

MY ACCOUNT > TWO-STEP LOGIN

Recovery Codes

Recovery Codes

If you activate 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 deactivate any enabled two-step login methods from outside your vault.

Tip


You should [get your recovery code](#) immediately after activating 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 activating 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:


Password Manager

Vaults

Send

Tools

Reports

Settings

My account

Security

Preferences

Domain rules

Emergency access

Free Bitwarden Famili...

Password Manager

Admin Console

More from Bitwarden

Security

Master password
Two-step login
Keys

Two-step login






Secure your account by requiring an additional step when logging in.

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.

View recovery code

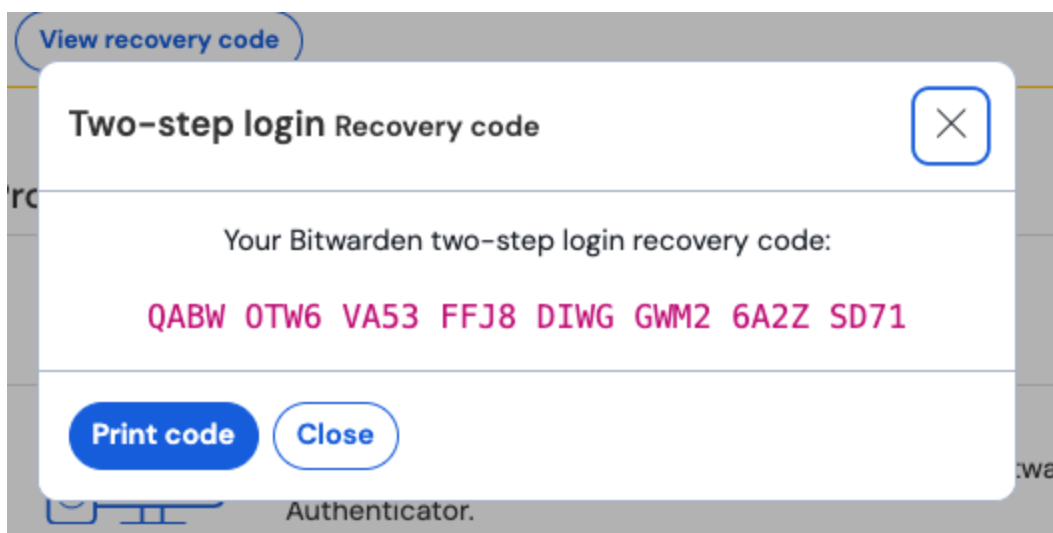
Providers

	Email Enter a code sent to your email.	Manage
	Authenticator app Enter a code generated by an authenticator app like Bitwarden Authenticator.	Manage
	Passkey Use your device's biometrics or a FIDO2 compatible security key.	Manage
	Yubico OTP security key Use a YubiKey 4, 5 or NEO device.	Manage
	Duo Enter a code generated by Duo Security.	Manage

Inloggen in twee stappen

- 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:

© 2025 Bitwarden Inc | Page 3 of 4



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 deactivating and re-activating 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 fully logged in to your vault and all two-step login methods deactivated**, and your device will be considered recognized for [new device login protection](#).

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

Note

Recovery codes will not deactivate 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.