

Vaultwarden

Password & authentication code manager for CBTS accounts. Shared accounts are managed through Vaultwarden.

- [What is Vaultwarden?](#)
- [1. Creating Your Vaultwarden Account](#)
- [2. Next Steps](#)
- [Logging in to the Browser Extension](#)
- [Adding 2FA \(TOTP/Authenticator\) codes to Vaultwarden](#)
- [Can't Login on the Bitwarden Extension](#)

What is Vaultwarden?

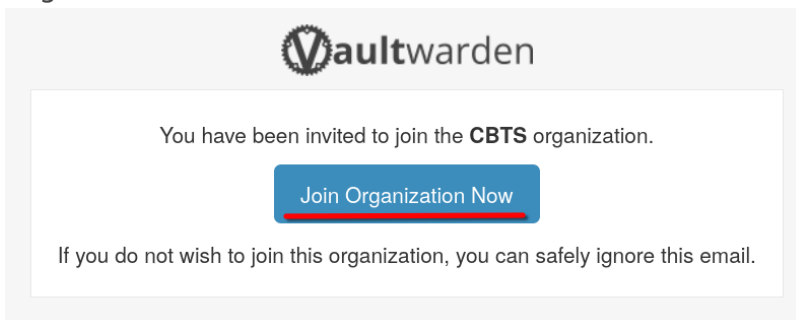
Vaultwarden is CBTS's internal password manager that allows users to store, manage, and share sensitive information (such as passwords, TOTP keys, passkeys, notes, etc) securely.

We will use it primarily as a password manager for shared accounts/passwords, but also recommend using it for your individual CBTS account logins. It can also be used to securely share files & notes using the Send feature.

Vaultwarden integrates with/uses the Bitwarden suite of apps. Apps are available for Desktop and Mobile users and are available as extensions/add-ons for all major browsers.

1. Creating Your Vaultwarden Account

1. You will receive an email with an invite to set up your Vaultwarden account. Click "Join Organization Now".



2. An account creation page will open. Fill out the password lines and create a helpful password hint. Then click "Create Account".
Note: This password can be different from your CBTSCommons password. We suggest using the same password but it is your choice.

A screenshot of the "Join CBTS" account creation page. At the top is a lock icon with three stars and a minus sign. Below it is the heading "Join CBTS" and the instruction "Finish joining this organization by setting a master password." The form contains four numbered steps: 1. "Master password (required)" with a password field, a strength indicator showing "Strong", and a note: "Important: Your master password cannot be recovered if you forget it! 12 character minimum." 2. "Confirm master password (required)" with a password field. 3. "Master password hint" with a text field containing "Helpful password hint here" and a note: "If you forget your password, the password hint can be sent to your email. 26/50 character maximum." 4. A checkbox labeled "Check known data breaches for this password" which is checked. At the bottom is a blue "Create account" button.

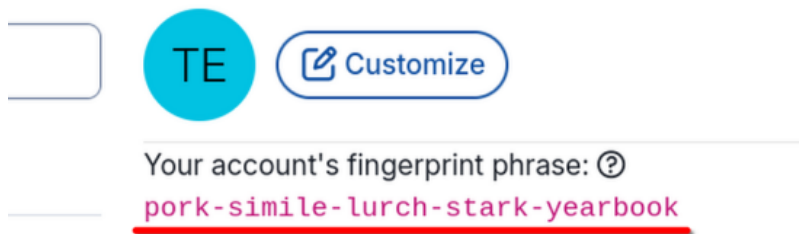
3. Your account has been created. You will be offered the Bitwarden browser extension which integrates Vaultwarden with your browser; we recommend installing it.
 1. If you install the extension, close the tab it opens up.

You will not immediately have access to the CBTS shared passwords; please [see Next Steps](#) for how to gain access.

2. Next Steps

You will not immediately have access to the CBTS shared passwords; we can only grant accounts access after they have been set up.

1. After you have created your Vaultwarden account, please email Isaac (best@cbtseminary.org) to let him know you have set up your Vaultwarden account; he will grant you access to the CBTS shared passwords.
2. In that email, please include your Vaultwarden account's fingerprint phrase:
 1. Go to your Vaultwarden Account settings - <https://vaultwarden.cbtscommons.org/#/settings/account>
 2. Copy the fingerprint phrase to your email draft

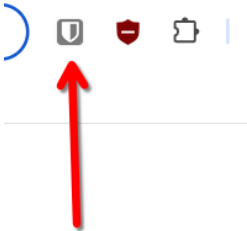


We recommend installing the browser extension for ease of use. The [extension setup page](#) will direct you to the correct extension/add-on store to install it. Then, [log in to Vaultwarden in the extension](#).

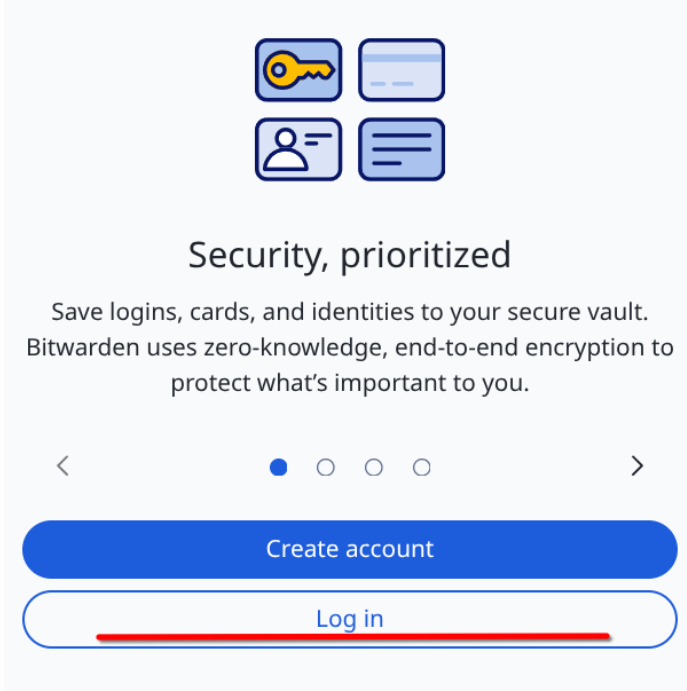
You may find it useful to install a [mobile apps](#) to access Vaultwarden on your phone.

Logging in to the Browser Extension

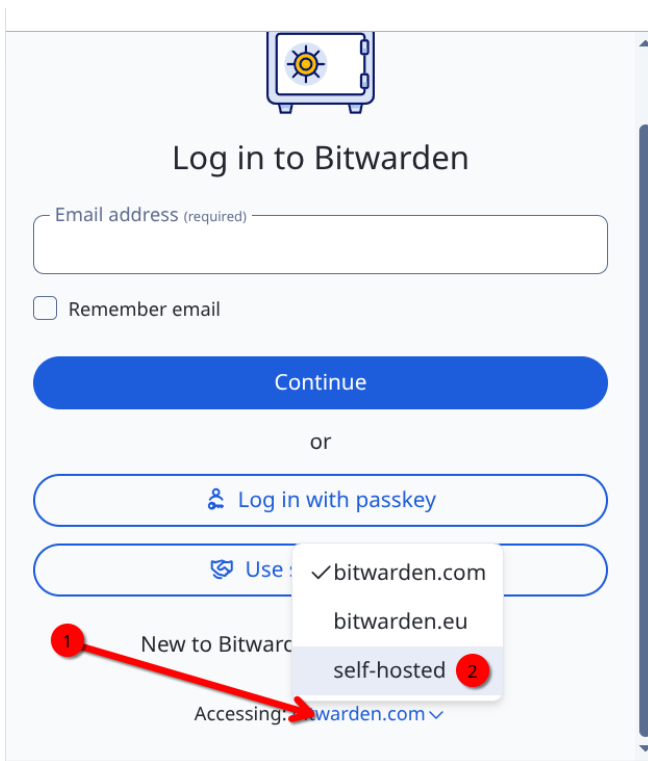
1. Click the extension icon in your browser menu/tool bar.



2. At the bottom of the extension window, select "Log In".



3. At the bottom of the next screen (you may need to scroll down), select "Accessing: bitwarden.com", then select "self-hosted".

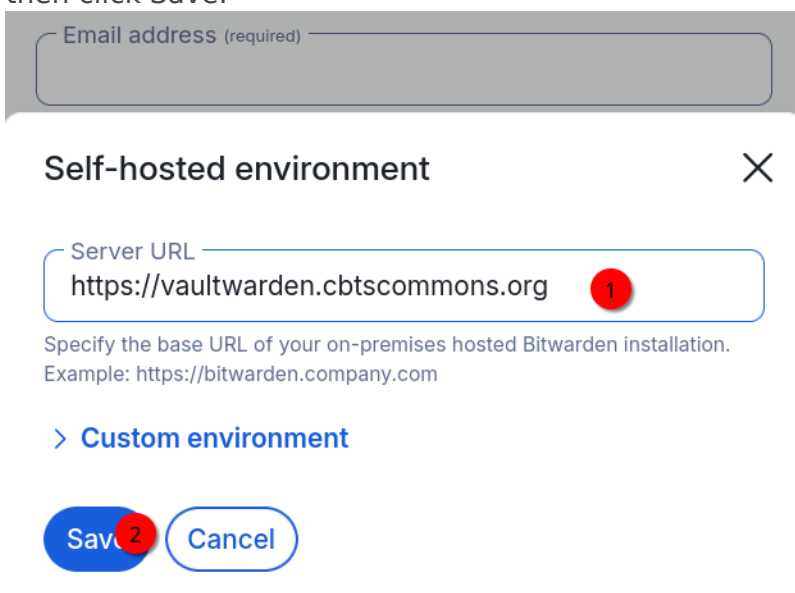


The image shows the Bitwarden login interface. At the top is a vault icon. Below it is the title "Log in to Bitwarden". There is a text input field for "Email address (required)". Below the field is a checkbox labeled "Remember email". A blue "Continue" button is present. Below the button is the word "or". There are two more buttons: "Log in with passkey" and "Use self-hosted". The "Use self-hosted" button is highlighted with a red circle labeled "2". A dropdown menu is open below it, showing options: "bitwarden.com" (checked), "bitwarden.eu", and "self-hosted" (highlighted with a red circle labeled "2"). A red arrow labeled "1" points from the "New to Bitwarden" link to the "self-hosted" option. At the bottom, it says "Accessing: vaultwarden.com".

4. Fill out the Server URL blank with

`https://vaultwarden.cbtscommons.org`

then click Save.



The image shows a "Self-hosted environment" configuration dialog. It has a title bar with a close button. Inside, there is a text input field for "Server URL" containing the value "https://vaultwarden.cbtscommons.org", which is highlighted with a red circle labeled "1". Below the field is a note: "Specify the base URL of your on-premises hosted Bitwarden installation. Example: https://bitwarden.company.com". There is a link "> Custom environment". At the bottom, there are two buttons: "Save" (highlighted with a red circle labeled "2") and "Cancel".

5. In the Email Address field, enter your CBTSCCommons username/email. Click continue.

Log in to Bitwarden

Email address (required) 1

☒ Remember email

Continue 2

or

6. Enter your Vaultwarden password, then click "Login with master password".

Welcome back

best@cbtscommons.org

Master password (required) 1

[Get master password hint](#)

Log in with master password 2

7. You are now logged in on the extension.

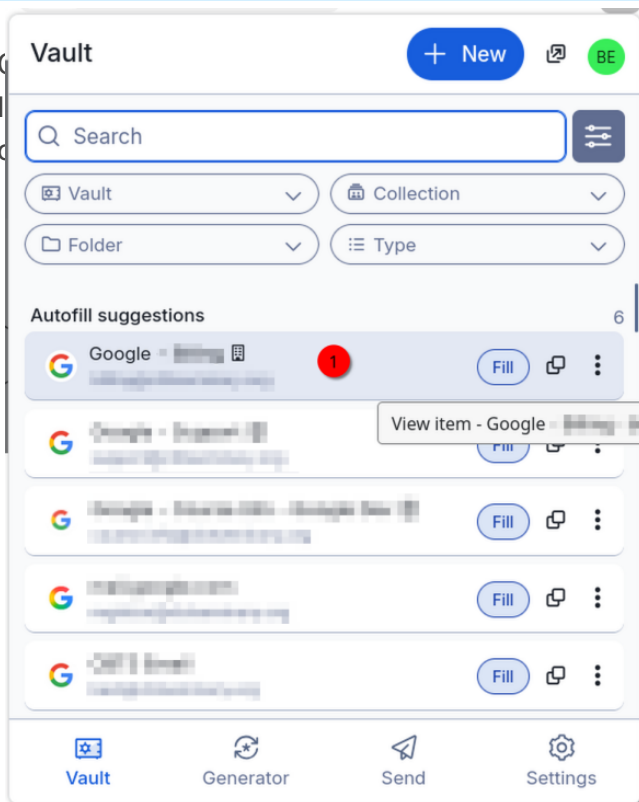
Adding 2FA (TOTP/Authenticator) codes to Vaultwarden

Vaultwarden can be used to generate TOTP/2FA codes in the place of Authenticator apps (such as Google Authenticator/Microsoft Authenticator). This article will walk you through setting up an account to use Vaultwarden for 2FA codes.

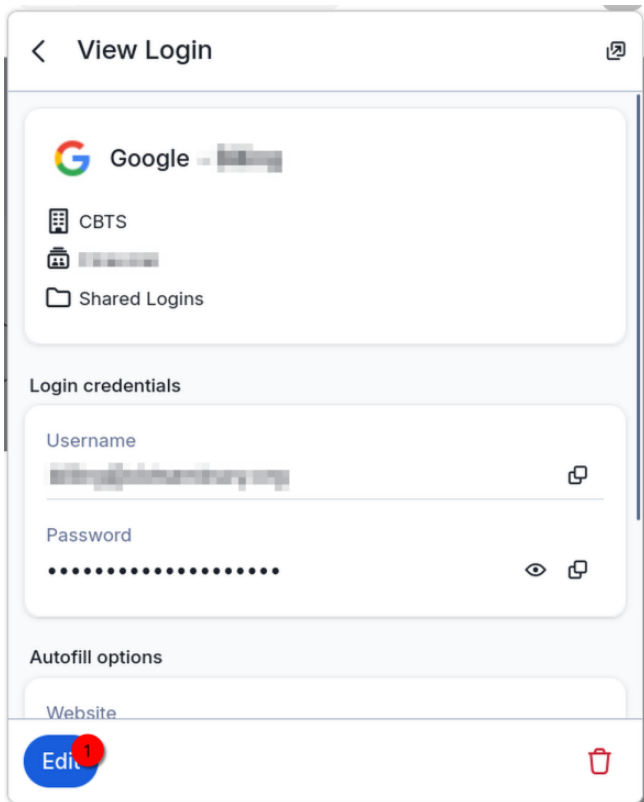
Most services that offer 2FA will give you a QR code to scan. We will begin at this step and use a Google Account as an example. The Vaultwarden steps will be the same for most/all accounts.

1. Click the Bitwarden extension icon.

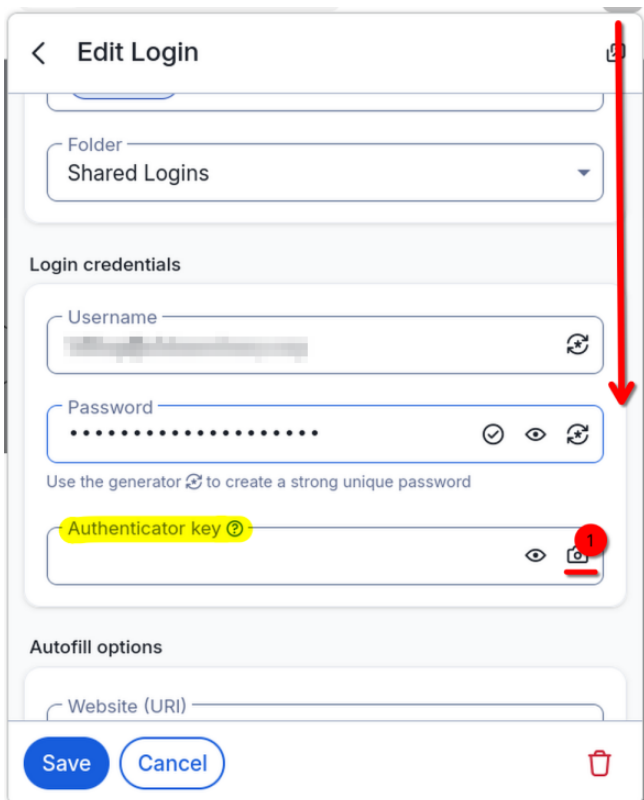
2. In the dropdown menu, click the account to which you are adding 2FA. (You can skip to step #4. in case, skip to step #4.)



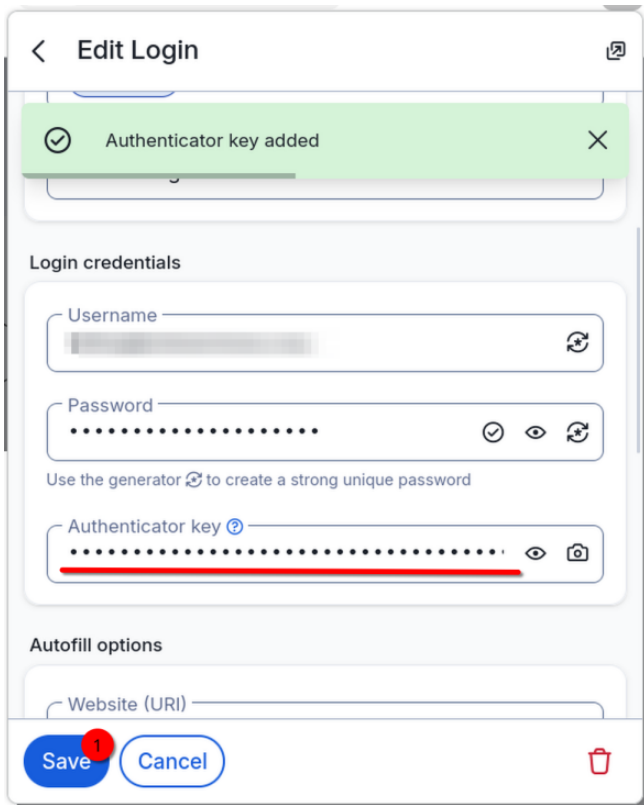
3. Select "Edit" in the lower left corner.



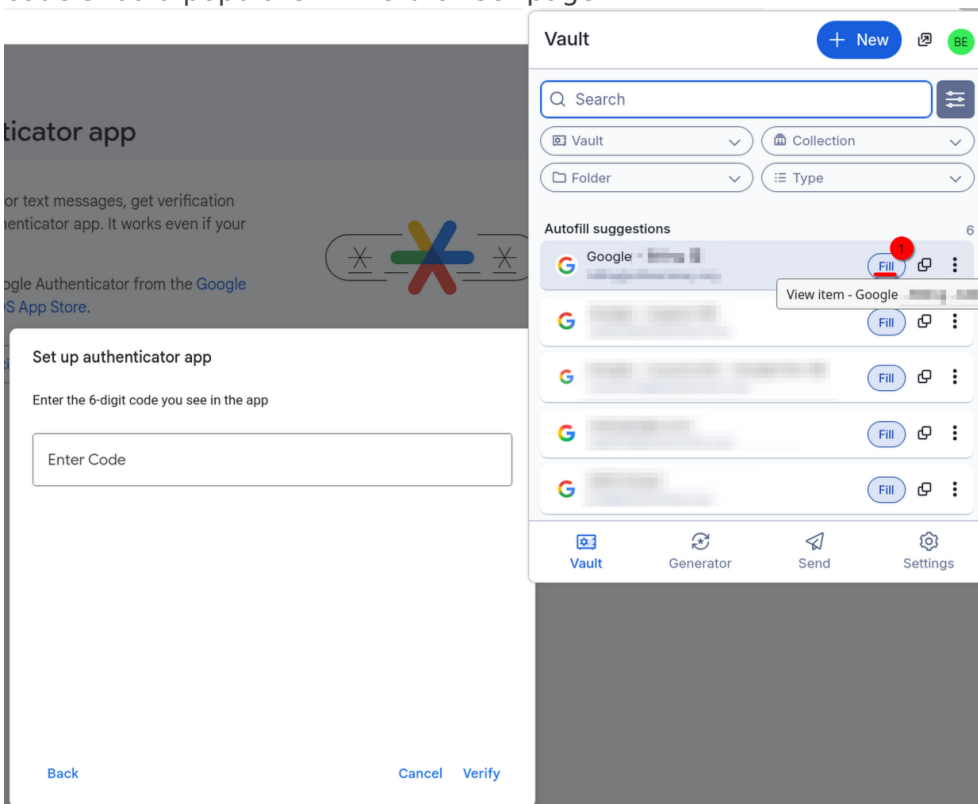
4. Scroll down to the section labeled "Login credentials" and find the "Authenticator key" text box. Select the camera icon.



5. The QR code will be scanned and the key added to Vaultwarden. Click "Save".



6. Continue in the browser (usually you will click "Next"). You should be prompted to enter your 2FA code.
7. Open the Bitwarden extension again and select "Fill" next to the correct account. Your 2FA code should populate in the browser page.



1. You can also try simply pasting from your clipboard. When the Bitwarden extension generates a 2FA code, it automatically copies it into your clipboard.
8. Select "Verify" (or whatever the appropriate option for your specific account).

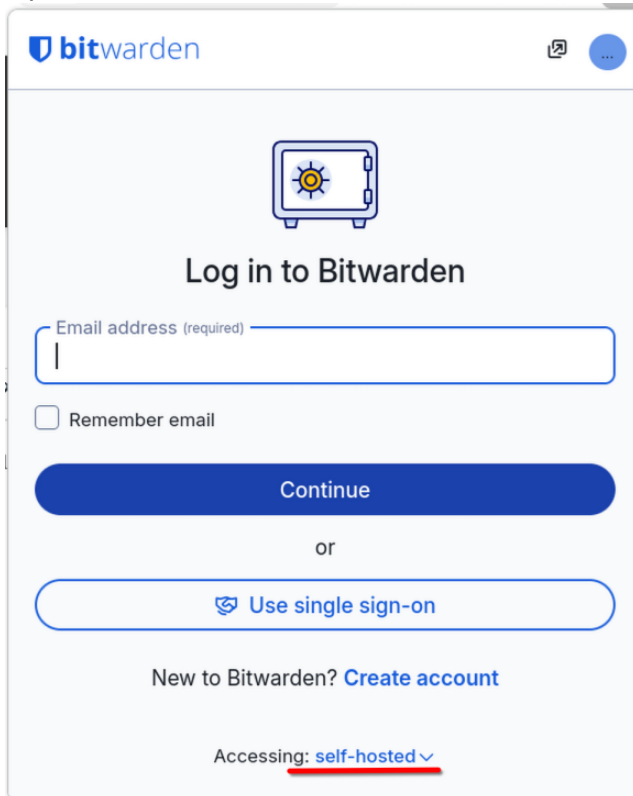
9.

You have set up Vaultwarden to generate 2FA codes for your account.

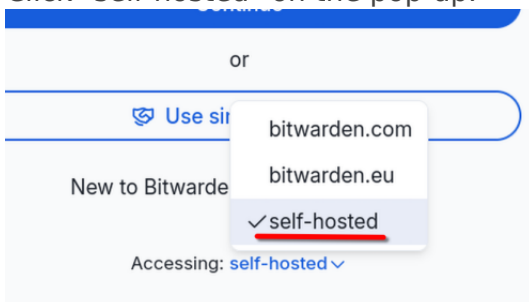
Can't Login on the Bitwarden Extension

If you receive a "KDF Config is Required" error when trying to log in on the Bitwarden extension, the most likely reason for this is that you have entered the Vaultwarden URL incorrectly.

1. Open the extension and scroll down to the "Accessing: self-hosted" item. Click it.



2. Click "self-hosted" on the pop-up.



3. Make sure you have correctly entered our Vaultwarden address/URL in the text box.

`https://vaultwarden.cbtscommons.org`

Then click "Save".

Self-hosted environment

Server URL

https://vaultwarden.cbtscommons.org

Specify the base URL of your on-premises hosted Bitwarden installation.
Example: https://bitwarden.company.com

> Custom environment

Save

Cancel

4. Try logging in again. If you still encounter errors, contact IT.