HELP CENTER

Emergency Access

bitwarden

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 lapses 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.

How it works

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 public key.
2. Grantee is notified of invitation via email and accepts the invitation to become a trusted emergency contact. On acceptance, the grantee's public key is stored with the invite.
3. Grantor is notified of acceptance via email and confirms the grantee as their trusted emergency contact. On confirmation, the grantor's master key is encrypted using the grantee's public key and stored once encrypted. 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 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 master key is delivered to grantee for decryption with grantee's private key.
6. Depending on the specified user access level, the grantee will either:
   - Obtain view/read access to items in the grantor's vault (**view**).
   - Be asked to create a new master password for the grantor's vault (**takeover**).

Trusted emergency contacts

Trusted emergency contacts must be existing Bitwarden users, or will be asked to 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. 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.

> **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 can 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.

Setup emergency access

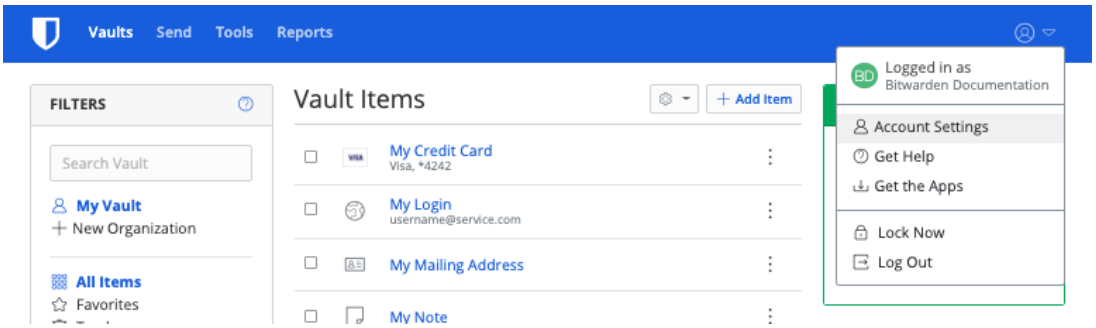
The following sections will walk you setting up emergency access, separated by whether you want to **Give access** to your vault or **Receive access** to another user's vault:

⇒Give access

Invite a trusted emergency contact

To invite a trusted emergency contact for your vault:

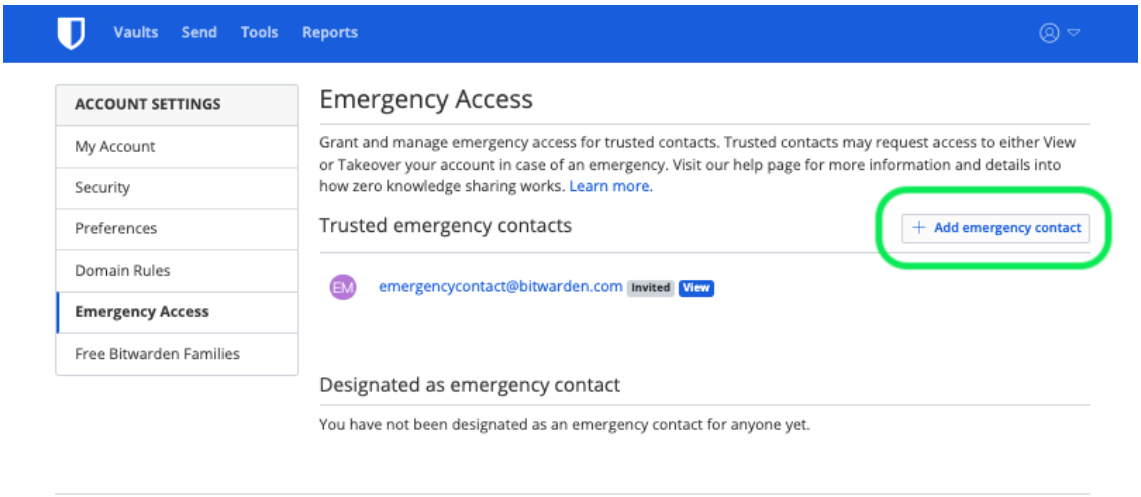
1. In the web vault, select the profile icon and choose **Account Settings** from the dropdown:



Account Settings

2. From the Account Settings menu, select **Emergency Access**.

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



Add emergency contact

4. 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.

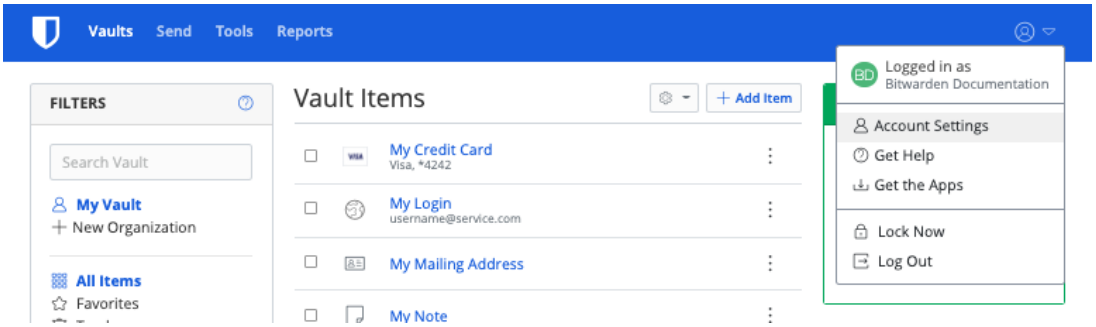
5. Set a **User Access** level for the trusted emergency contact (View-only or Takeover).
6. Set a **Wait Time** for vault access. Wait time dictates how long your trusted emergency contact must wait to access your vault after initiating an emergency access request.
7. Select the **Save** button to send the invitation. Your trusted emergency contact must now accept the invitation (see **Receive access** tab).

> **Note**
>
> Invitations to become a trusted emergency contact are only valid for 5 days.

Confirm an accepted invitation

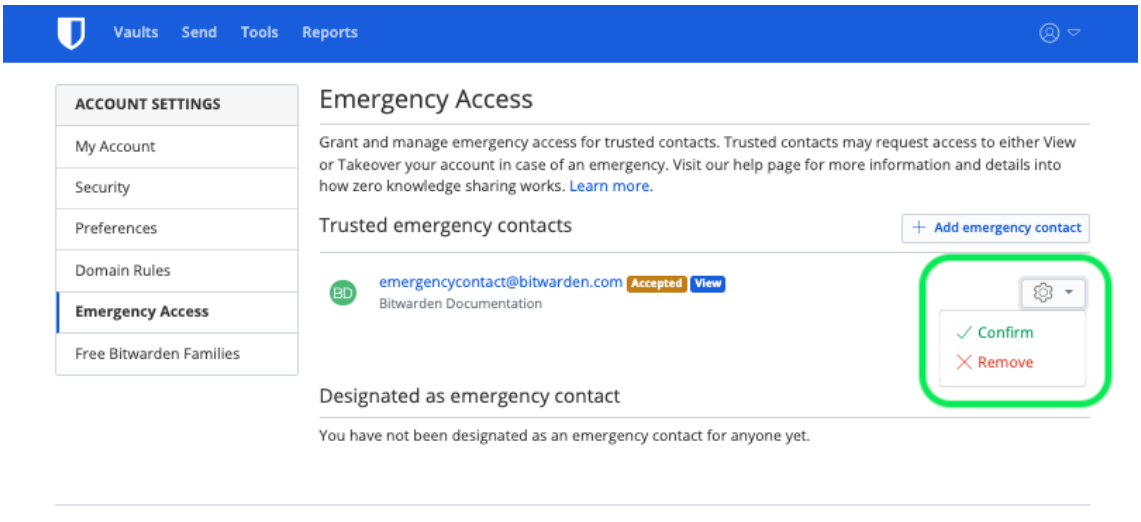
Once your trusted emergency contact has accepted the invitation, complete the following steps to confirm:

1. In the web vault, select the profile icon and choose **Account Settings** from the dropdown:



Account Settings

2. From the Account Settings menu, select **Emergency Access**. In the **Trusted emergency contacts** section, the invited user should appear with an `Accepted` status card.
3. Hovering over the user, select the gear icon and select **Confirm** from the dropdown menu.



Confirm Emergency Contact

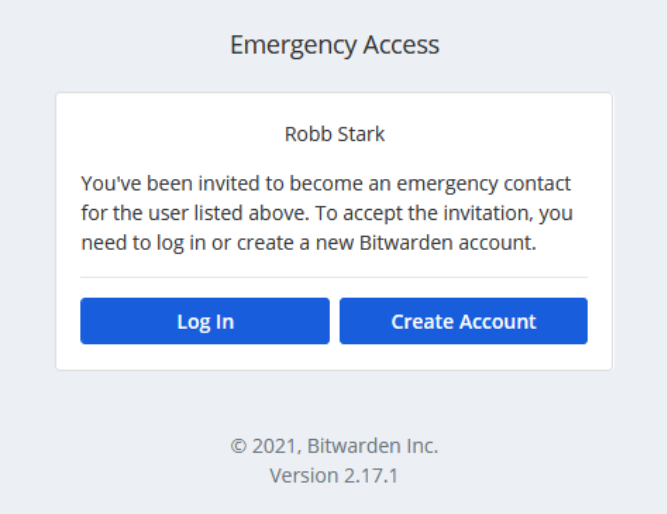
To ensure the integrity of your encryption keys, verify the displayed fingerprint phrase with the grantee before completing confirmation.

⇒Receive access

Accept an invitation

Complete the following steps to accept an invitation to become a trusted emergency contact:

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 (see **Give access** tab).

Use Emergency Access

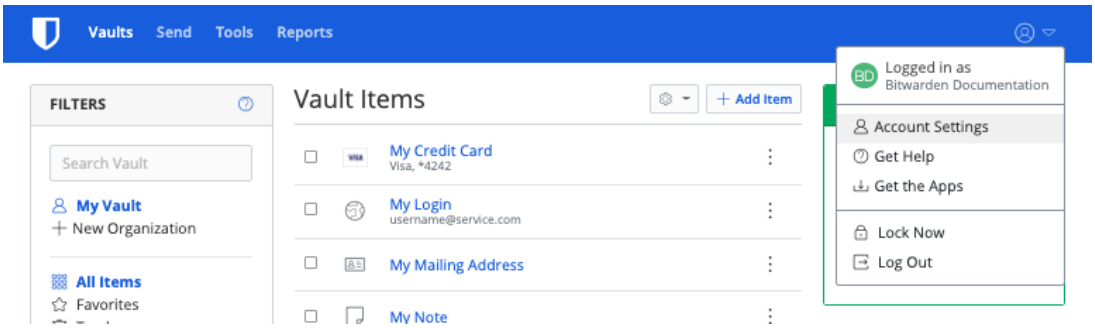
Once setup, the following sections will help you **Initiate access** as a trusted emergency contact or **Manage access** as someone who has designated a trusted emergency contact:

⇒Initiate access

Initiate emergency access

Complete the following steps to initiate an emergency access request:

1. In to the web vault, select the profile icon and choose **Account Settings** from the dropdown:

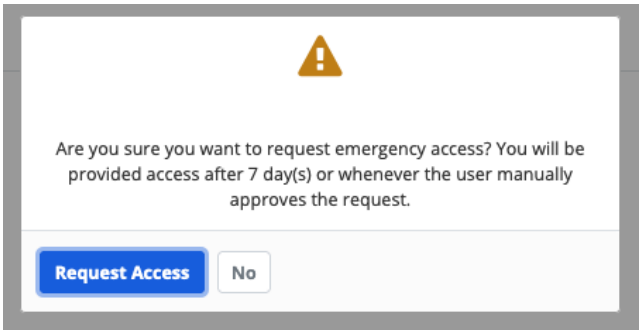


Account Settings

2. From the Account Settings menu, select **Emergency Access**.

3. In the **Designated as emergency contact** section, select the ⚙ gear icon and choose **Request Access**.

4. In the request access window, select the **Request Access** button.



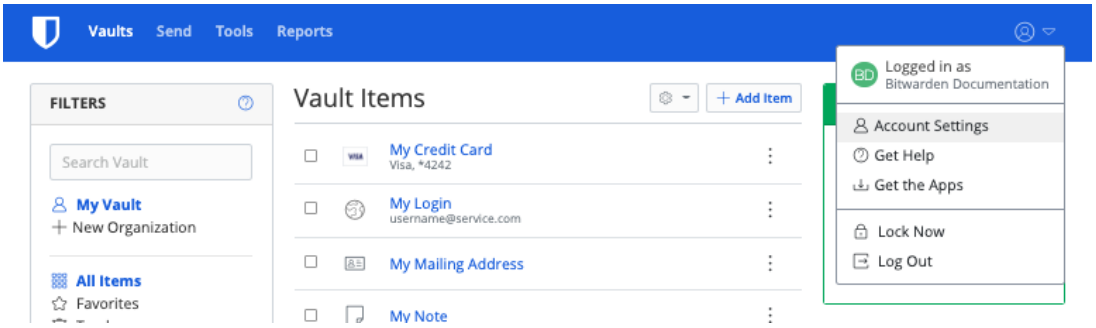
Request Access

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 web vault, select the profile icon and choose **Account Settings** from the dropdown:



Account Settings

2. From the Account Settings menu, select **Emergency Access.**
3. In the **Designated as emergency contact** section, hover over the person whose vault you want to access, and select the ⚙ gear icon.
4. Select the option from the dropdown that corresponds with your assigned access:

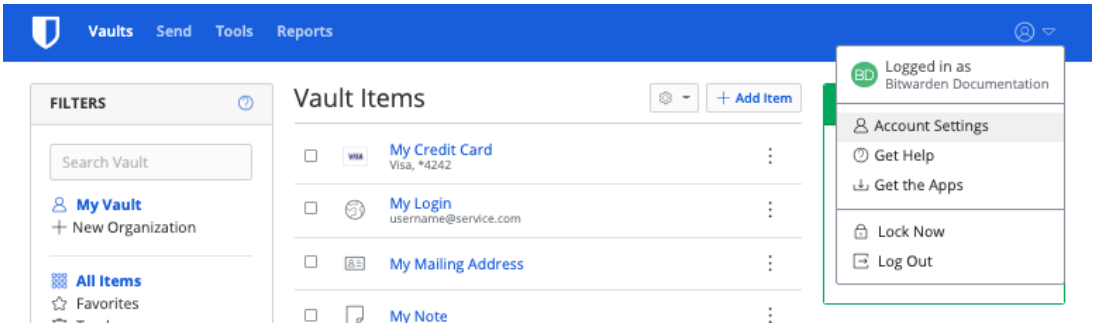
- **View** - Selecting this option will display the grantor's vault items on this screen.
- **Takeover** - Selecting this option will allow you to enter and confirm a new master password for the grantor's account. Once saved, log in to Bitwarden as normal, entering the the grantor's email address and 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 web vault, select the profile icon and choose **Account Settings** from the dropdown:



Account Settings

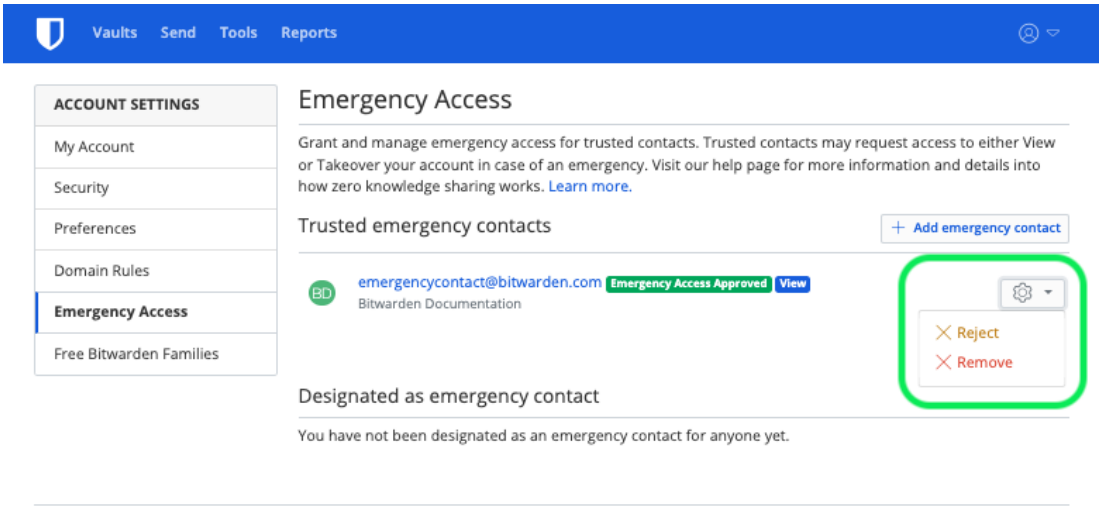
2. From the Account Settings menu, select **Emergency Access.**
3. Hovering over the user with the `Emergency Access Initiated` status card, select the gear icon.
4. From the gear dropdown, select **Approve** or **Reject**.

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 ⚙ **gear** dropdown to ✕ **Reject** access:



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.