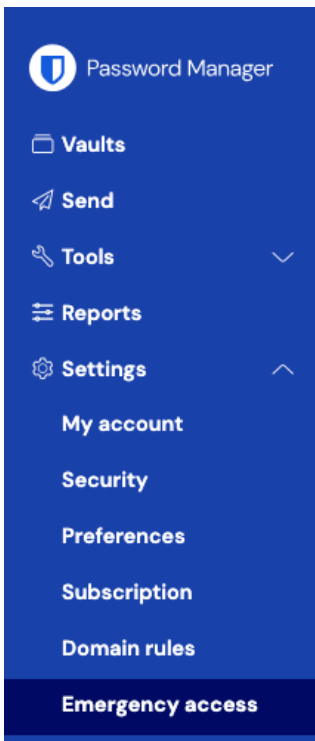
You have not added any emergency contacts yet, invite a trusted contact to get started.

Designated as emergency contact

You have not been designated as an emergency contact for anyone yet.

Emergency access page

2. In the **Trusted emergency contacts** section, use the  menu icon to select **Approve** or **Reject**:






Emergency access



Grant and manage emergency access for trusted contacts. Trusted contacts may request access to either View or Takeover your account in case of an emergency. Visit our [help page](#) for more information and details into how zero knowledge sharing works. [Learn more about emergency access](#)

Trusted emergency contacts

[+ Add emergency contact](#)

Name	Access level	Options
  Emergency access initi...	View	 <ul style="list-style-type: none">✓ Approve✗ Reject✗ Remove

Designated as emergency contact

You have not been designated as an emergency contact for anyone yet.

Approve or reject emergency access

Revoking access

The steps to take to regain exclusive access to your vault after using emergency access depend on which [access level](#) was granted:

Revoke view access

Trusted emergency contacts who are given **View** access will be able to view your vault items once they are approved and until their access is manually revoked. To manually revoke access, use the menu to **Reject** access:

Emergency access

Grant and manage emergency access for trusted contacts. Trusted contacts may request access to either View or Takeover your account in case of an emergency. Visit our help page for more information and details into how zero knowledge sharing works. [Learn more about emergency access](#)

Trusted emergency contacts + Add emergency contact

Name	Access level	Options
Emergency access app...	View	 Reject Remove

Designated as emergency contact

You have not been designated as an emergency contact for anyone yet.

Revoke Emergency Access

Revoke a takeover

Trusted emergency contacts who are given **Takeover** access will, once used, have created a new master password for your account. As a result, the only way to revoke access involves:

1. Obtaining the new master password they created for your account and using it to log in the [web vault](#).
2. [Changing your master password](#) to one that they do not know.

More information

Trusted emergency contacts

Trusted emergency contacts must be existing Bitwarden users, or must create a Bitwarden account before they can accept an invitation. Trusted emergency contacts do not need to have premium to be designated as such.

A user's status as a trusted emergency contact is tied to a unique Bitwarden account ID, meaning that if a trusted emergency contact [changes their email address](#) there is no reconfiguration required to maintain their emergency access. Likewise, if the emergency access grantor changes their email address, no reconfiguration is required.

If a trusted emergency contact creates a new Bitwarden account and [deletes](#) the old account, they will automatically be removed as a trusted emergency contact and must be [re-invited](#).

There is no limit to the number of trusted emergency contacts a user can have.

💡 Tip

You can [reject](#) an emergency access request by your trusted emergency contact at any time before the configured wait time lapses.

User access

Trusted emergency contacts can be granted one of the following user access levels:

- **View:** When an emergency access request is granted, this user is granted view/read access to all items in your individual vault, including passwords of login items and attachments.

💡 Tip

You may [revoke access](#) to a trusted emergency contact with view access at any time.

- **Takeover:** When an emergency access request is granted, this user must create a master password for permanent read/write access to your vault (this will **replace** your previous master password). Takeover disables any [two-step login methods](#) enabled for the account.

If the grantor is a member of an organization, the grantor will be automatically removed from any organization(s) for which they are not an [owner](#) on takeover. Owners will not be removed from or lose permissions to their organization(s), however the [master password requirements](#) policy will be enforced on takeover if enabled. Policies that are not usually enforced on owners will not be enforced on takeover.

How it works

📌 Note

The following information references encryption key names and processes that are covered in the [Hashing, key derivation, and encryption](#) section. Consider reading that section first.

Emergency access uses public key exchange and encryption/decryption to allow users to give a [trusted emergency contact](#) permission to [access vault data](#) in a zero knowledge encryption environment:

1. A Bitwarden user (the grantor) invites another Bitwarden user to become a trusted emergency contact (the grantee). The invitation (valid for only five days) specifies a user access level and includes a request for the grantee's **RSA Public Key**.
2. Grantee is notified of the invitation via email and accepts the invitation to become a trusted emergency contact. On acceptance, the grantee's **RSA Public Key** is stored with the user record.
3. Grantor is notified of the invitation's acceptance via email and confirms the grantee as their trusted emergency contact. On confirmation, the grantor's **User Symmetric Key** is encrypted using the grantee's **RSA Public Key** and stored with the invitation. Grantee is notified of confirmation.
4. An emergency occurs, resulting in grantee requiring access to grantor's vault. Grantee submits a request for emergency access.

5. Grantor is notified of the request via email. The grantor may manually approve the request at any time, otherwise the request is bound by a grantor-specified wait time. When the request is approved or the wait time lapses, the **Public Key-encrypted User Symmetric Key** is delivered to the grantee for decryption with the grantee's **RSA Private Key**.

Alternatively, the grantor may reject the request, which will prevent the grantee gaining access as described in the next step. Rejecting a request will not remove the grantee from being a trusted emergency contact or prevent them from making access requests in the future.

6. Depending on the specified user access level, the grantee will either:

- Obtain view/read access to items in the grantor's vault.
- Be asked to create a new master password for the grantor's vault.