MY ACCOUNT > TWO-STEP LOGIN >

Two-step Login via FIDO2 WebAuthn Passkey

Two-step Login via FIDO2 WebAuthn Passkey

Two-step login using FIDO2 WebAuthn credentials is available for free to all Bitwarden users.

Any FIDO2 WebAuthn Certified credentials can be used, including security keys such as YubiKeys, SoloKeys, and Nitrokeys, as well as native biometrics options like Windows Hello and Touch ID.

> 💡 **Tip**
>
> All new FIDO keys set up with Bitwarden are registered as WebAuthn keys. If you have a registered FIDO key that is marked **(Migrated from FIDO)** in the Two-step Login → Manage FIDO2 WebAuthn view of the web app, it is a U2F key and should be removed and re-registered to automatically set the key up with WebAuthn. Bitwarden will begin phasing out support for **(Migrated from FIDO)** U2F keys in 2025.

FIDO2 WebAuthn is compatible with most Bitwarden applications. If you wish to use a version that doesn't support it, ensure you turn on an alternative two-step login method. Supported applications include:

- **Web vault** on a device with a FIDO2-supported browser.

- **Browser extensions** for a FIDO2-supported browser.

- **Desktop apps** on Windows 10 and above.

- **Mobile apps** for Android and iOS 13.3+ with a FIDO2-supported browser.

Setup FIDO2 WebAuthn

To enable two-step login using FIDO2 WebAuthn:

> ⚠️ **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:

Two-step login

3. Locate the **Passkey** 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	**Yubico OTP security key** Use a YubiKey 4, 5 or NEO device.	Manage
DUO	**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. Give your security key a friendly **Name**.

5. Plug the security key into your device's USB port and select **Read Key**. If your security key has a button, touch it.

> ⓘ **Note**
>
> Some devices, including those with Windows Hello or macOS devices that support passkeys, are native FIDO2 authenticators that will offer these options as defaults. If you want to register a security key or other authenticator, you may need to select a **Try another way**, **Other Options**, or **Cancel** button to open up your other options.

6. Select **Save**. A green `Enabled` message will indicate that two-step login using FIDO2 WebAuthn has been successfully enabled and your key will appear with a green checkbox (✓).

7. Select the **Close** button and confirm that the **FIDO2 WebAuthn** option is now enabled, as indicated by a green checkbox (✓).

Repeat this process to add up to 5 FIDO2 WebAuthn security keys to your account.

> ⓘ **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 FIDO2 WebAuthn

The following assumes that **FIDO2 WebAuthn** is your highest-priority enabled method. To access your vault using a FIDO2 WebAuthn device:

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

   You will be prompted to insert your security key into your device's USB port. If it has a button, touch it.
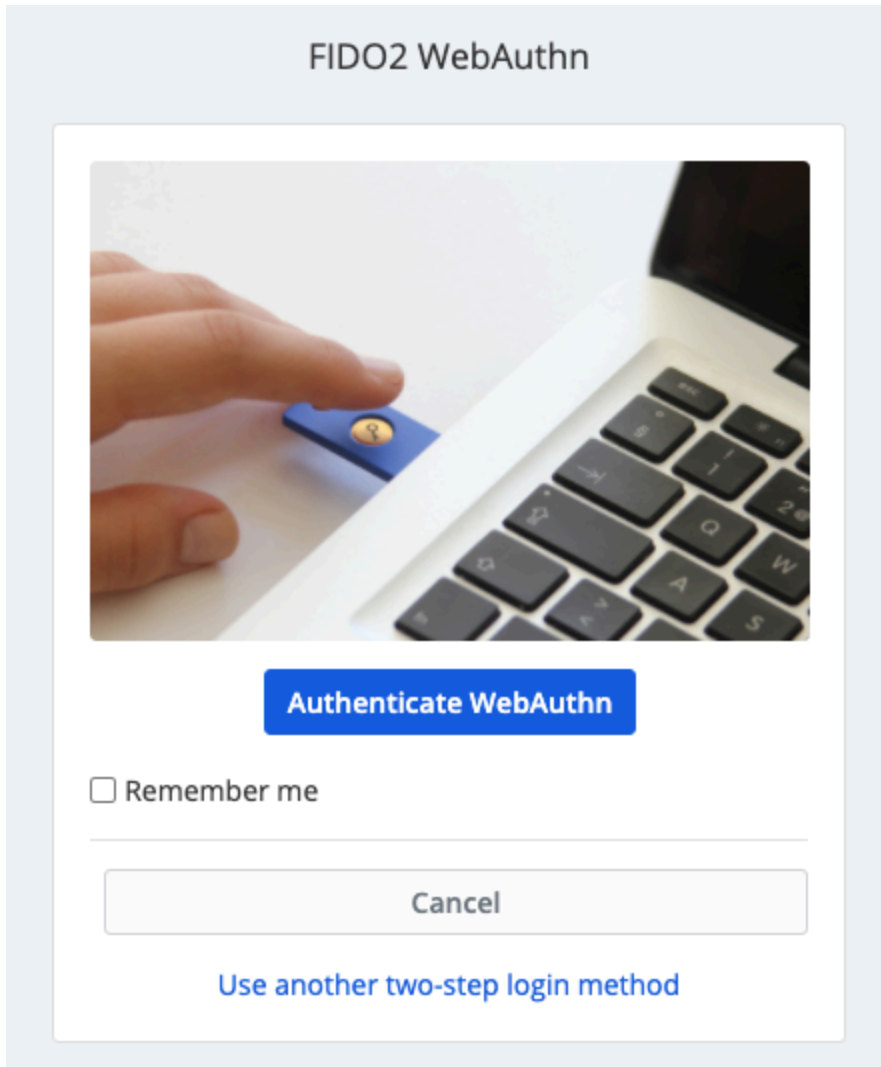
FIDO2 Prompt

> 💡 **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.

You will not be required to complete your secondary two-step login setup to **unlock** your vault once logged in. For help configuring log out vs. lock behavior, see vault timeout options.

bitwarden

Secure and trusted open source password manager for business

NFC troubleshooting

If you are using a FIDO2 authenticator with NFC functionality like a YubiKey or other hardware security key, you may need to practice finding the NFC reader in your device as different devices have NFC readers in different physical locations (for example, top of phone vs. bottom of phone, or front vs. back).

> 💡 **Tip**
>
> Hardware security keys typically have a physical plug, which will work more reliably in cases where NFC is difficult.

Troubleshooting YubiKey NFC

On mobile devices, you may encounter a scenario where your YubiKey is read twice consecutively. You will know this has occurred when your device's browser opens the YubiKey OTP website (`https://demo.yubico.com/yk`) and if your device vibrates multiple times to signal multiple NFC reads.

To solve this, use the YubiKey Manager application to disable the **NFC → OTP** interface for your key:

YubiKey Manager
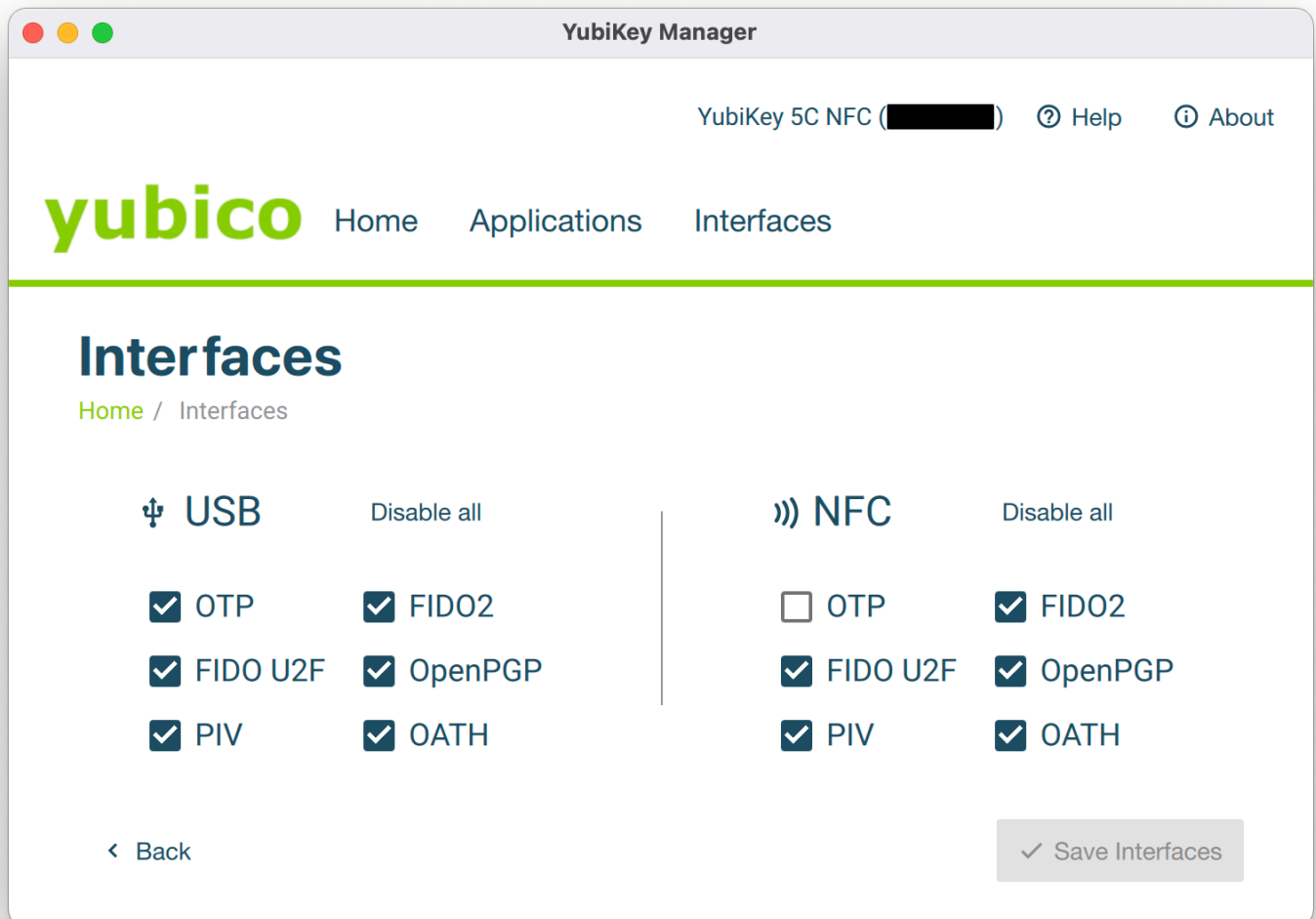
> ⚠ **Warning**
>
> Disabling **NFC** → **OTP** will prevent you from being able to use two-step login via YubiKey (OTP) over NFC with this key. In this scenario, OTP via USB will still function as expected.