

PASSWORD MANAGER > AUTOFILL > MORE AUTOFILL OPTIONS

Autofill Passkeys

View in the help center:

<https://bitwarden.com/help/storing-passkeys/>

Autofill Passkeys

Tip

Bitwarden provides functionality both for [logging in to Bitwarden with a passkey](#) and [autofilling a stored passkey for other websites and services](#).

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.

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.

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](#).

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.

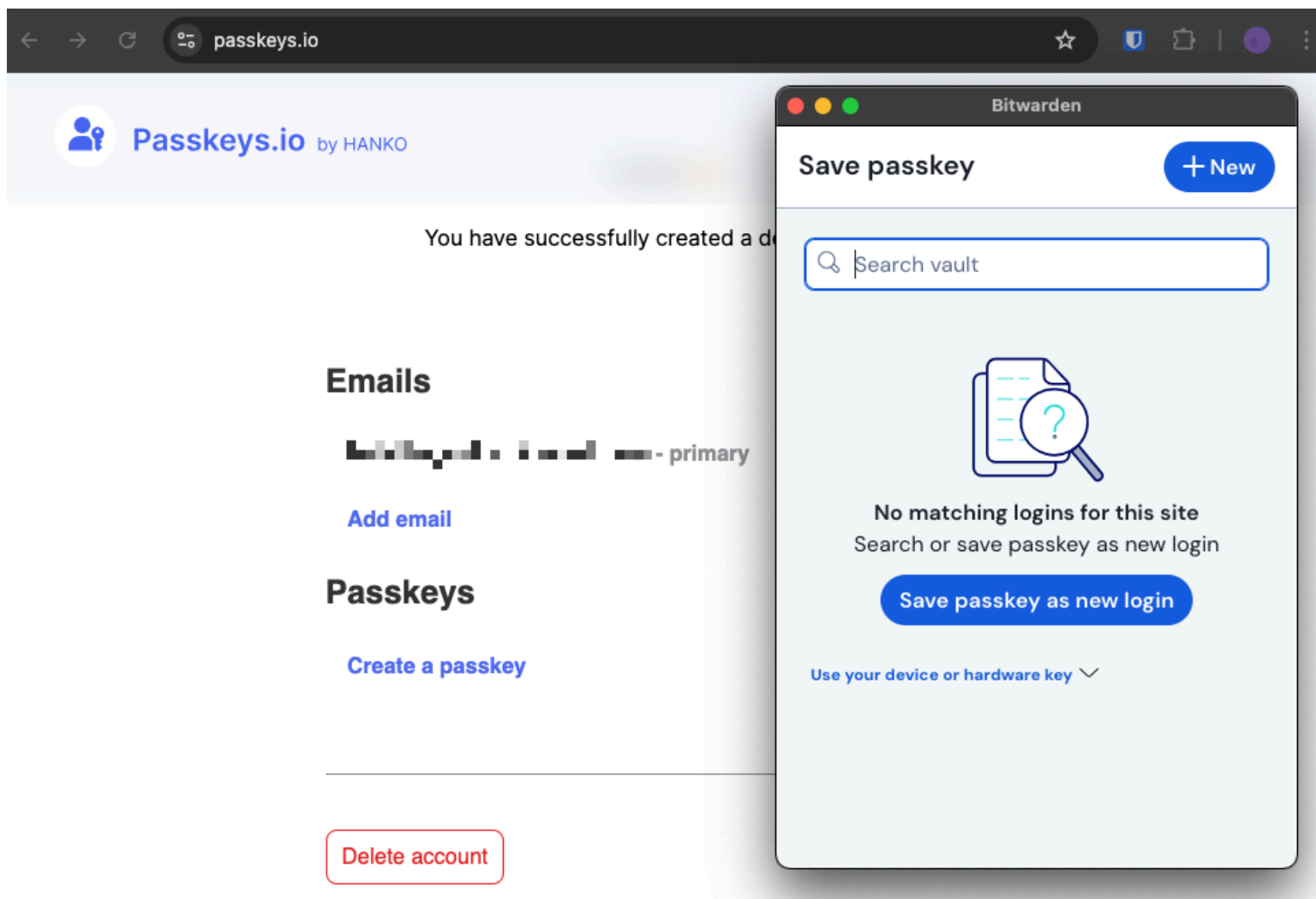
Ask to save and use passkeys

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:

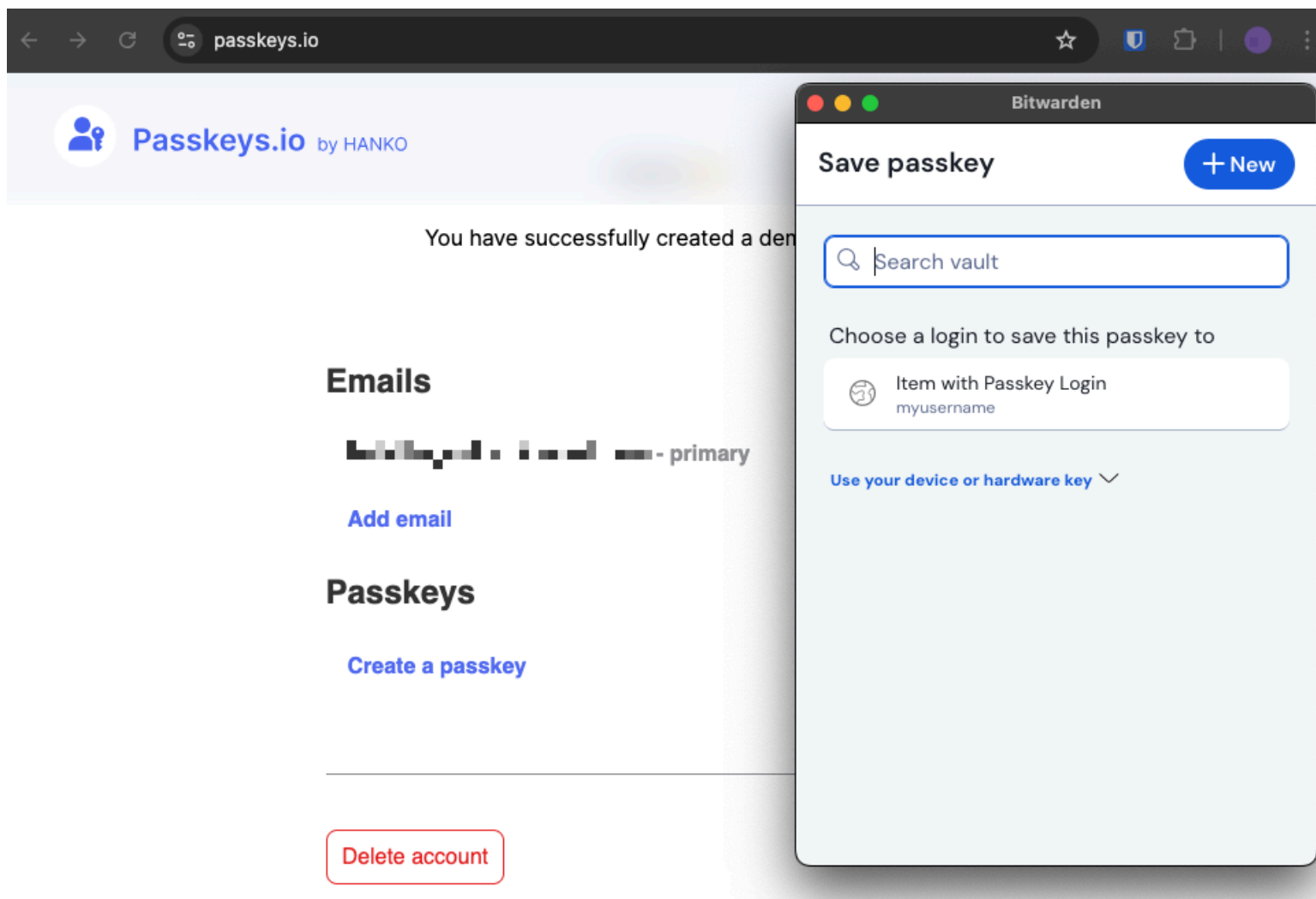


Save passkey

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

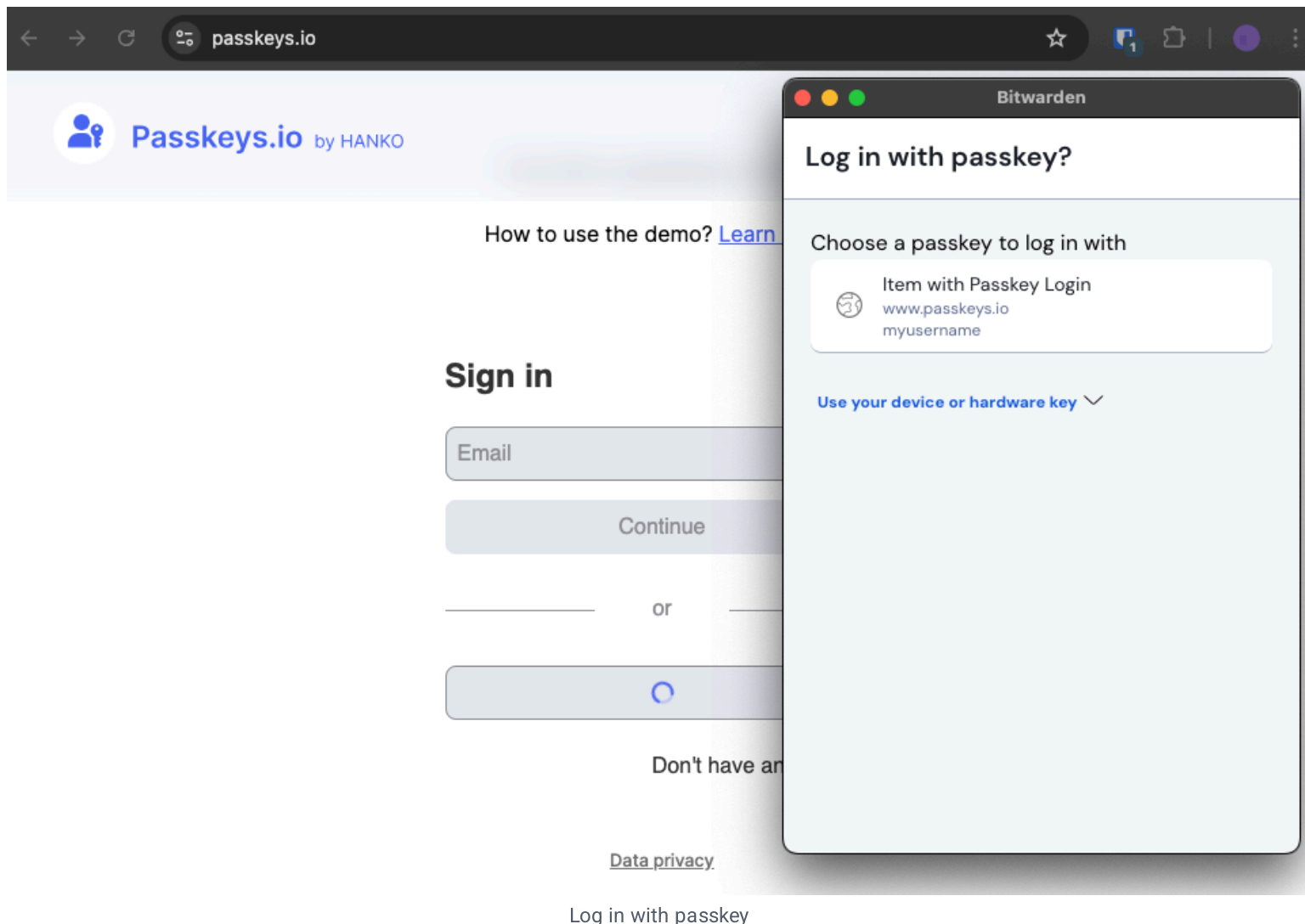
Only one passkey can be saved per login item. If a credential is saved in multiple places, for instance as two separate login items in the individual vault and organization vault respectively, a different passkey can be stored with each login item.

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.



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.

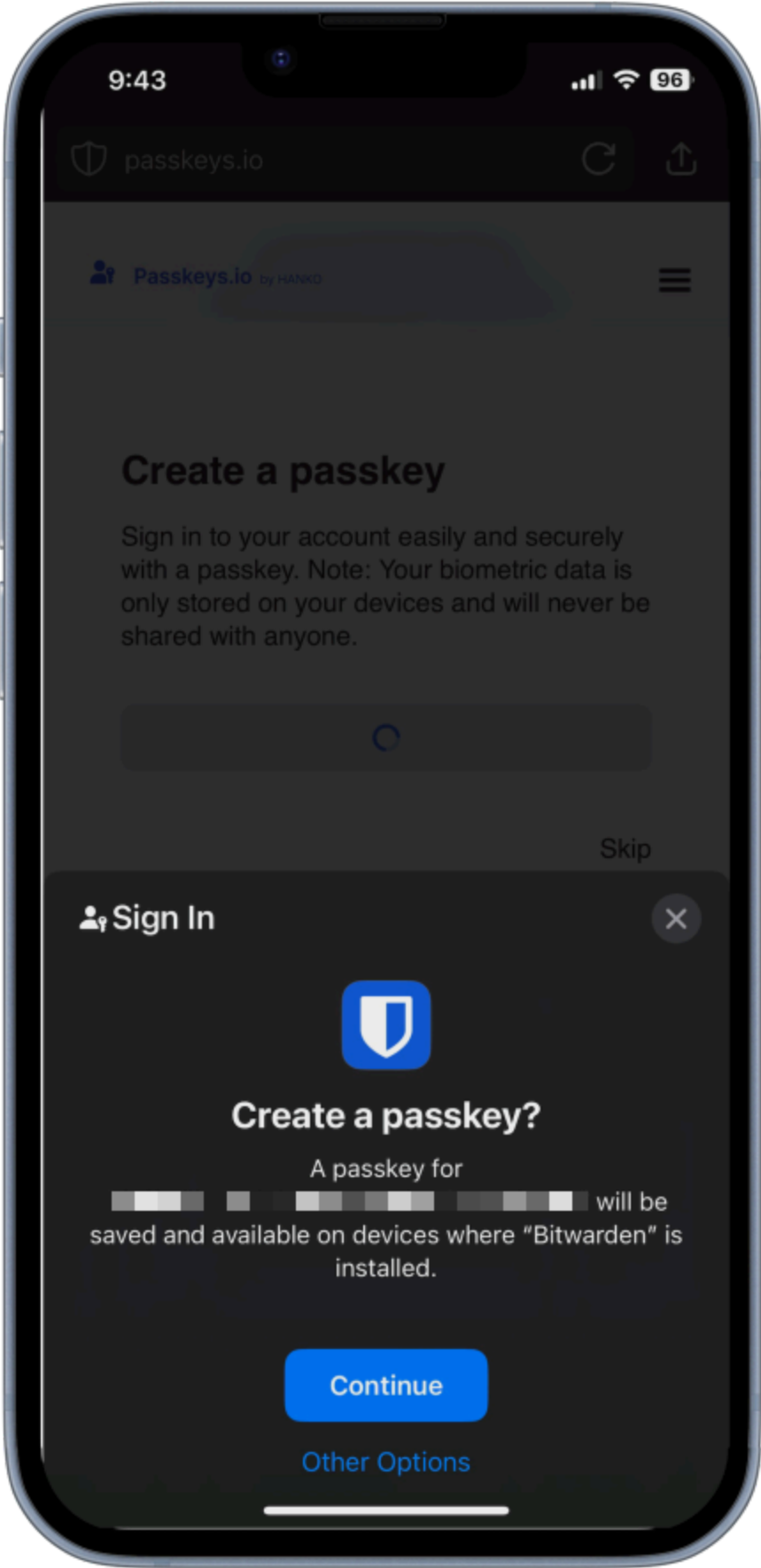
⇒iOS**Setup Bitwarden for use with passkeys**

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 Paskeys** 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:



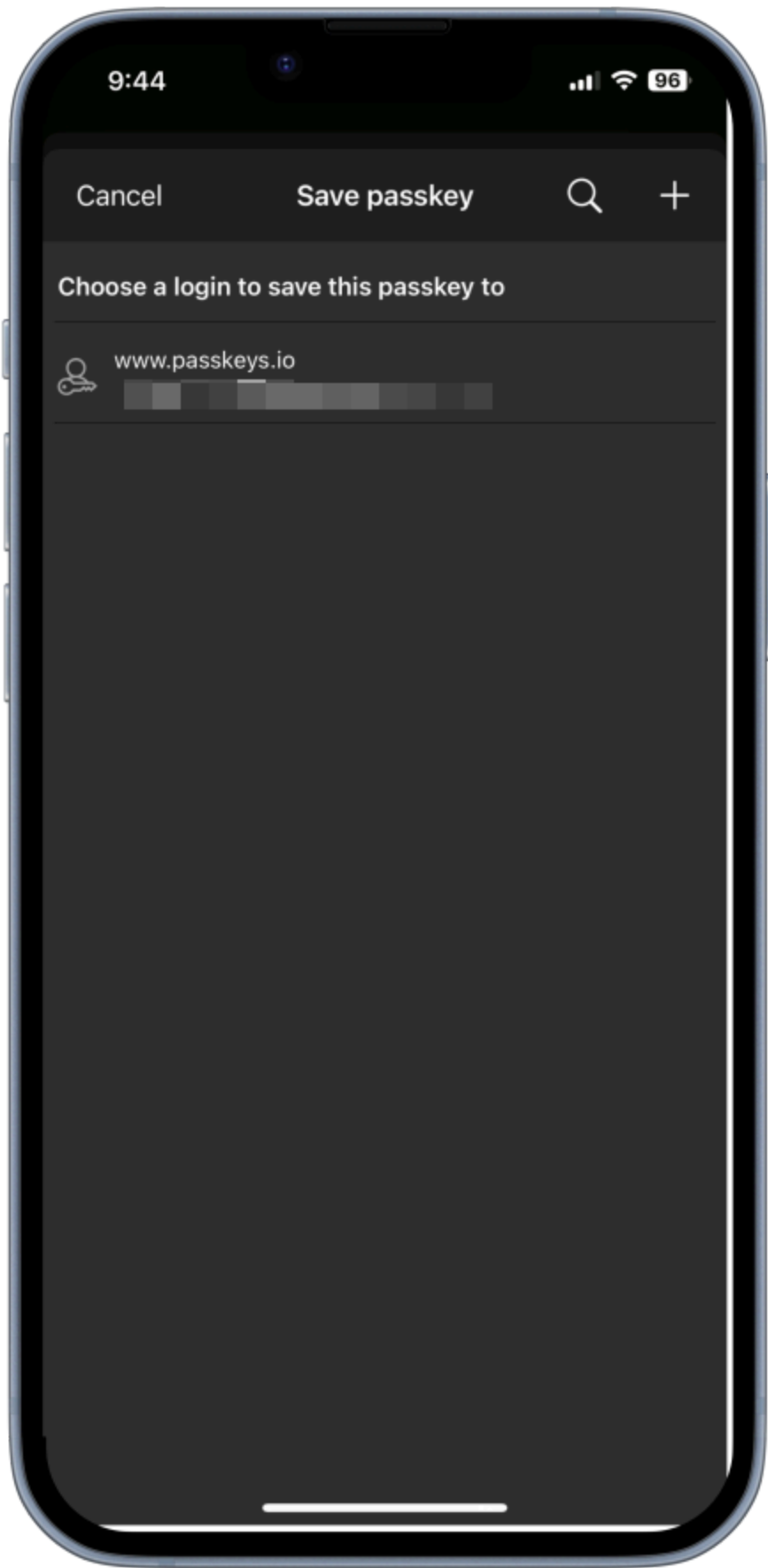
Create a passkey

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:



Save or overwrite a passkey

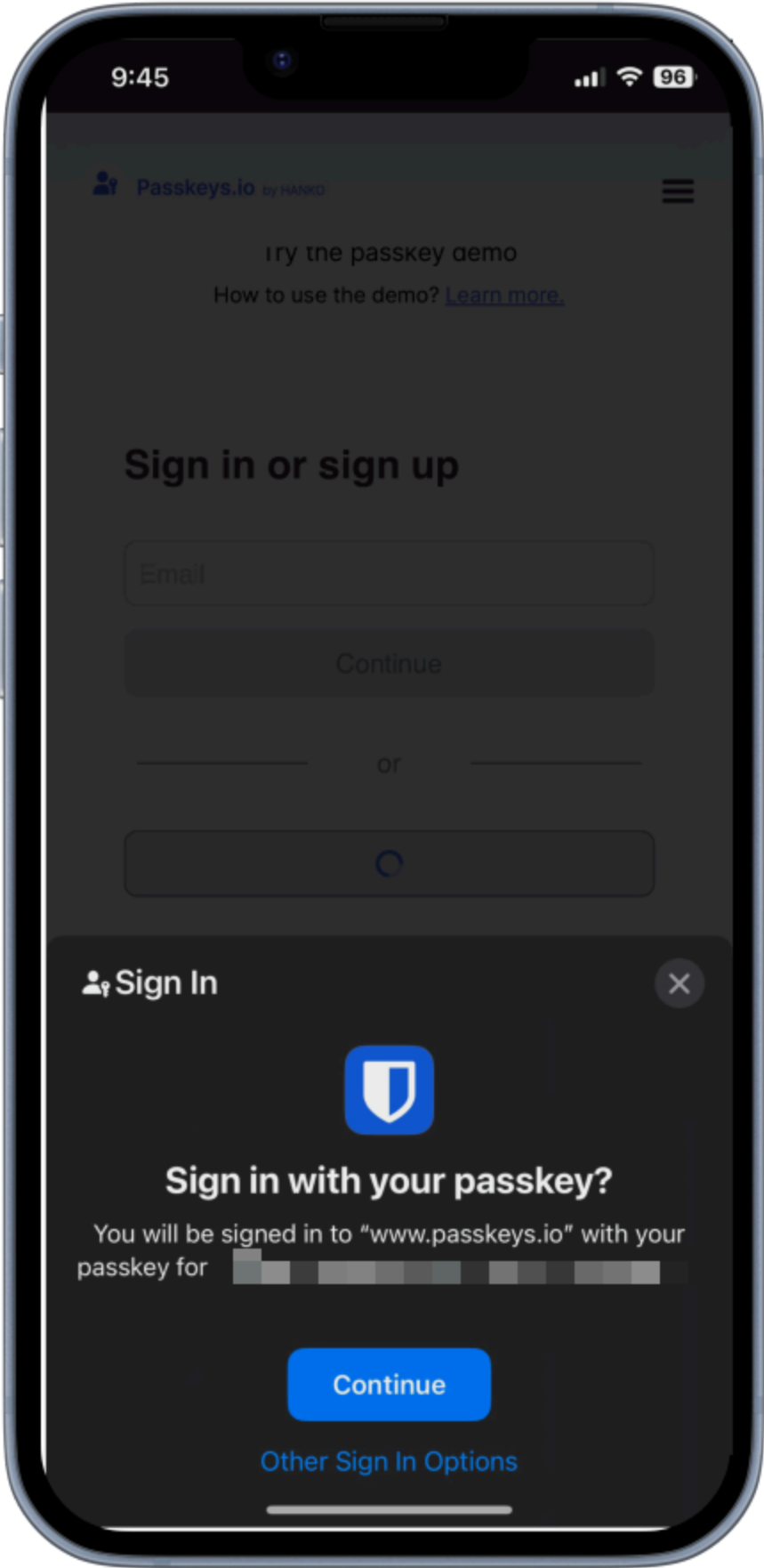
Duplicate passkeys cannot be saved for the same username and service. You may edit or overwrite an existing cipher if you wish to save a new passkey with the username and service.

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 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:



Sign in with passkey

Select **Continue**.**Note**

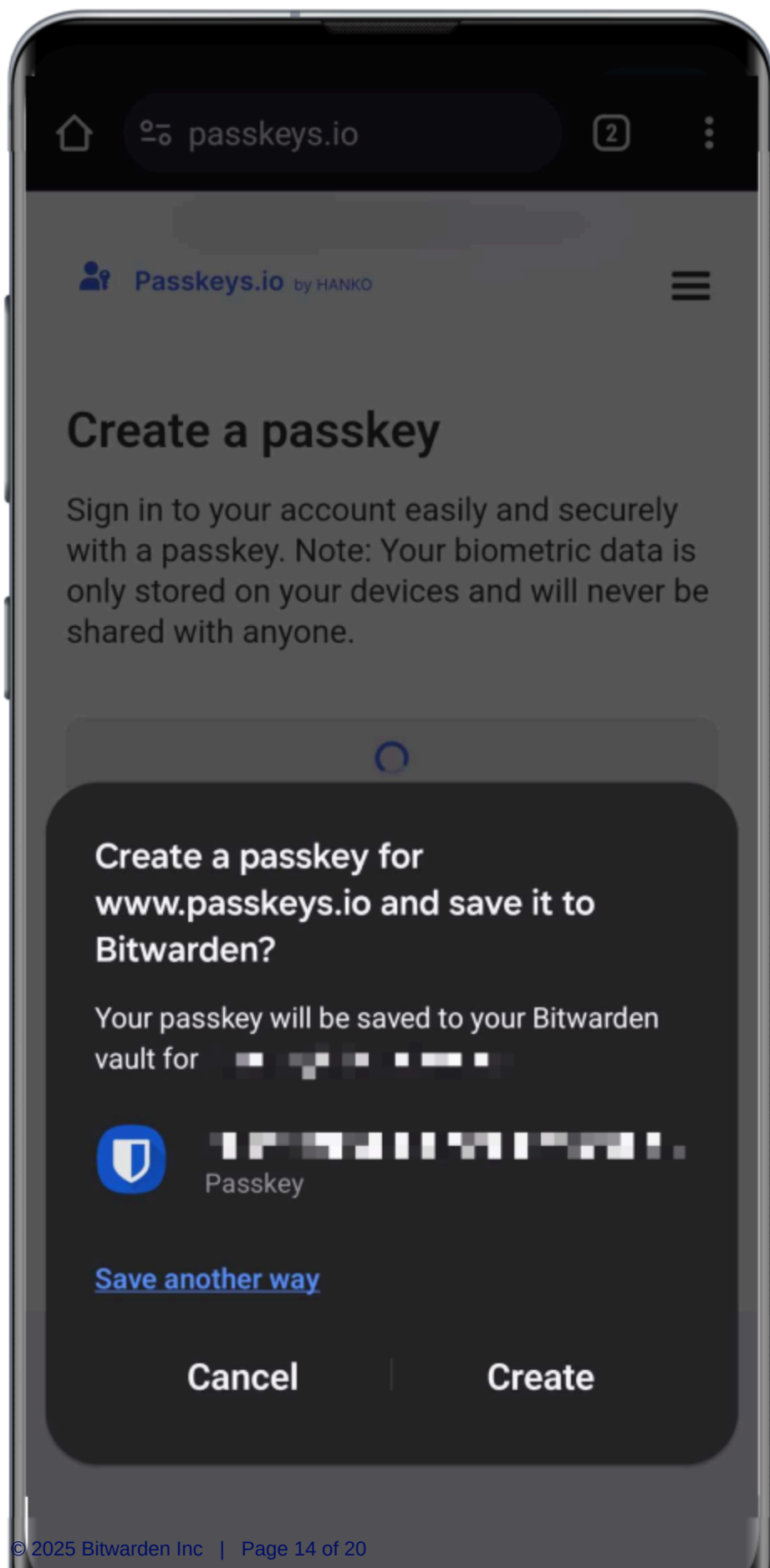
Select **Other Options** if you do not wish to store the passkey in Bitwarden or **Other Sign In Options** to sign in with a passkey not stored in Bitwarden.

⇒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. Please 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.

Create a passkey

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



Create a passkey

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:



Save or overwrite a passkey

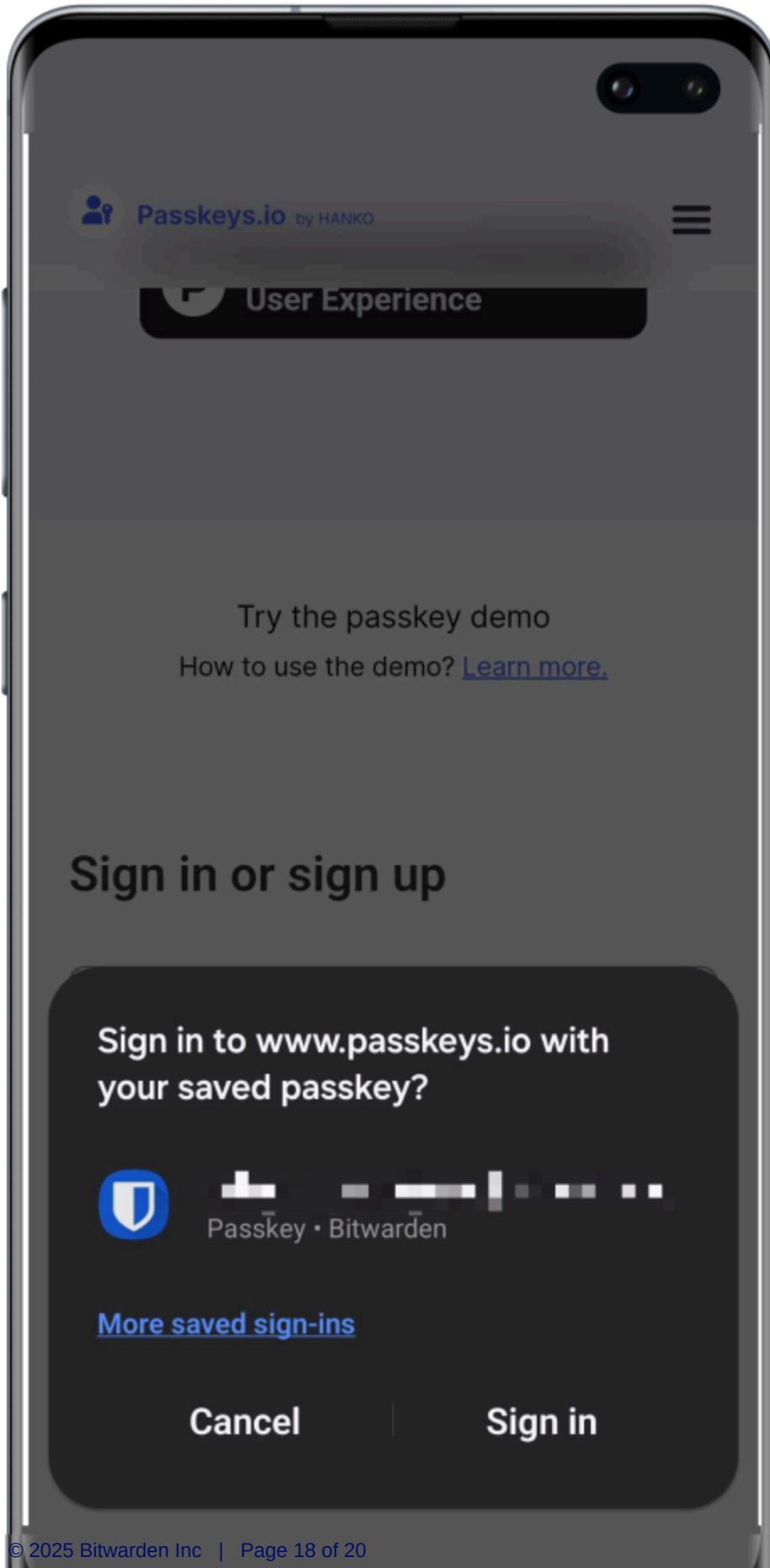
Duplicate passkeys cannot be saved for the same username and service. You may edit or overwrite an existing cipher if you wish to save a new passkey with the username and service.

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 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:



Sign in with passkey

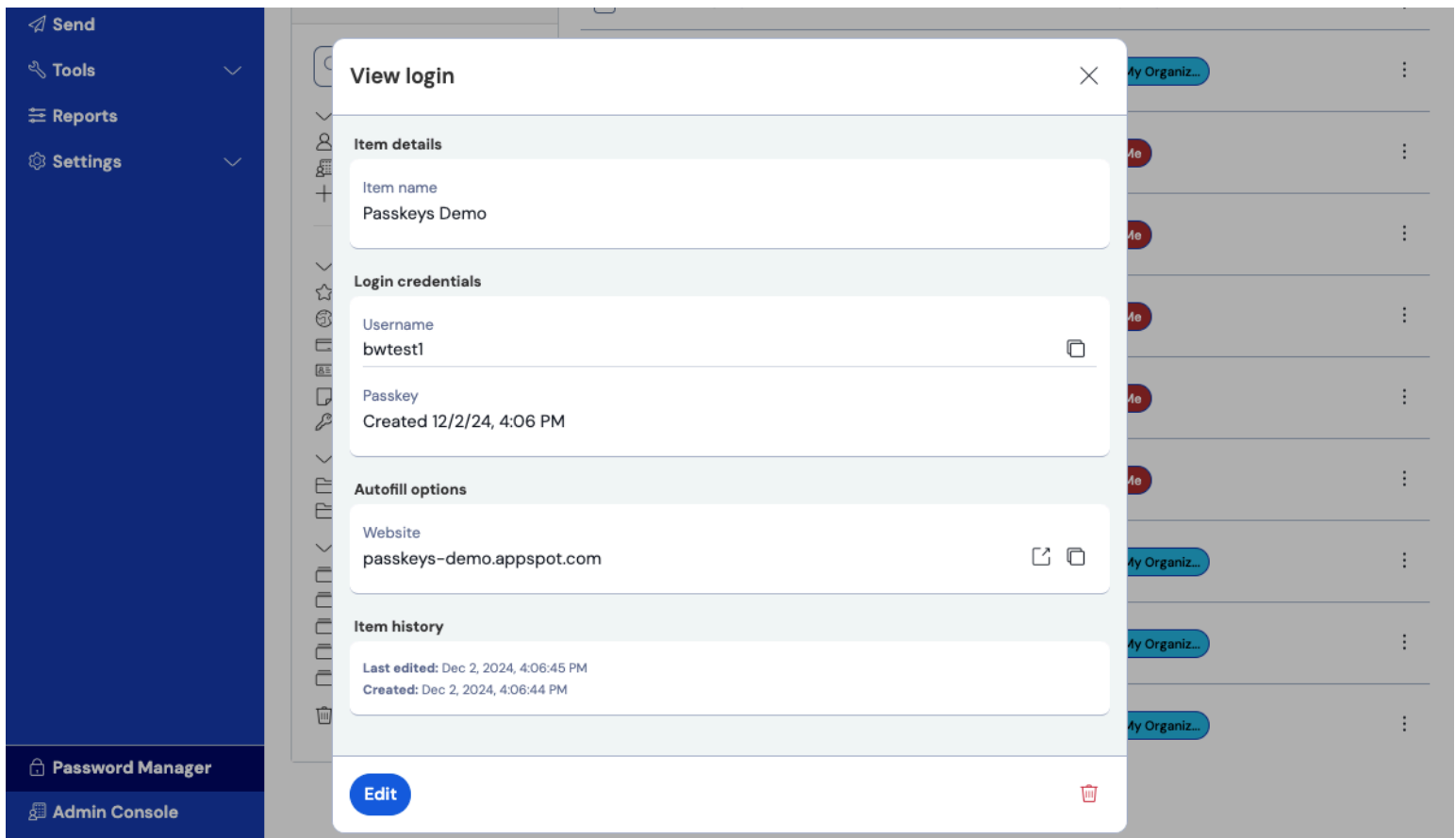
Select **Sign in** to use your passkey.

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

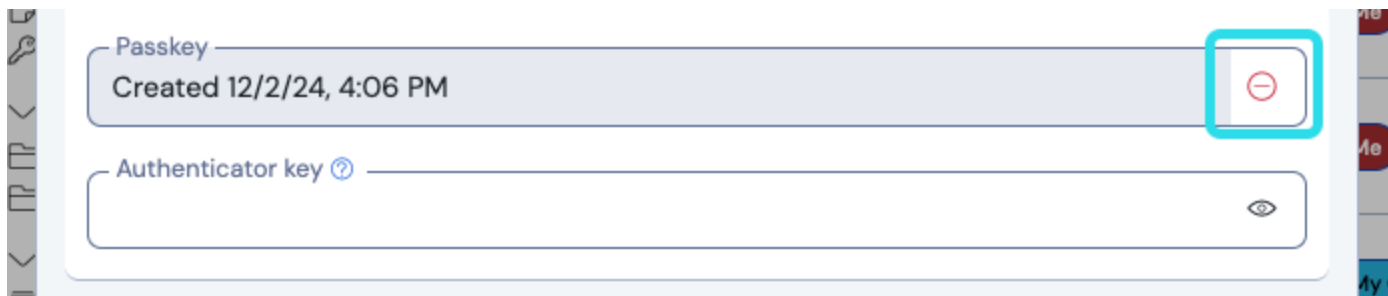
Note

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](#)).