

Passkeys

Passkeys are a secure alternative to traditional passwords that let you log in to apps and websites without entering a password. Built on the standards set by the [FIDO Alliance](#), passkeys avoid the vulnerabilities of standard passwords, such as phishing.

Save passkeys in your WALLIX Enterprise Vault and use the browser extension or mobile apps to autofill them across the apps and websites you use every day. Stored passkeys are protected by the same end-to-end encryption as the rest of your vault.

Page Navigation

- [What are passkeys?](#)
- [Save and autofill passkeys](#) - [Browser extension](#) - [iOS](#) - [Android](#)
- [View passkeys in your vault](#)
- [Delete a passkey](#)
- [Export and import passkeys](#)

What are passkeys?

Passkeys are a replacement for passwords that provide fast, easy, and secure sign-ins to websites and apps. A passkey is a discoverable FIDO credential that can either be synced to allow passwordless sign-in across your devices, or dedicated to a single piece of hardware as a device-bound passkey.

Some apps and services may ask that a passkey be verified with a PIN, password, pattern, or biometric factor when you save or use it.

Passkeys are stored and used through the WALLIX Enterprise Vault browser extension and mobile apps. Both discoverable passkeys and non-discoverable FIDO2 credentials can be stored and used to sign in to websites that support passkeys.

Note: the browser extension will not offer to save or use a passkey for any domain on your [excluded domains](#) list.

Save and autofill passkeys

Browser extension

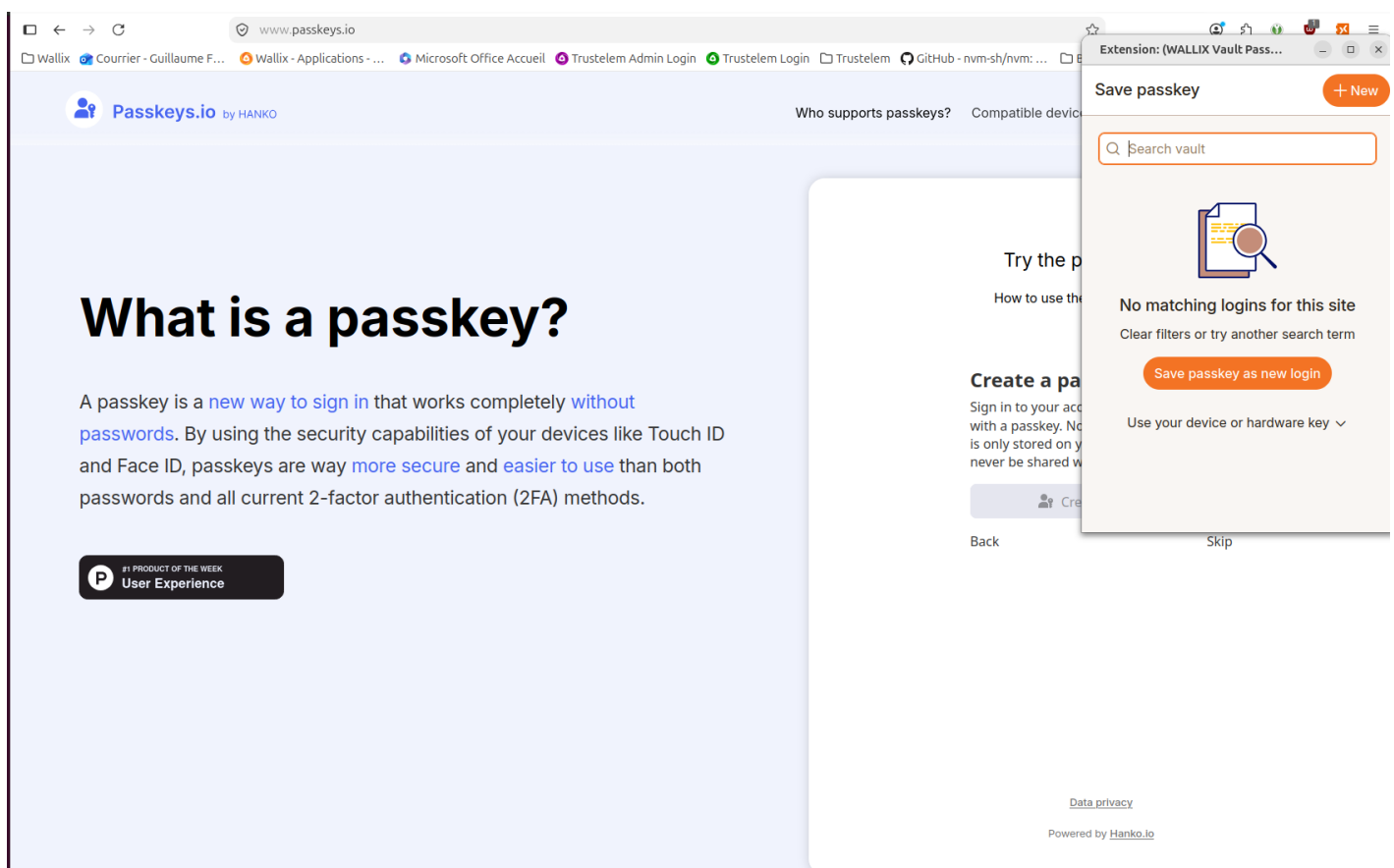
Allow passkeys in the extension

1. Open the WALLIX Enterprise Vault browser extension.
2. Go to **Settings** → **Notifications**.
3. Make sure **Ask to save and use passkeys** is checked.

If there are sites you don't want to use WALLIX Enterprise Vault for passkeys with, add them to your [excluded domains](#).

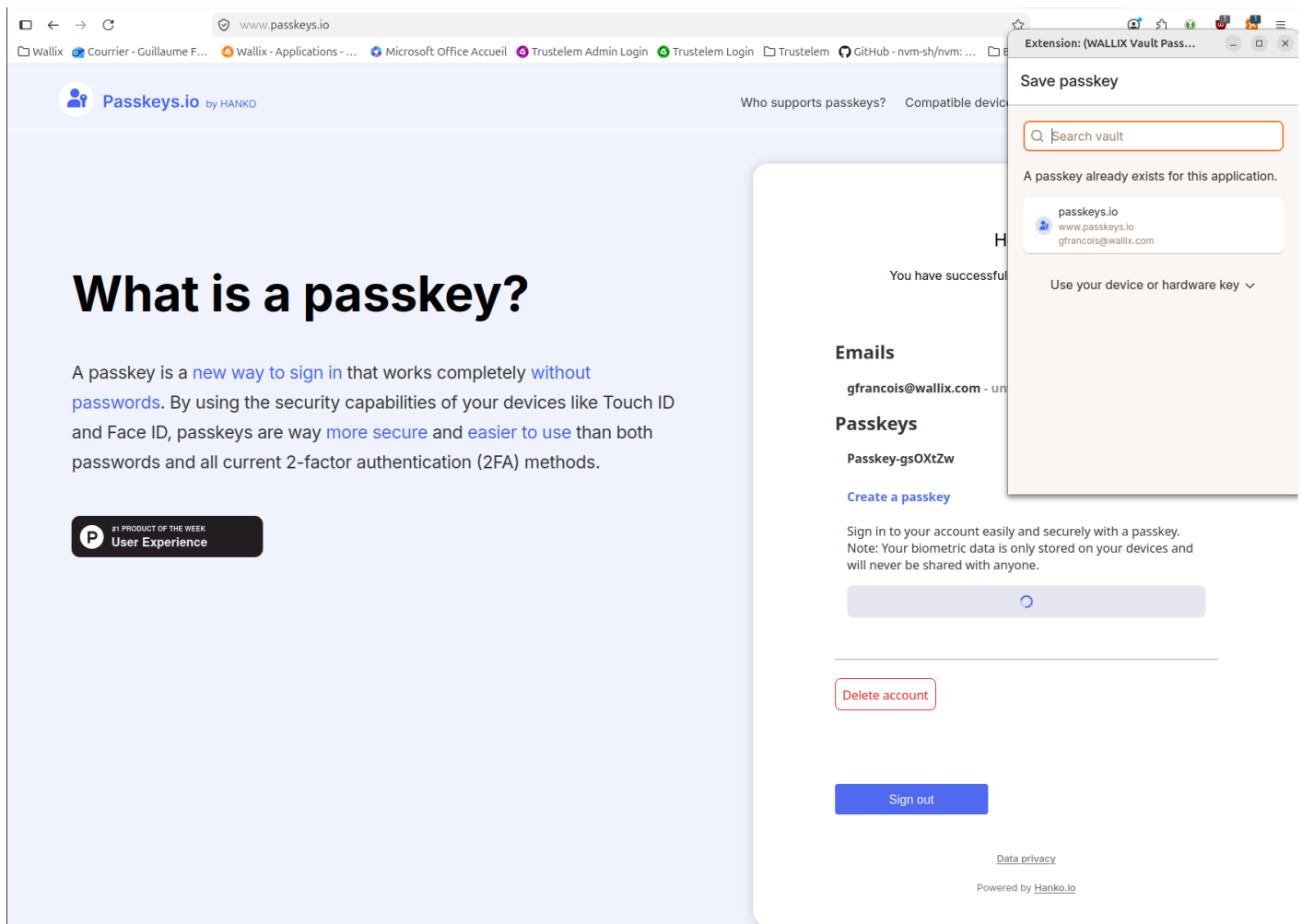
Create a passkey

When you create a new passkey on a website or app, the browser extension will prompt you to store it.



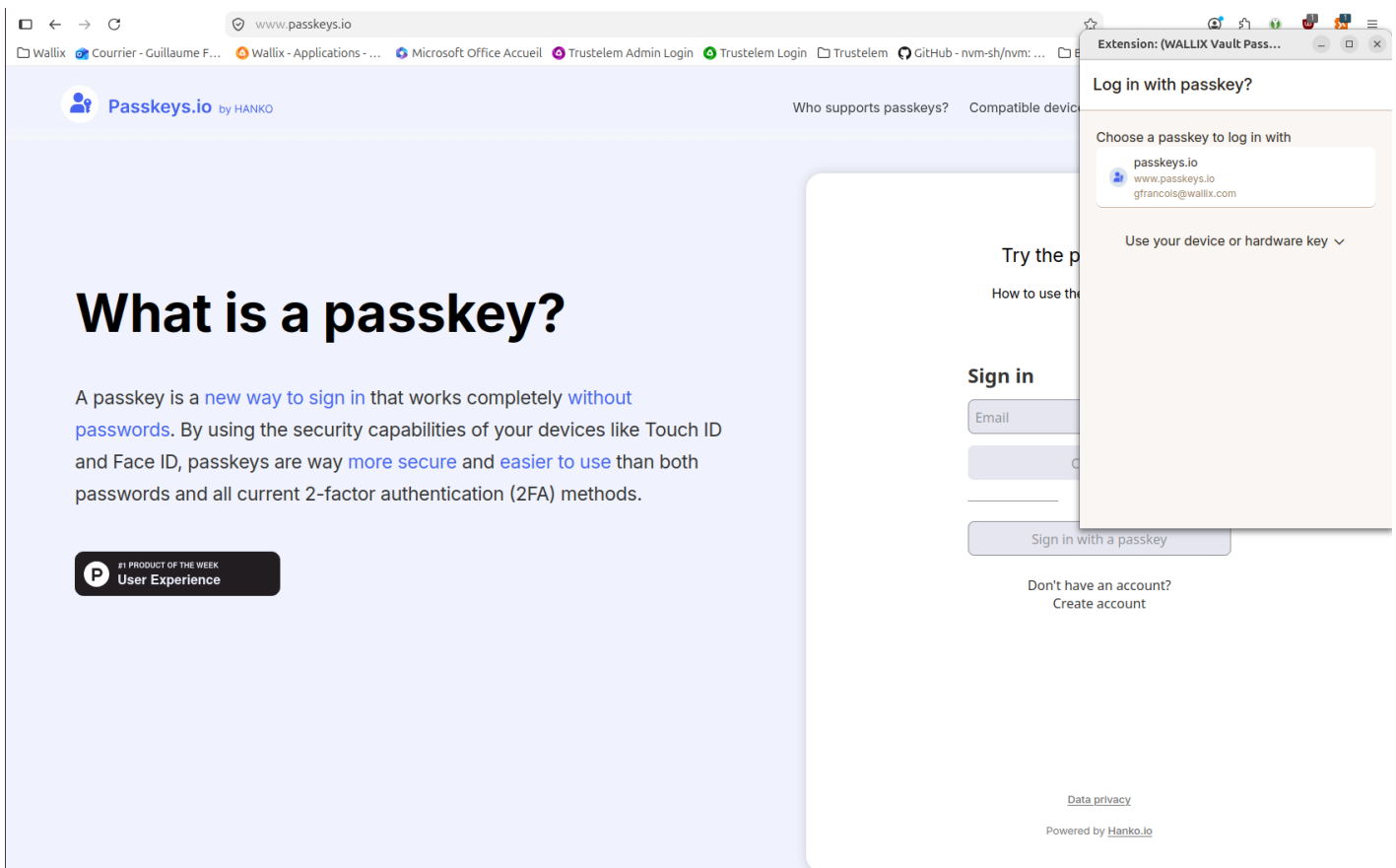
Note: select **Use your device or hardware key** if you don't want to store the passkey in WALLIX Enterprise Vault.

Only one passkey can be saved per login item. If a passkey already exists for a service, you can either overwrite it or select the **Add** icon to create a new login item and store an additional passkey.



Sign in with a stored passkey

1. Make sure **Ask to save and use passkeys** is turned on (**Settings** → **Notifications**).
2. Start the passkey sign-in on the website.
3. In the window that appears, select your saved passkey.



You can also authenticate with a passkey directly from the inline autofill menu.

Note: if you previously chose **Use your device or hardware key** for a site, WALLIX Enterprise Vault won't offer to save or fill a passkey for it. To change this, remove the site from your blocked domains — the extension will then ask to save the passkey again next time you sign in.

View passkeys in your vault

Saved passkeys can be viewed from any WALLIX Enterprise Vault client (web app, browser extension, mobile apps, desktop app). Open the login item — the **Passkey** field shows the date and time the passkey was created.

Note: if [master password re-prompt](#) is enabled on the item, you'll be asked to re-enter your master password to access the passkey.

Delete a passkey

To remove a passkey from a vault item:

1. Open the item's **Edit** screen from the web app, browser extension, or desktop app.
2. Select the **Delete** icon next to the **Passkey** field.
3. Confirm by selecting **Delete**.
4. Select **Save**.

Export and import passkeys

Passkeys are included in JSON exports of your vault and can be re-imported into a WALLIX Enterprise Vault account the same way as any other export.

Revision #6

Created 11 September 2026 07:13:16 by WALLIX Admin

Updated 11 September 2026 09:07:18 by WALLIX Admin