

MY ACCOUNT > TWO-STEP LOGIN >

Two-step Login via Email

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.

View in the help center:

<https://bitwarden.com/help/setup-two-step-login-email/>

Two-step Login via Email

Two-step login using email is available for free to all Bitwarden users.

Warning

Two-step login via email is not recommended if you are using [login with SSO](#), as using multiple methods will cause errors. Consider setting up [two-step login via a free authenticator](#) instead.

Setup Email Verification

To enable two-step login using email:

Warning

Losing access to your two-step login device can permanently lock you out of your vault unless you write down and keep your two-step login recovery code in a safe place or have an alternate two-step login method enabled and available.

Get your [recovery code](#) from the **Two-step login** screen immediately after enabling any method. Additionally, users may create a Bitwarden [export](#) to backup vault data.

1. Log in to the Bitwarden web app
2. Select **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: '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:

Provider	Description	Action
	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

Two-step login

3. Locate the **Email** option and select the **Manage** button:

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

Two-step login providers

You will be prompted to enter your master password to continue.

4. Enter the email that you wish you receive verification codes and click the **Send Email** button.

Tip

If you have multiple email addresses, the address you use for two-step login doesn't have to be the same address you used to sign up for Bitwarden.

5. Check your inbox for the six-digit verification code. Enter the code in the dialog box in your web vault and select the **Enable** button.

A green **Enabled** message will indicate that two-step login via email has been enabled.

6. Select the **Close** button and confirm that the **Email** option is enabled, as indicated by a green checkbox (✓).

Note

We recommend keeping your active web vault tab open before proceeding to test two-step login in case something was misconfigured. Once you have confirmed it's working, logout of all your Bitwarden apps to require two-step login for each. You will eventually be logged out automatically.

Use Email verification

The following assumes that **Email** is your [highest-priority enabled method](#). To access your vault using email 2FA:

1. Log in to your Bitwarden vault on any any app and enter your email address and master password.

You will be prompted to enter the six-digit verification code that was emailed to your configured email.

2. Check your inbox for the six-digit verification code. Enter this code on the vault login screen.

 **Tip**

Check the **Remember Me** box to remember your device for 30 days. Remembering your device will mean you won't be required to complete your two-step login step.

3. Select **Continue** to finish logging in.

You will not be required to complete your secondary two-step Login step to **Unlock** your vault once logged in. For help configuring log out vs. Lock behavior, see [vault timeout options](#).