

MY ACCOUNT > TWO-STEP LOGIN

Recovery Codes

View in the help center:
<https://bitwarden.com/help/two-step-recovery-code/>

Recovery Codes

If you enable any [two-step login methods](#), it's important to understand that losing access to your secondary device(s) (for example, a mobile device with an installed authenticator, a security key, or a linked email inbox) has the potential to lock you out of your Bitwarden vault.

To protect against this, Bitwarden generates a **recovery code** that can be used with your master password to disable any enabled two-step login methods from outside your vault.

Tip

You should [get your recovery code](#) immediately after enabling any two-step login method. Additionally, get a new recovery code every time you [use it](#), as it will change with each use.

In addition to securing recovery codes, users may wish to create an [export](#) to backup vault data prior to enabling two-factor authentication.

Get your recovery code

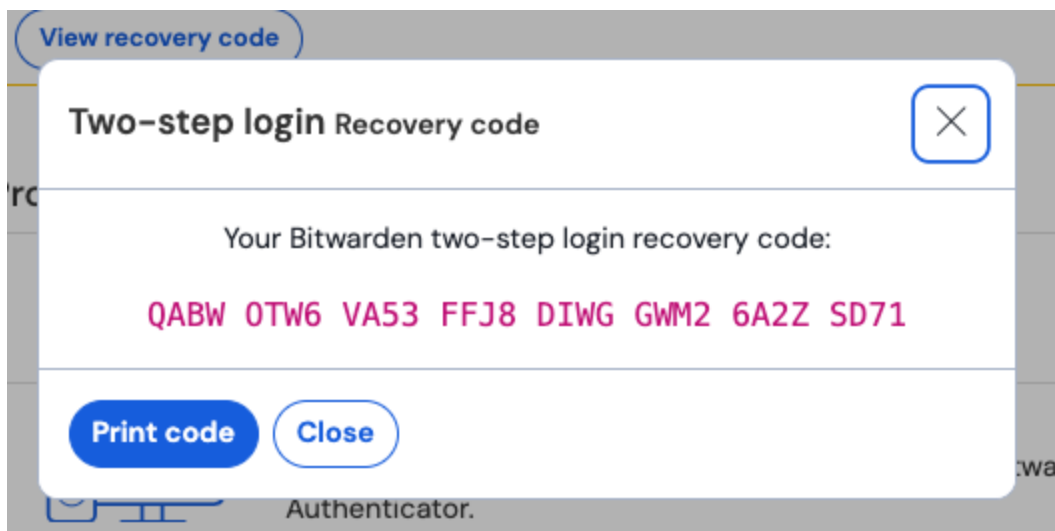
To get your recovery code:

1. Log in to the Bitwarden web app.
2. Select the **Settings** → **Security** → **Two-step login** from the navigation:

The screenshot shows the Bitwarden Security settings page. The left sidebar contains navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, My account, Security (highlighted), Preferences, Domain rules, Emergency access, and Free Bitwarden Famili... The main content area is titled 'Security' and has three tabs: Master password, Two-step login (selected), and Keys. Under 'Two-step login', there is a warning box with a yellow border and a warning icon. The warning text states: 'Warning: Setting up two-step login can permanently lock you out of your Bitwarden account. A recovery code allows you to access your account in the event that you can no longer use your normal two-step login provider (example: you lose your device). Bitwarden support will not be able to assist you if you lose access to your account. We recommend you write down or print the recovery code and keep it in a safe place.' Below the warning is a 'View recovery code' button. Underneath is a 'Providers' section with a list of authentication methods, each with an icon, a description, and a 'Manage' button: Email (envelope icon), Authenticator app (phone and screen icon), Passkey (key icon), Yubico OTP security key (yubico logo), and Duo (duo logo).

Two-step login

3. Select the **View recovery code** button near the top of the screen. You will be prompted to enter your master password, which will open a recovery code panel:



Sample Recovery Code

Save your recovery code in the way that makes the most sense for you. Believe it or not, printing your code and keeping it somewhere safe is one of the best ways to ensure that the code isn't vulnerable to theft or inadvertent deletion.

Note

When does a recovery code change?

Neither disabling and re-enabling two-step login, nor changing your master password will change your recovery code. Your recovery code will only change **when you use it**. After you use a recovery code, immediately get a new one and save it in the way that makes the most sense for you.

Use your recovery code

To use your recovery code, navigate to <https://vault.bitwarden.com/#/recover-2fa/>, <https://vault.bitwarden.eu/#/recover-2fa/>, or, if you are self-hosting, <https://your.domain.com/#/recover-2fa/>.

Using your recovery code is like the normal login procedure, requiring your (i) email address, (ii) master password, and (iii) recovery code. On successful authentication of all three, you will be logged in to your vault and **all two-step login methods will be disabled**.

Once used, get a new recovery code, as it will change with each use. You should also at this point re-enable any two-step login methods you want to use in the future.

Note

Recovery codes will not disable Duo for organizations. If you are locked out of your vault by an organizational Duo prompt, reach out to the Duo administrator at your company for help bypassing the prompt.

If you're not sure whether the Duo prompt is setup personally or by your organization, try using the **Use another two-step login method** button.