

MY ACCOUNT > TWO-STEP LOGIN >

Two-step Login via Authenticator

View in the help center:

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

Two-step Login via Authenticator

Two-step login using a third-party authenticator app (for example, the standalone [Bitwarden Authenticator](#)) is available for free to all Bitwarden users.

Note

Some authenticator apps do not automatically backup your 2FA tokens for easy migration to a new mobile device. In these cases, you should manually save each token's authenticator recovery codes. See [Recovery codes](#) for additional information to safely store and use recovery codes.

Some apps, such as Authy, do support backup and sync across devices. In these cases, be sure to set a strong backup password and keep a record of it in your Bitwarden vault.

Set up an authenticator

To enable two-step login using an authenticator app:

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: '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:

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 **Authenticator App** 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. Scan the QR code or manually enter the key using your authenticator app of choice.

If you don't have an authenticator app on your mobile device yet, download one like [Bitwarden Authenticator](#) and scan the QR code.

5. Once scanned, your authenticator app will return a 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 authenticator has been enabled.

6. Select the **Close** button and confirm that the **Authenticator App** option now 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.

Setup on multiple devices or authenticators

Bitwarden two-step login can be made to work with multiple compatible devices. To add 2FA to an additional device, follow the steps above and scan the QR code with your additional device or manually enter the QR key to enable 2FA on the additional device. This can also be done to setup two-step login for multiple authenticators on a single device.

Use an authenticator

The following assumes that **Authenticator App** is your [highest-priority enabled method](#). To access your vault using an authenticator:

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

You will be prompted to enter the six-digit verification code from your authenticator app.

2. Open your authenticator app and find the six-digit verification code for your Bitwarden vault. Enter this code on the vault login screen. Typically, verification codes will change every 30 seconds.

 **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](#).