bitwarden | Help Center Article

PASSWORD MANAGER > VAULT BASICS

Storing Passkeys

View in the help center:
https://bitwarden.com/help/storing-passkeys/

Storing Passkeys

Passkeys can be stored and used by Bitwarden Password Manager. Using browser extensions and mobile apps, users can log in to their favorite apps and websites that have passkey login capability. Passkeys are a safe, passwordless alternative for users to log into services across their devices.

> **Note**
>
> On iOS, version 17.0 or higher is required for storing and using passkeys. Learn more.
>
> On Android, version 14.0 or higher is required for storing and using passkeys. There may be additional setup steps required. Learn more.

Developed with the standards set by the FIDO Alliance, passkeys allow a user to secure their accounts and bypass the vulnerabilities that come with standard password authentication, such as phishing. Stored passkeys are protected with Bitwarden's trusted end-to-end encryption.

What are passkeys?

Passkeys are a replacement for passwords that provide fast, easy, and secure sign-ins to websites and apps across a user's devices. More precisely, "passkey" is a consumer-friendly term for a discoverable FIDO credential that can be synced to allow secure passwordless sign-ins across devices, or dedicated to a single piece of hardware as a device-bound passkey.

Apps and services can request that passkeys created with them are verified with a PIN, password, pattern, or biometric factor when you save or access them. For more general information about passkeys, see Passkey FAQs.

Types of passkeys

Passkeys are stored and invoked via Bitwarden browser extensions and mobile apps. This means that both discoverable passkeys and non-discoverable FIDO2 credentials can be stored in Bitwarden and used to log in to websites with passkey capabilities.

Using passkeys with Bitwarden

> **Note**
>
> Saving and using passkeys are a feature of Bitwarden browser extensions and mobile apps. Please note:
>
> - On iOS, version 17.0 or higher is required for storing and using passkeys. Learn more.
> - On Android, version 14.0 or higher is required for storing and using passkeys. There may be additional setup steps required. Learn more.

⇒Browser extensions

> **Note**
>
> When a domain is in the **Excluded Domains** list, Bitwarden browser extensions won't issue passkey prompts.

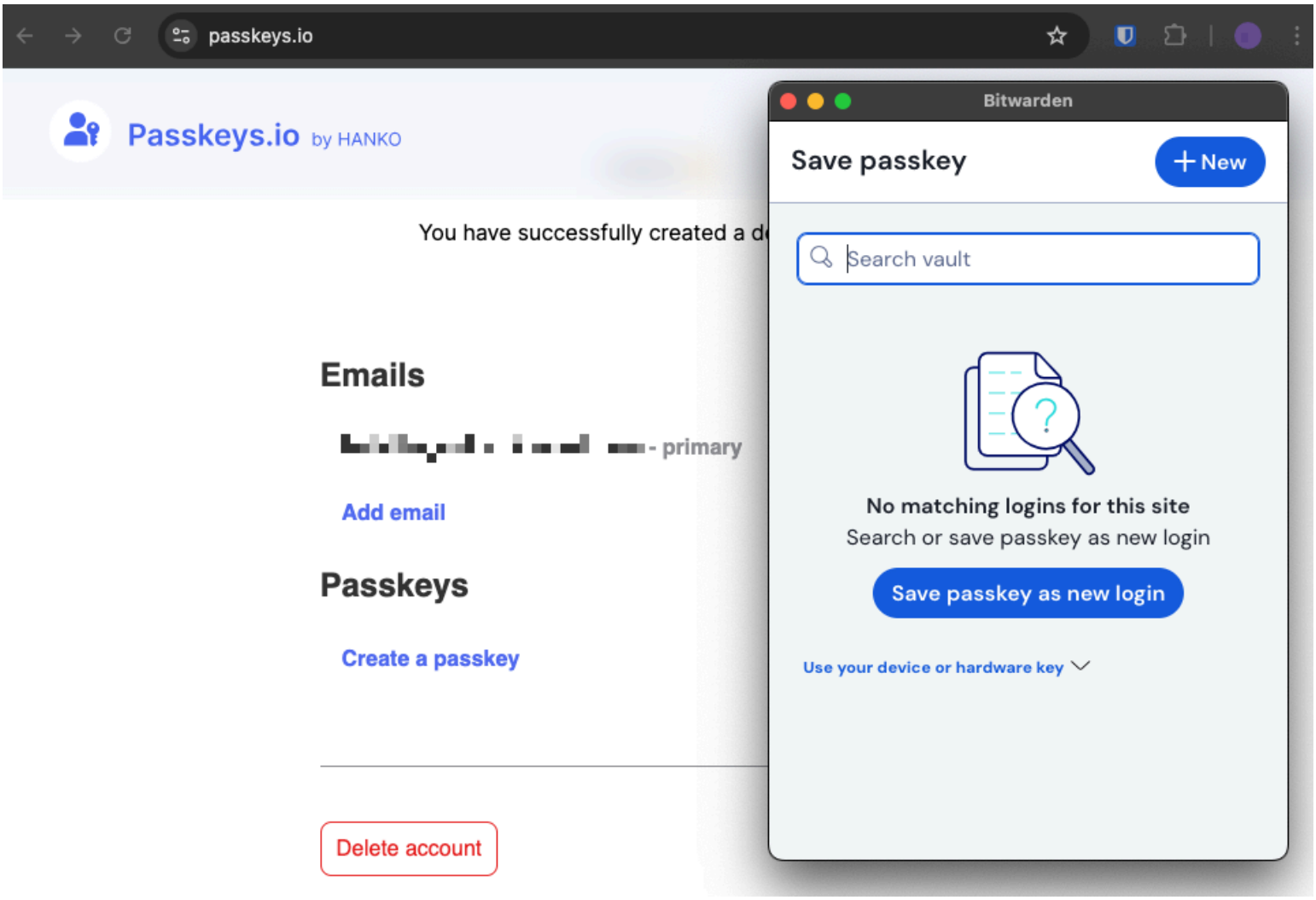
Ask to save and use passkeys

To use the functionality described below, make sure that the **Ask to save and use passkeys** option, located in the browser extensions **Settings** → **Notifications** menu, is toggled on.

You can set excluded domains if there are specific sites you do not wish to use Bitwarden for passkeys with.

Create a passkey

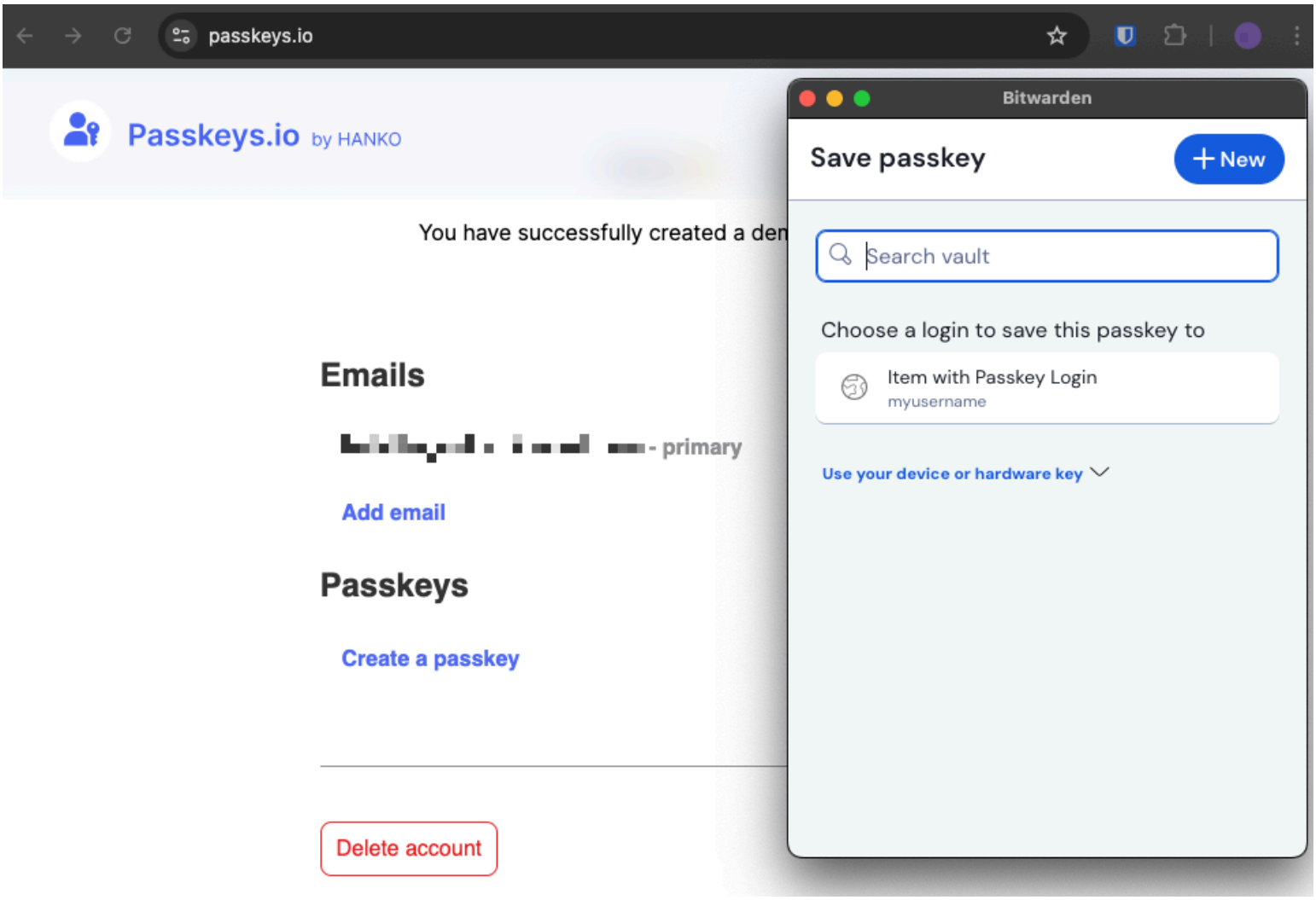
When creating a new passkey on a website or app, the browser extension will prompt you to store the passkey:



Save passkey

> **Note**
>
> Select **Use your device or hardware key** if you do not wish to store the passkey in Bitwarden.

If a passkey already exists for this service, Bitwarden will allow you to save a new passkey by selecting the + icon to create a new item, or by overwriting an existing passkey:



Save passkey with existing login

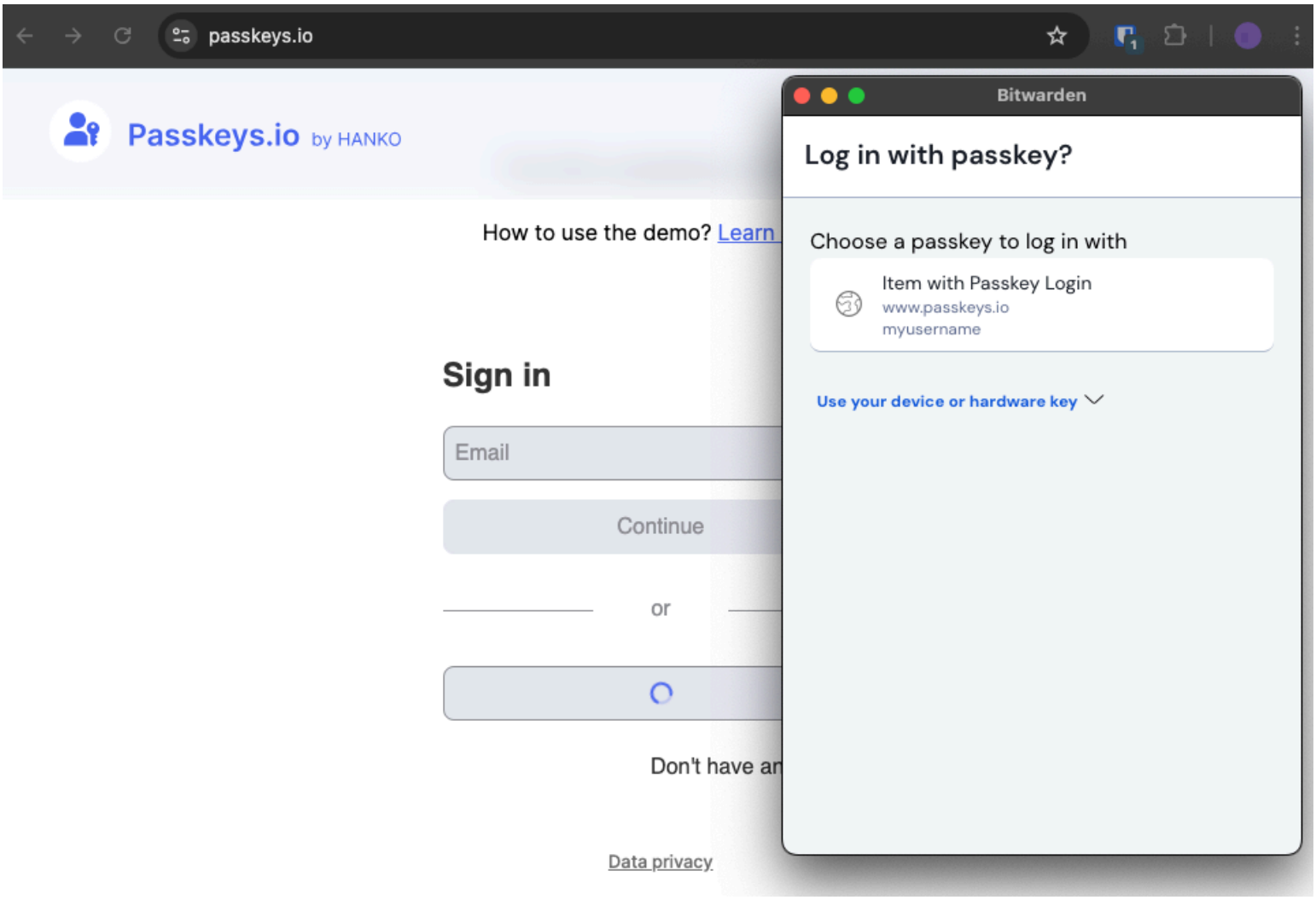
Duplicate passkeys cannot be saved for the same username and service. You may edit or overwrite an existing cipher if you wish to save a new passkey with the username and service.

> **Note**
>
> Only one passkey can be saved per login item. If a credential is saved in multiple places, for instance as two separate login items in the individual vault and organization vault respectively, a different passkey can be be stored with each login item.

Sign in using a passkey stored in Bitwarden

To use a passkey stored in Bitwarden, initiate the passkey login on the website. When the **Ask to save and use passkeys** option is on, the browser extension will provide an option to login using the passkey stored in your Bitwarden vault:

> **Tip**
>
> The inline autofill menu can also be used to easily authenticate with passkeys.



Log in with passkey

Select the passkey you would like to use.

> **Note**
>
> Select **Use your device or hardware key** if you do not wish to store the passkey in Bitwarden, or to use an existing passkey that is not stored in Bitwarden.

⇒iOS

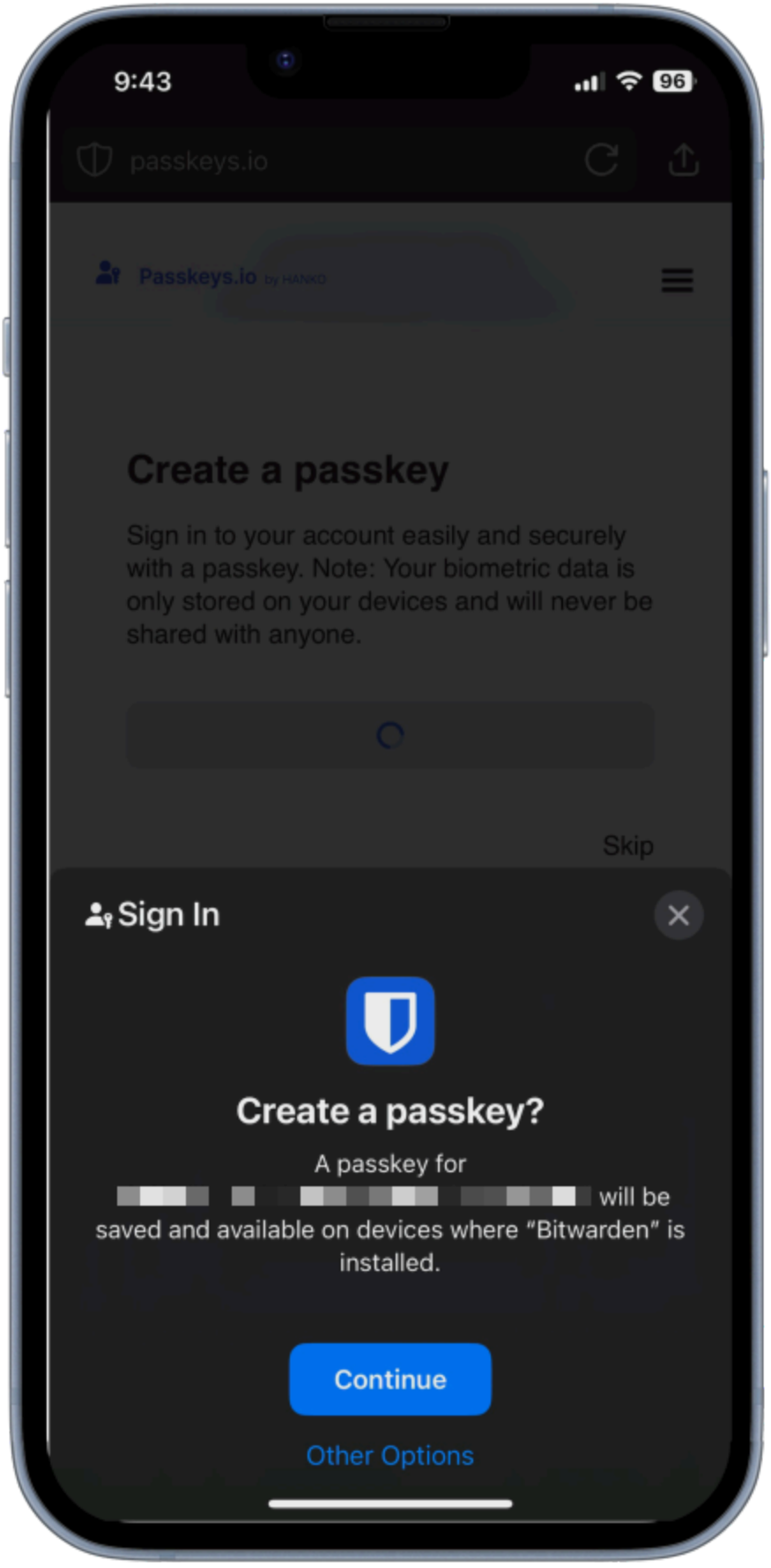
Setup Bitwarden for use with passkeys

To use the functionality described below, open your iOS **Settings** app and navigate to **Passwords → Password Options**. Toggle the following options on:

- Toggle **AutoFill Passwords and Passkeys** on.
- Toggle **Bitwarden** on in the **Use passwords and passkeys from:** list.

Create a passkey

When creating a new passkey on a website or app, the iOS application will prompt you to store the passkey:


9:43
96
passkeys.io
Passkeys.io by HANKO
Create a passkey
Sign in to your account easily and securely with a passkey. Note: Your biometric data is only stored on your devices and will never be shared with anyone.
Skip
Sign In
Create a passkey?
A passkey for
will be saved and available on devices where "Bitwarden" is installed.
Continue
Other Options

Select **Continue**.

> **Note**
>
> Select **Other Options** if you do not wish to store the passkey in Bitwarden or **Other Sign In Options** to sign in with a passkey not stored in Bitwarden.

If a passkey already exists for this service, Bitwarden will allow you to save a new passkey by selecting the + icon to create a new item, or by overwriting an existing passkey:


9:44
96
Cancel
Save passkey
Choose a login to save this passkey to
www.passkeys.io

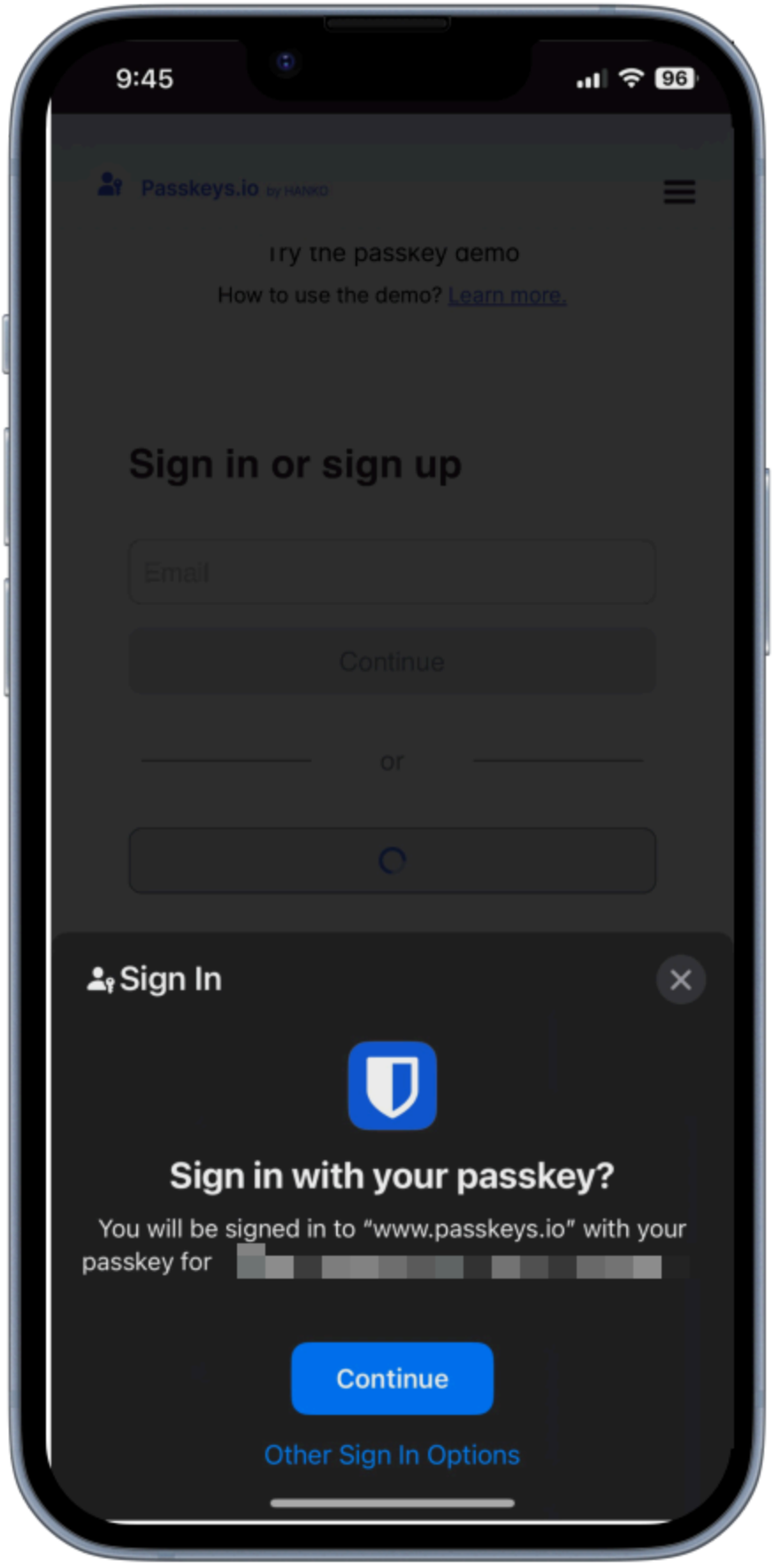
Save or overwrite a passkey

Duplicate passkeys cannot be saved for the same username and service. You may edit or overwrite an existing cipher if you wish to save a new passkey with the username and service.

> **Note**
>
> Only one passkey can be saved per login item. If a credential is saved in multiple places, for instance as two separate login items in the individual vault and organization vault respectively, a different passkey can be be stored with each login item.

Sign in using a passkey stored in Bitwarden

To use a passkey stored in Bitwarden, initiate the passkey login on the website. The mobile app will provide an option to login using the passkey stored in your Bitwarden vault:


9:45
96
Passkeys.io by HANKO
Try the passkey demo
How to use the demo? Learn more.
Sign in or sign up
Email
Continue
or
Sign In
Sign in with your passkey?
You will be signed in to "www.passkeys.io" with your passkey for
Continue
Other Sign In Options

Select **Continue**.

> **Note**
>
> Select **Other Options** if you do not wish to store the passkey in Bitwarden or **Other Sign In Options** to sign in with a passkey not stored in Bitwarden.

⇒Android

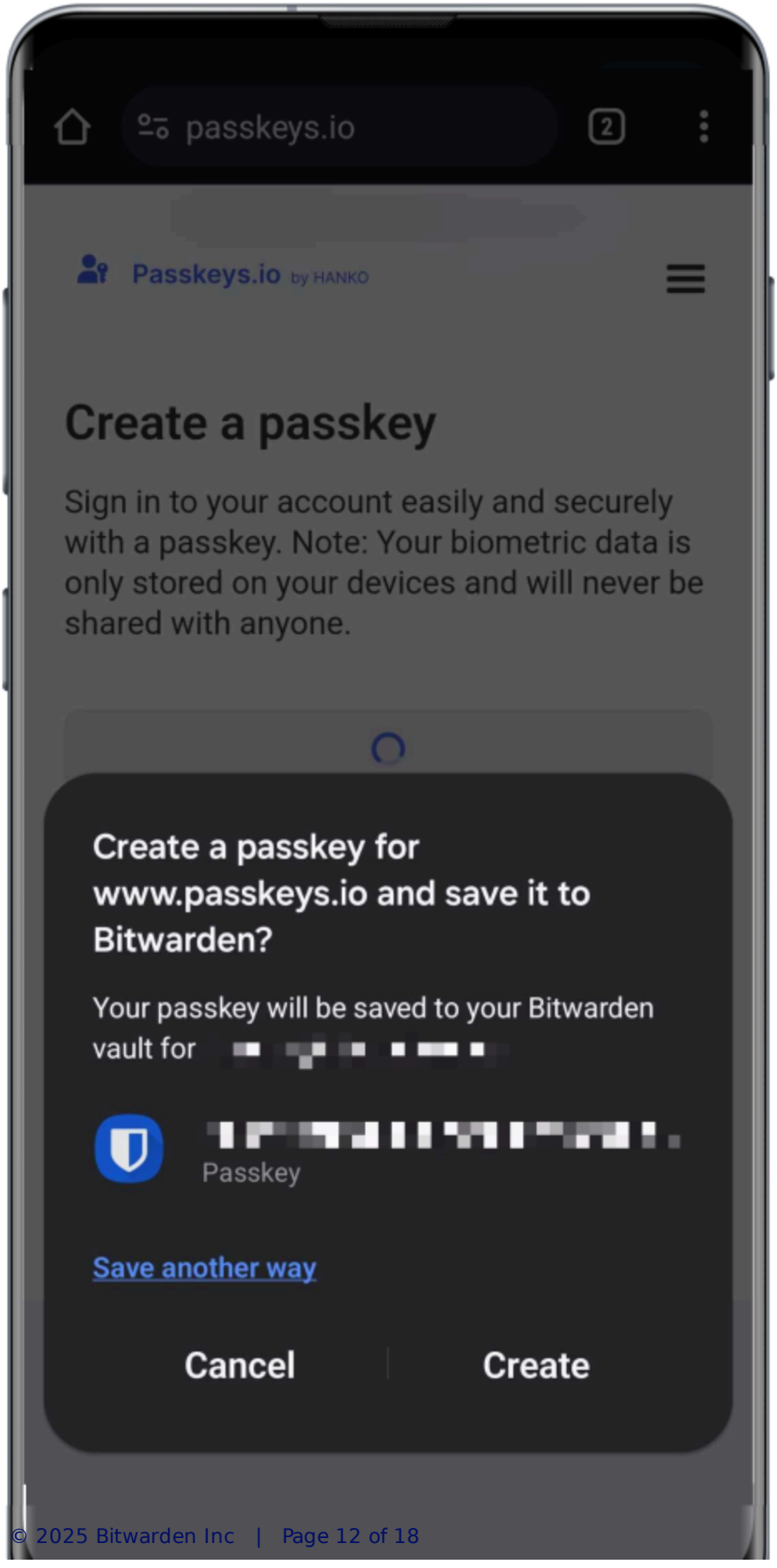
Setup Bitwarden for use with passkeys

Once the Bitwarden application is updated to the latest version, go to **Settings** → **Auto-fill** and tap **Passkey management** to access the Android settings to configure Bitwarden as your passkey provider.

> **Warning**
>
> In order to activate Bitwarden as your preferred passkey provider it may be necessary to:
>
> - For Chrome users:
>   - Navigate to `chrome://flags` and select **Enabled for 3rd party passkey providers** under **Android Credential Management for passkeys**. If this option is not shown, your browser may need to be updated.
> - Disable and re-enable Bitwarden as your autofill provider once updated to the latest version.
> - Reboot your phone after changing the above settings.
> - Remove any passkeys stored in Google Password Manager, as Android will preference this provider (be sure not to delete any important passkeys that will result in lockout from an account).
>
> Please also note that Android does not allow 3rd party passkey providers like Bitwarden to support passkey-based 2FA (a.k.a. "non-discoverable credentials"); Bitwarden-stored passkeys can only be used as a primary login credential.
>
> Additionally, while passkeys for web browsers are supported, support for apps is coming soon in a future build.

Create a passkey

When creating a new passkey on a website or app, the Android application will prompt you to store the passkey:


passkeys.io
2
Passkeys.io by HANKO
Create a passkey
Sign in to your account easily and securely with a passkey. Note: Your biometric data is only stored on your devices and will never be shared with anyone.
Create a passkey for www.passkeys.io and save it to Bitwarden?
Your passkey will be saved to your Bitwarden vault for
Passkey
Save another way
Cancel
Create

Select **Create**.

> **Note**
>
> Select **Save another way** if you do not wish to store the passkey in Bitwarden or **More saved sign-ins** to sign in with a passkey not stored in Bitwarden.

If a passkey already exists for this service, Bitwarden will allow you to save a new passkey by selecting the + icon to create a new item, or by overwriting an existing passkey:


Items for passkeys.io
Matching items
1
passkey.io

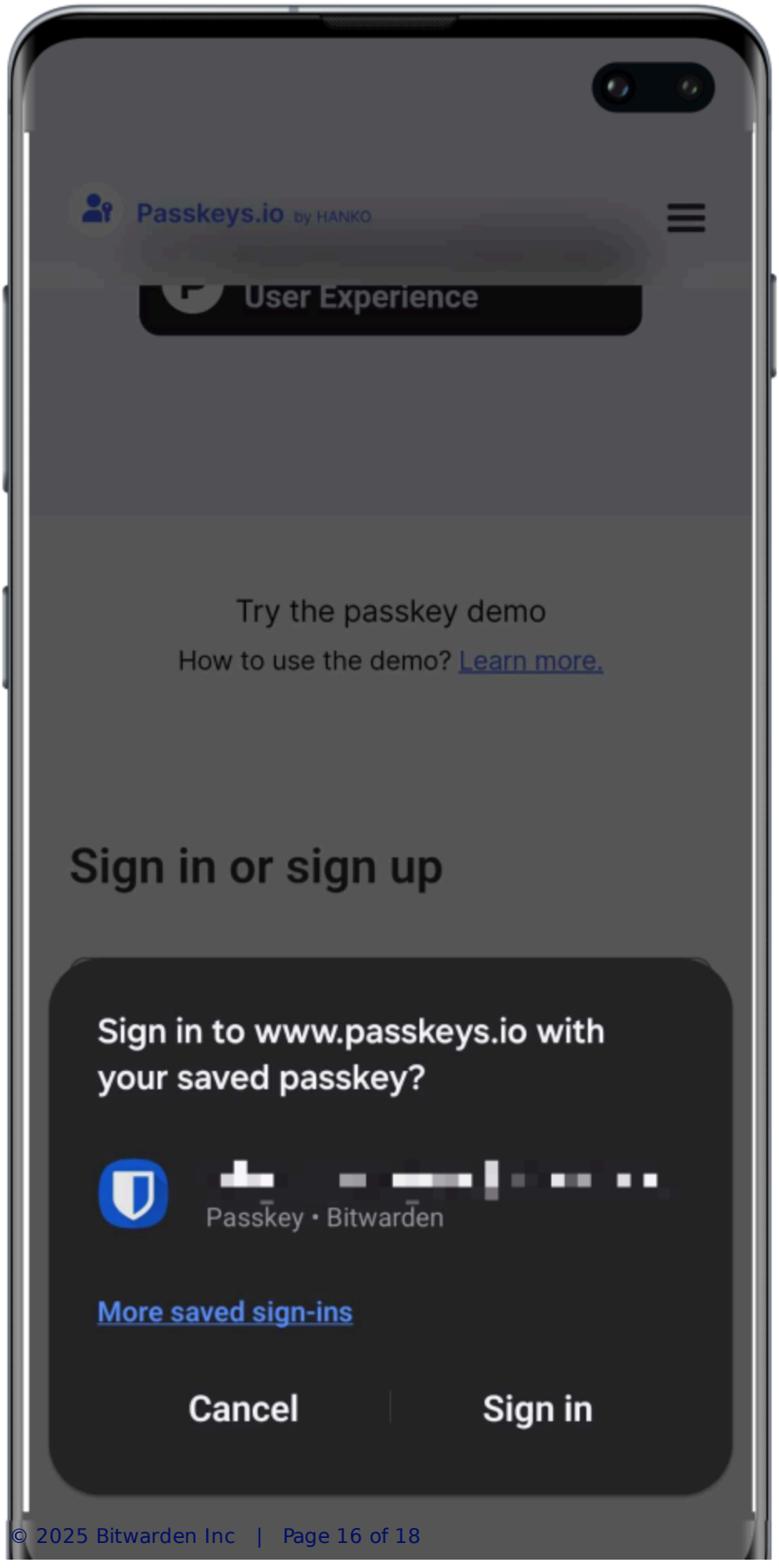
Save or overwrite a passkey

Duplicate passkeys cannot be saved for the same username and service. You may edit or overwrite an existing cipher if you wish to save a new passkey with the username and service.

> **Note**
>
> Only one passkey can be saved per login item. If a credential is saved in multiple places, for instance as two separate login items in the individual vault and organization vault respectively, a different passkey can be be stored with each login item.

Sign in using a passkey stored in Bitwarden

To use a passkey stored in Bitwarden, initiate the passkey login on the website. The mobile app will provide an option to login using the passkey stored in your Bitwarden vault:


Passkeys.io by HANKO
User Experience
Try the passkey demo
How to use the demo? Learn more.
Sign in or sign up
Sign in to www.passkeys.io with your saved passkey?
Passkey • Bitwarden
More saved sign-ins
Cancel
Sign in

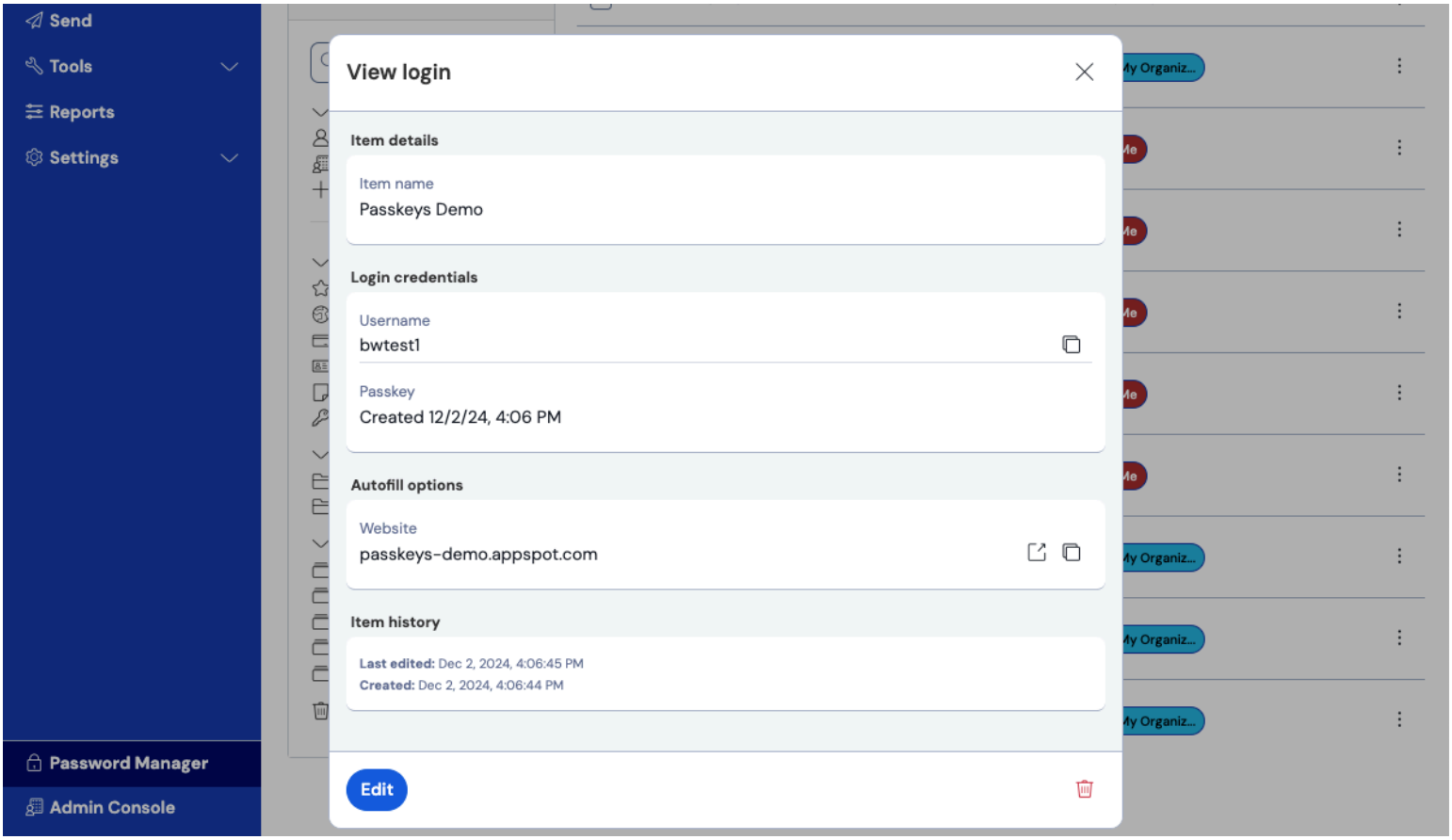
Sign in with passkey

Select **Sign in** to use your passkey.

> **Note**
>
> Select **Save another way** if you do not wish to store the passkey in Bitwarden or **More saved sign-ins** to sign in with a passkey not stored in Bitwarden.

Viewing passkeys in Bitwarden

Once a passkey has been saved, it can be viewed from any Bitwarden app and is located in the **Passkey** field:



Passkey in your vault

> **Note**
>
> If master password re-prompt has been enabled on the login item, you will be required to re-enter your master password in order to access the passkey.

Deleting passkeys

To delete a passkey from a vault item:

1. Open the item **Edit** screen from the Password Manager web app, browser extension or desktop app.
2. Select the ⊖ delete icon for the **Passkey** field.

Delete a passkey

Passkey Management FAQ

The following FAQ items are in reference to Bitwarden passkey storage. For general passkey information, see Passkey FAQs.

Q: Will passkeys be included if you clone a vault item?

A: Bitwarden will not copy a passkey when completing a clone action.

Q: Are stored passkeys included in Bitwarden imports and exports?

A: Passkeys are included in .json exports from Bitwarden. The ability to transfer your passkeys to or from another passkey provider is planned for a future release.

Q: Can I store passkeys in the mobile app?

A: Passkeys support for mobile applications is available for iOS (learn more) and for Android (learn more).