

PASSWORD MANAGER > AUTOFYLL >

Lagring av lösenord

View in the help center:

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

Lagring av lösenord

Lösenord kan lagras och användas av Bitwarden Password Manager. Genom att använda webbläsartillägg och mobilappar kan användare logga in på sina favoritappar och webbplatser som har möjlighet att logga in med lösenord. Lösenord är ett säkert, lösenordslöst alternativ för användare att logga in på tjänster över sina enheter.

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.](#)

Utvecklade med de standarder som fastställts av [FIDO Alliance](#), lösenordsnycklar tillåter en användare att säkra sina konton och kringgå de sårbarheter som kommer med standardlösenordsautentisering, såsom nätfiske. Lagrade lösenord är skyddade med Bitwardens betrodda end-to-end-kryptering.

Vad är lösenord?

Nyckelnycklar är en ersättning för lösenord som ger snabb, enkel och säker inloggning till webbplatser och appar på en användares enheter. Mer exakt är "lösenordsnyckel" en konsumentvänlig term för en upptäckbar FIDO-referens som kan synkroniseras för att tillåta säkra lösenordslösa inloggningar över enheter, eller dedikeras till en enda maskinvara som en enhetsbunden lösenordsnyckel.

Appar och tjänster kan begära att lösenord som skapats med dem verifieras med en PIN-kod, lösenord, mönster eller biometrisk faktor när du sparar eller kommer åt dem. För mer allmän information om lösenord, se [Vanliga frågor om lösenord](#).

Typer av lösenord

Nyckeln lagras och anropas via Bitwardens webbläsartillägg och mobilappar. Detta innebär att både upptäckbara lösenord och icke-upptäckbara FIDO2-uppgifter kan lagras i Bitwarden och användas för att logga in på webbplatser med lösenordsfunktioner.

Använda lösenord med 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.

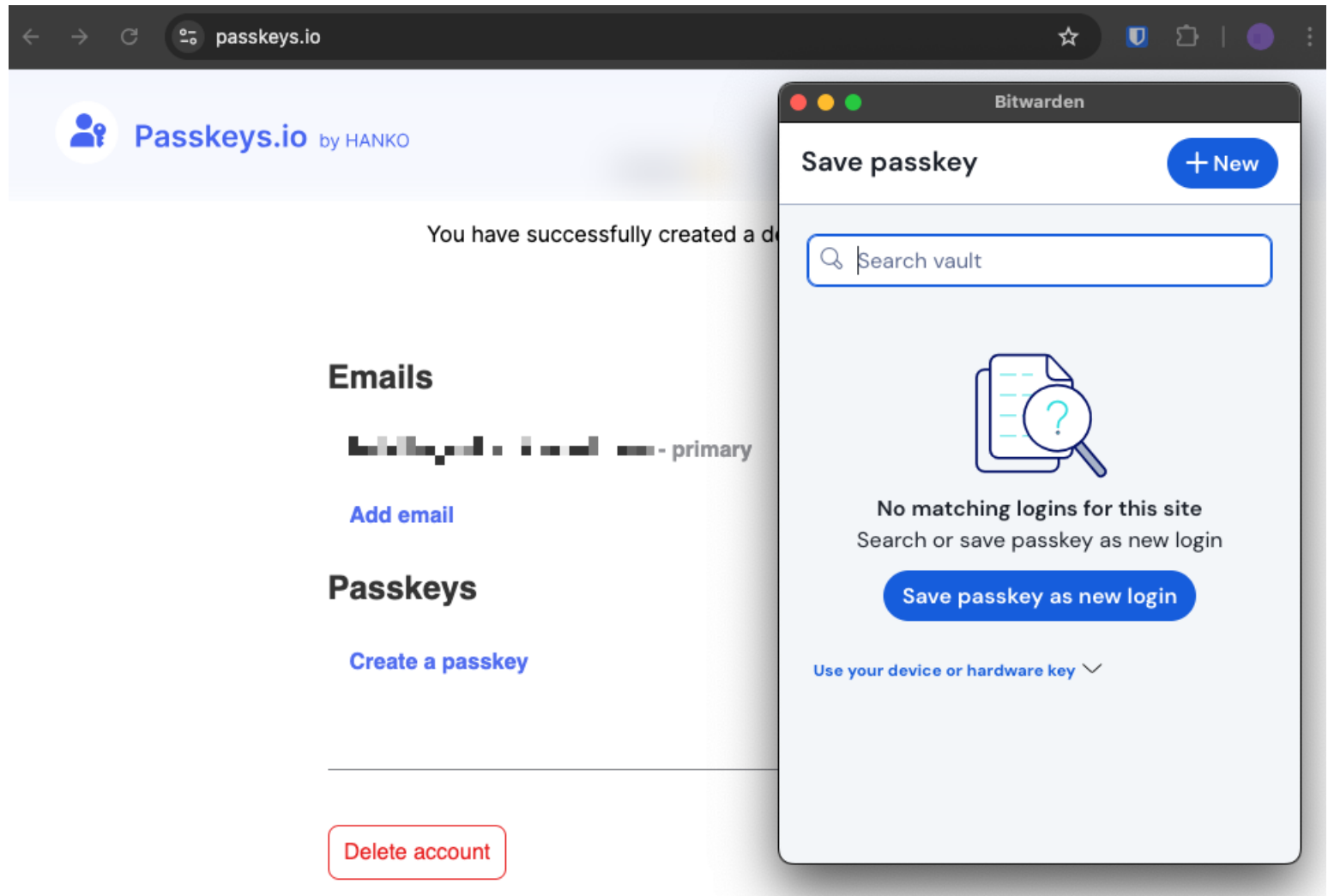
Ask to save and use passkeys

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:

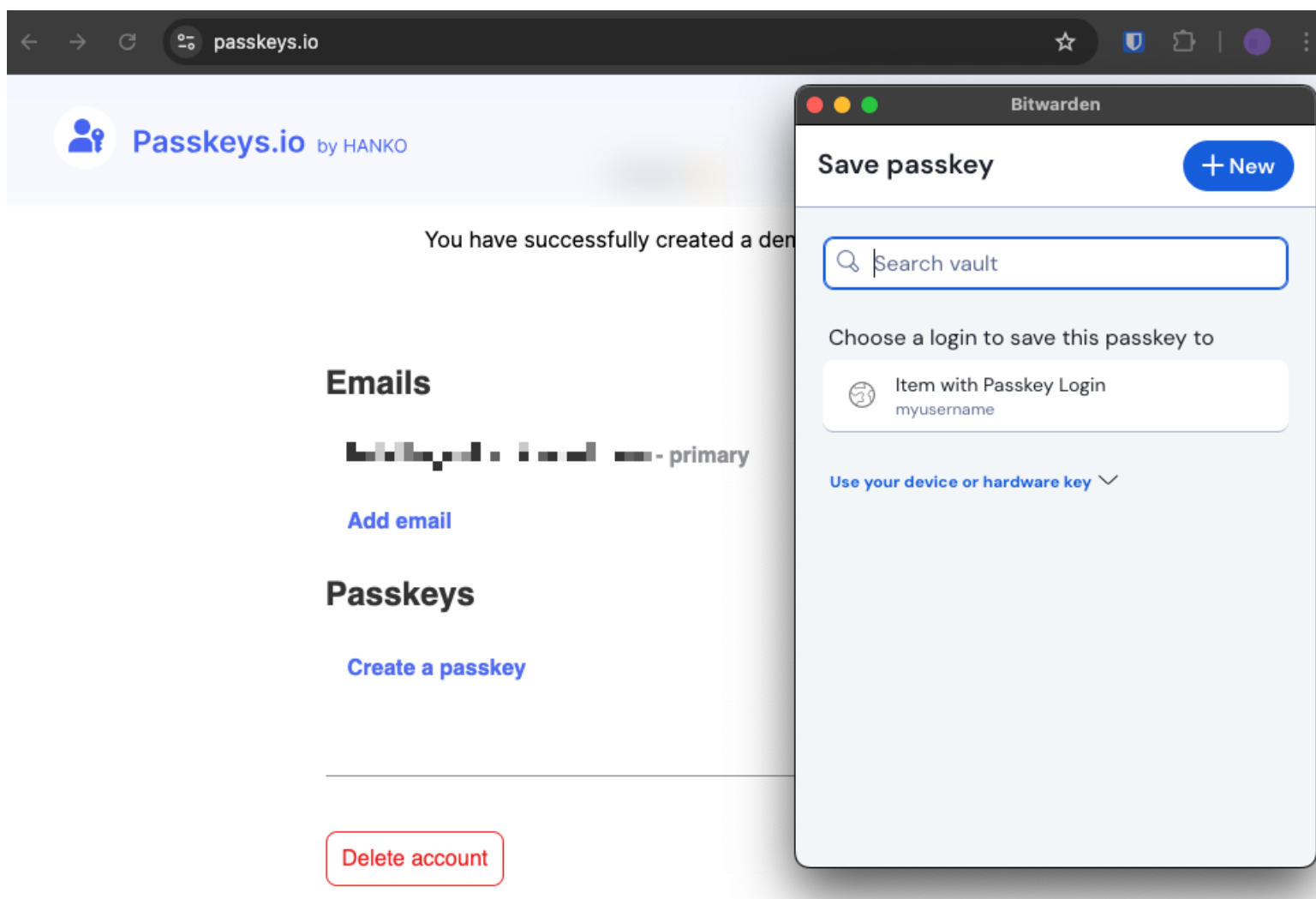


Save passkey

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

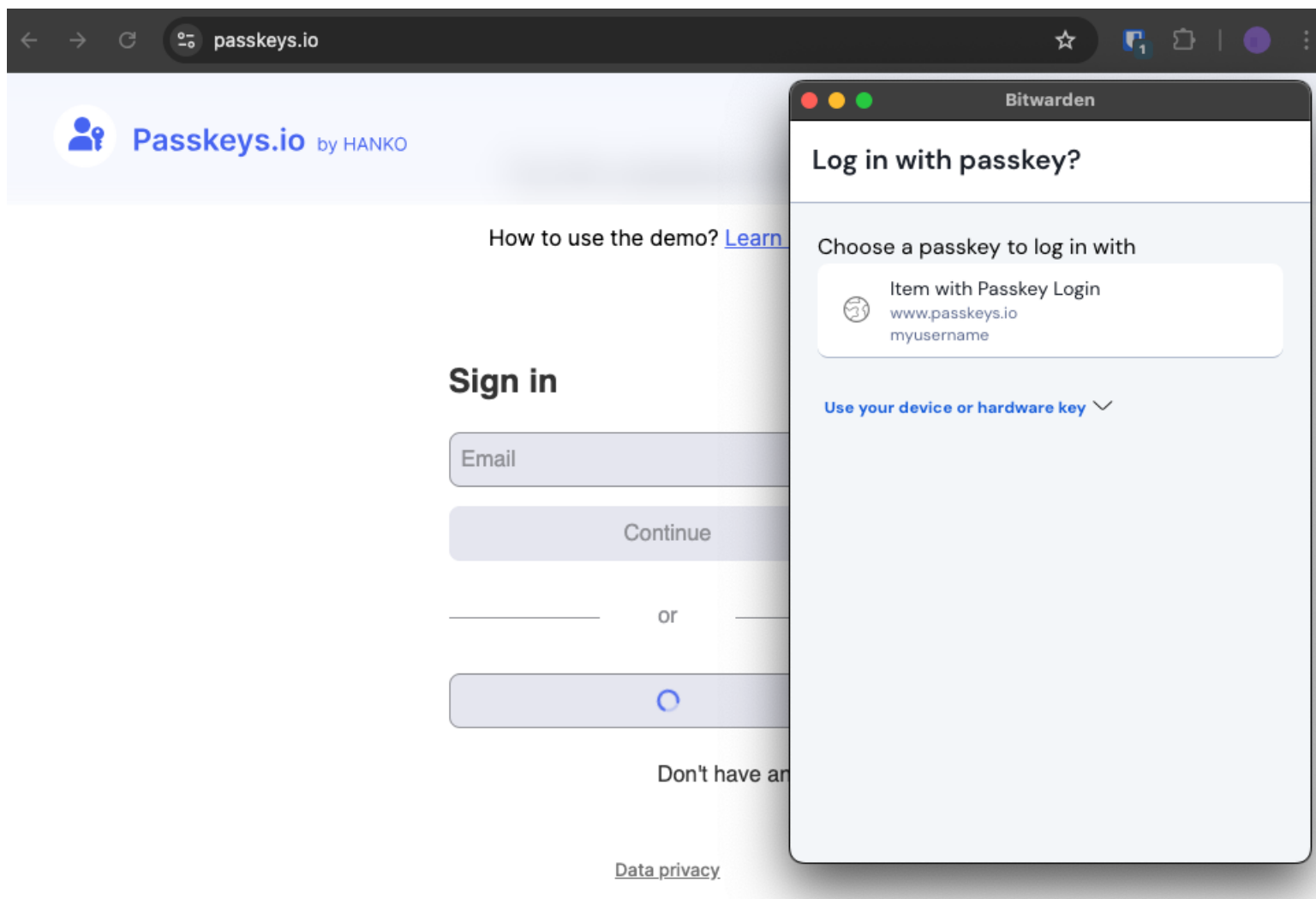
Only one passkey can be saved per login item. If a credential is saved in multiple places, for instance as two separate login items in the individual vault and organization vault respectively, a different passkey can be stored with each login item.

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.



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

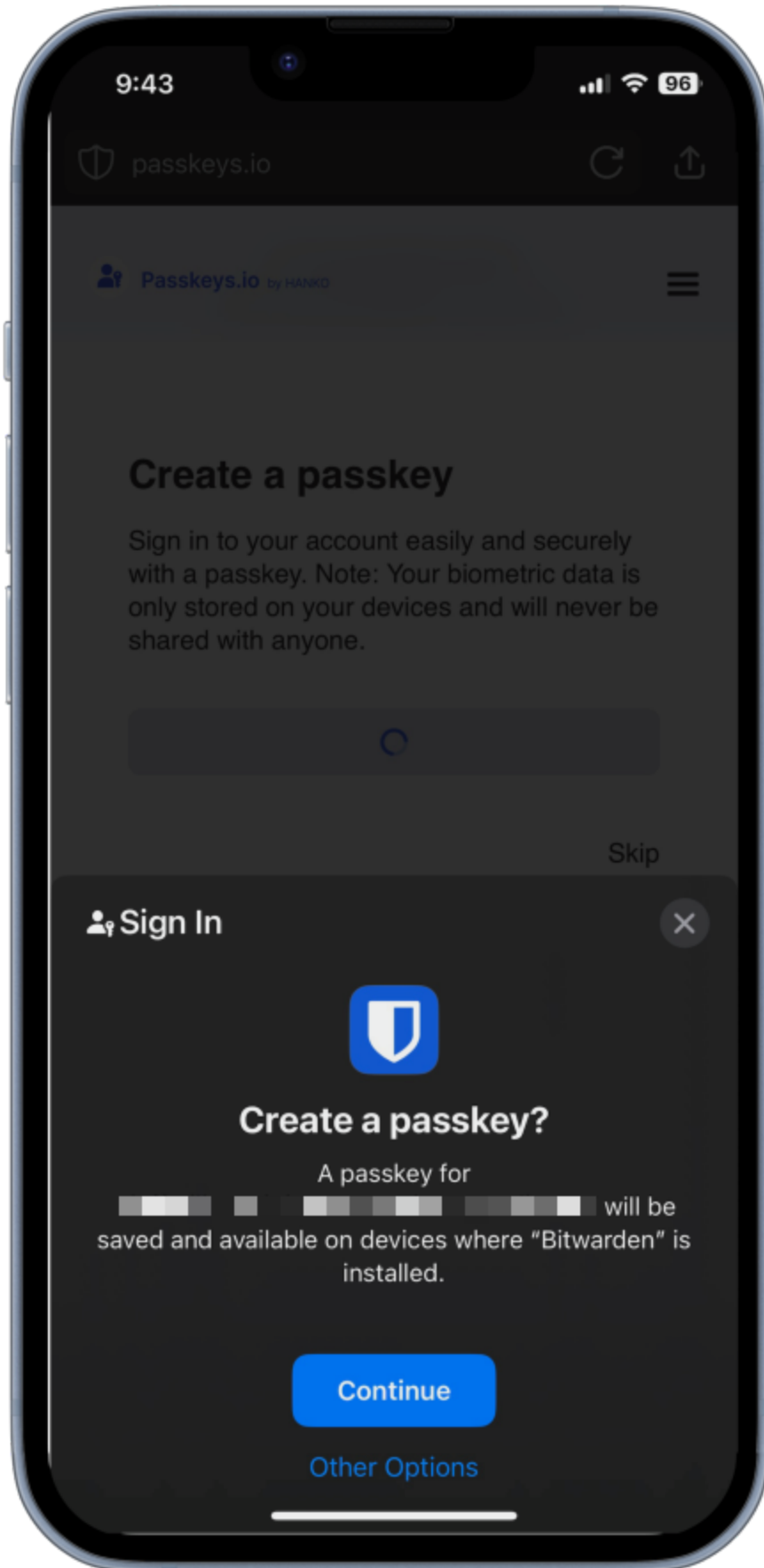
Setup Bitwarden for use with passkeys

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

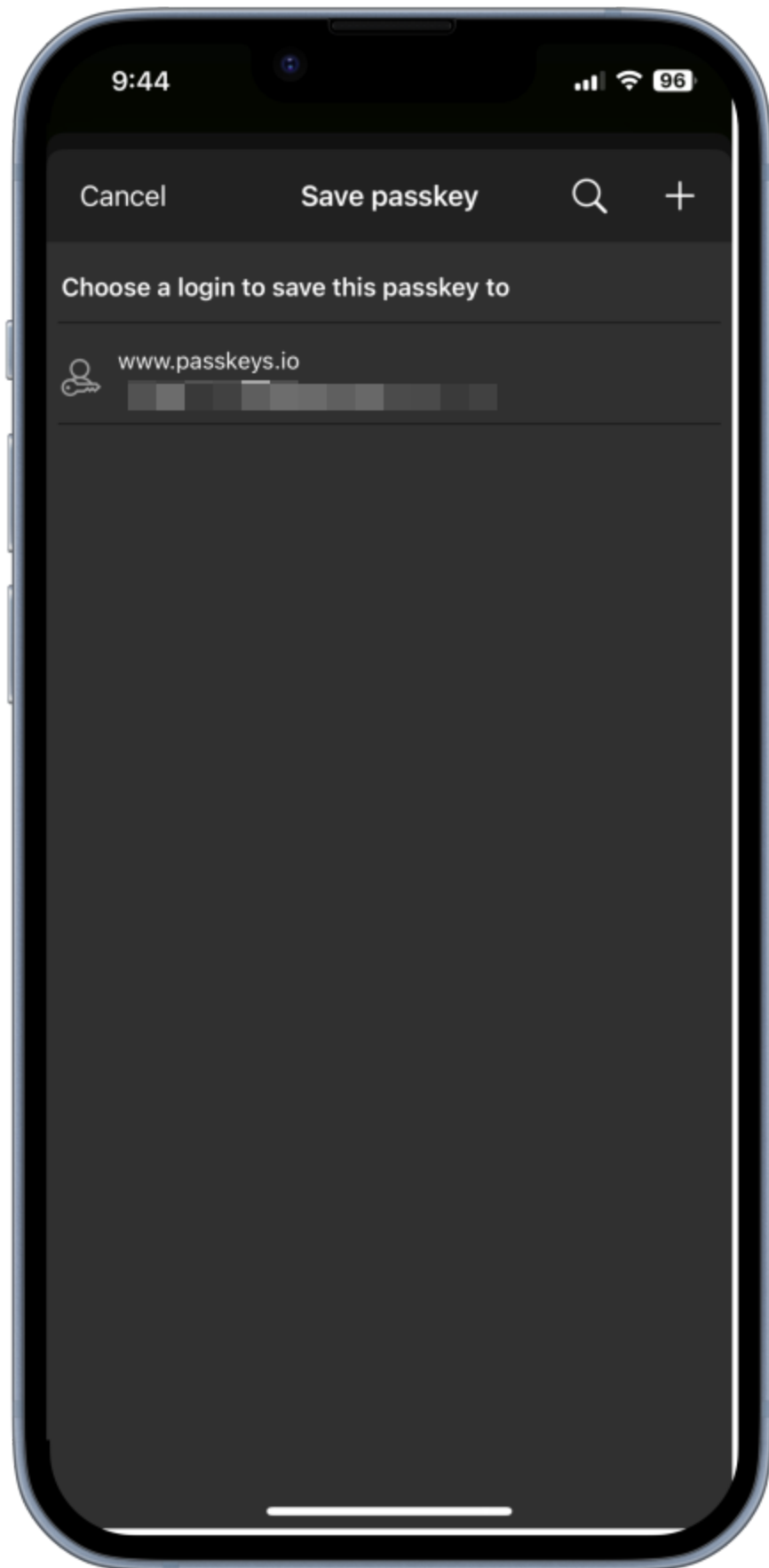
When creating a new passkey on a website or app, the iOS application will prompt you to store the passkey:



[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

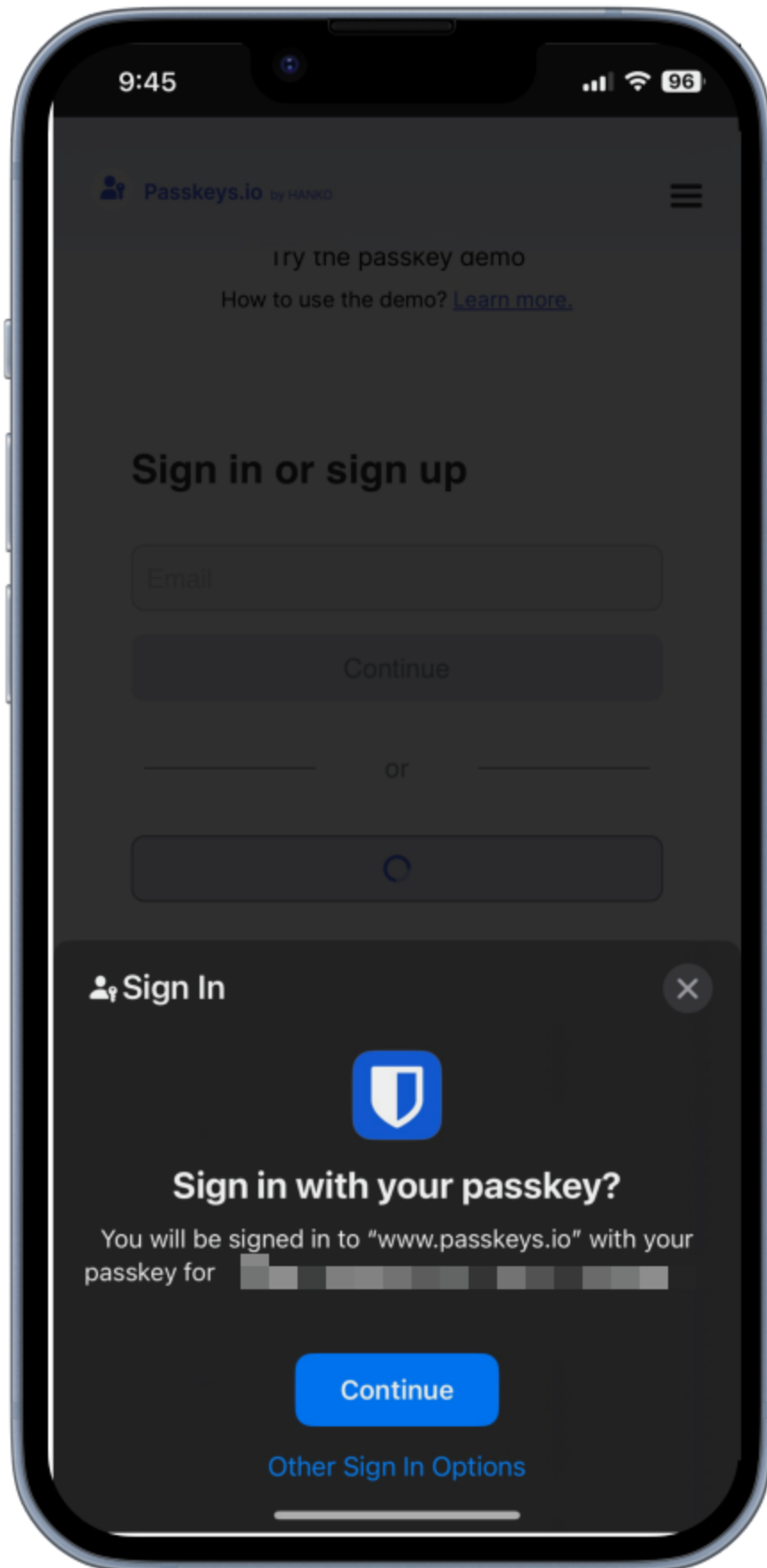
Duplicate passkeys cannot be saved for the same username and service. You may edit or overwrite an existing cipher if you wish to save a new passkey with the username and service.

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.

Warning

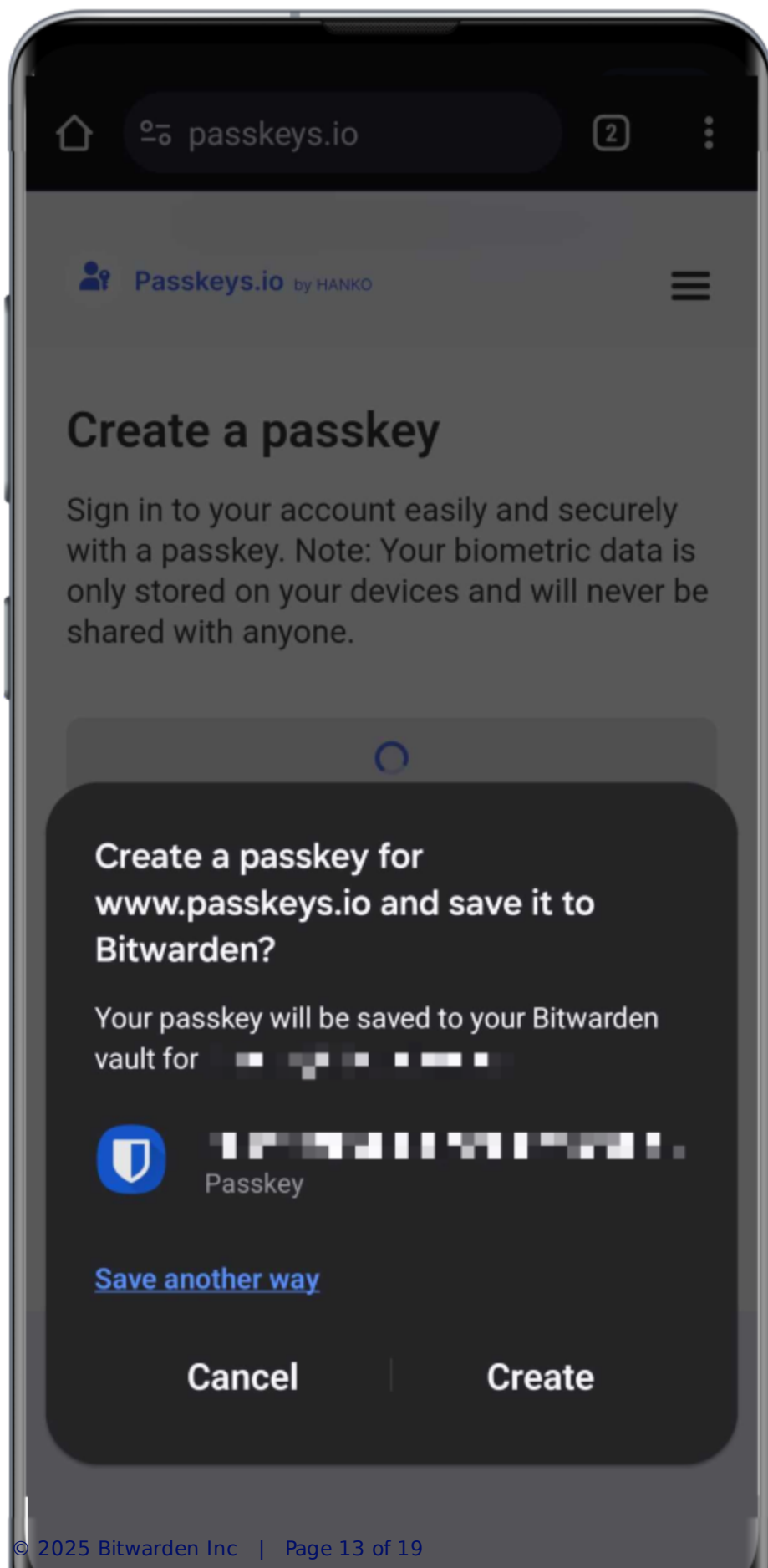
In order to activate Bitwarden as your preferred passkey provider it may be necessary to:

- 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.

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

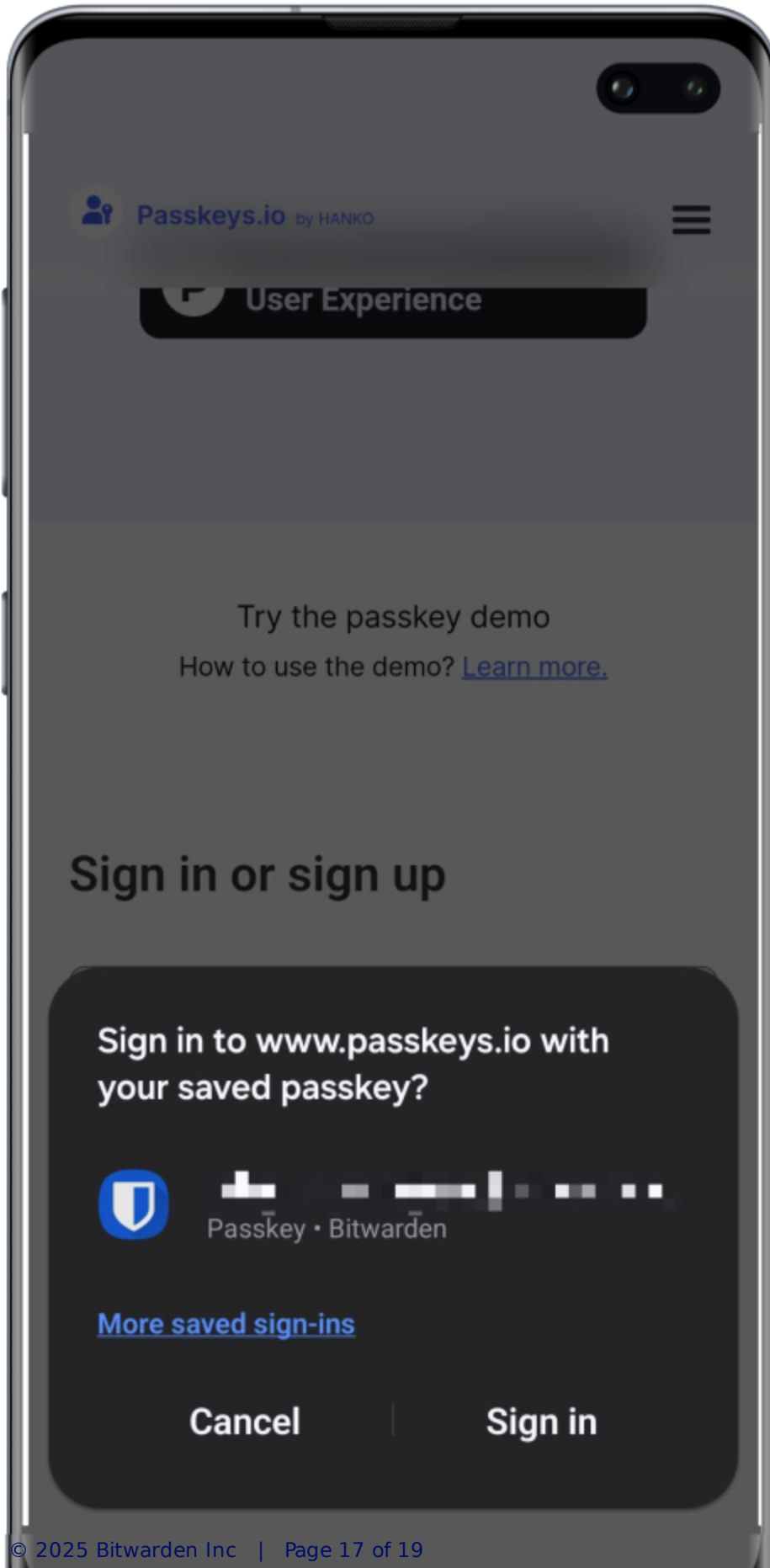
Duplicate passkeys cannot be saved for the same username and service. You may edit or overwrite an existing cipher if you wish to save a new passkey with the username and service.

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

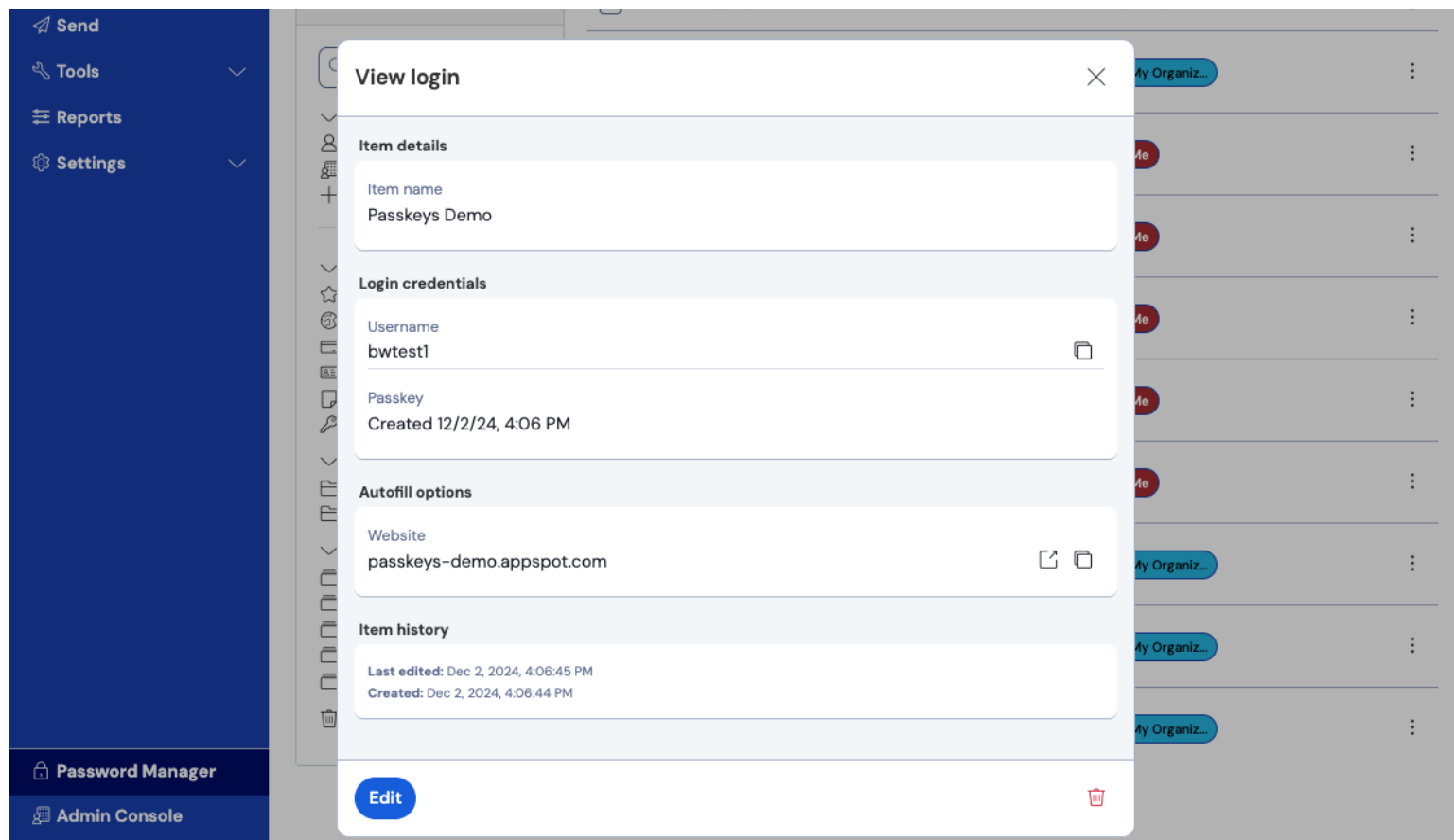
Select **Sign in** to use your passkey.

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.

Visa lösenord i Bitwarden

När en lösenordsnyckel har sparats kan den ses från vilken Bitwarden-app som helst och finns i fältet **Lösenord**:



The screenshot shows the Bitwarden interface with a 'View login' modal open. The modal displays the following information:

- Item details:** Item name: Passkeys Demo
- Login credentials:** Username: bwtest1, Passkey: Created 12/2/24, 4:06 PM
- Autofill options:** Website: passkeys-demo.appspot.com
- Item history:** Last edited: Dec 2, 2024, 4:06:45 PM; Created: Dec 2, 2024, 4:06:44 PM

The background shows the Bitwarden sidebar with options like Send, Tools, Reports, and Settings, and a list of items in the main area.

Passkey in your vault

Note

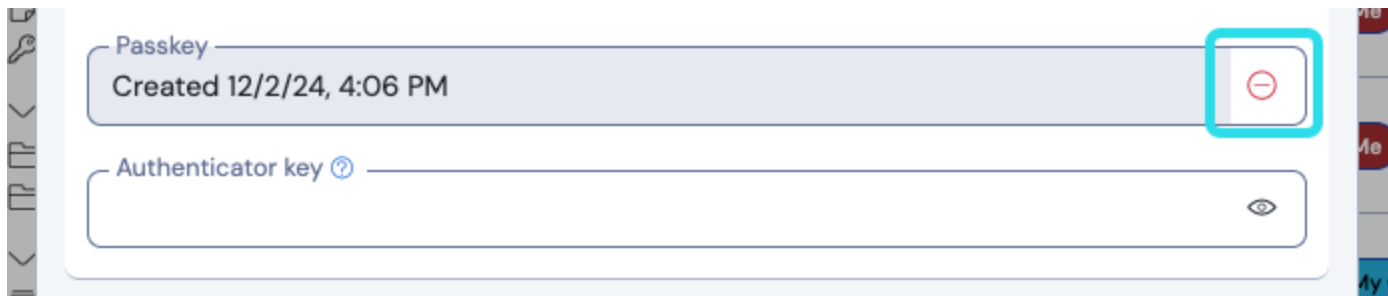
If master password re-prompt has been enabled on the login item, you will be required to re-enter your master password in order to access the passkey.

Tar bort lösenord

Så här tar du bort en lösenordsnyckel från ett valobjekt:

1. Öppna skärmen **Redigera** objekt från lösenordshanterarens webbapp, webbläsartillägg eller skrivbordsapp.

2. Välj raderingsikonen ⊖ för **lösenordsfältet**.



Delete a passkey

Vanliga frågor om lösenordshantering

Följande FAQ-objekt hänvisar till Bitwardens lösenordslagring. För allmän lösenordsinformation, se [Vanliga frågor om lösenord](#).

F: Kommer lösenord inkluderas om du [klona](#) ett valvobjekt?

S: Bitwarden kommer inte att kopiera en lösenordsnyckel när du slutför en klonåtgärd.

F: Ingår lagrade lösenord i Bitwarden-import och export?

S: Nyckelnycklar ingår i .json-exporter från Bitwarden. Möjligheten att överföra dina lösenord till eller från en annan lösenordsleverantör planeras för en framtida version.

F: Kan jag lagra lösenord i mobilappen?

S: Nyckelstöd för mobilapplikationer är tillgängligt för iOS ([läs mer](#)) och för Android ([läs mer](#)).