RESOURCE CENTER

Passwordless Future: A Comprehensive Passkeys FAQ

Get the full interactive view at
https://bitwarden.com/resources/passkeys-faq/

bitwarden

Passkey overview

What is a passkey and how does it work?

Passkeys are a form of authentication that allow you to quickly create and sign into accounts – without having to use a less secure password. This single-step, secure login method replaces traditional authentication methods, as well as the two-factor authentication (2FA) process. Even better, with passkeys, you'll never create a weak password again, because you'll never need to create a password again.

Do passkeys replace physical hardware keys, like Yubikeys?

A modern Yubikey can be used as a form of passkey. Specifically, they are what is known as a Security Key or "device-bound passkey" – where the key itself lives on the small device and is never synced or backed up. This can make them harder to use than a Synced Passkey, but can be useful in certain scenarios.

Are passkeys the same as passwordless?

Yes. Because passkeys do not require a password, they are considered a passwordless method of authentication. Note that Passkeys are in general safer than other means of passwordless authentication that can more easily be phished.

What's the best way to use passkeys?

Using a passkey is much simpler than you might think. When you sign up for a new account, instead of creating a traditional username and password (and the additional two-step login enrollment), you create a single passkey. That passkey can be coupled with the biometrics on your device (such as a fingerprint scanner) or a PIN if the passkey requires user verification. So when you go to log into the account, you'll only be required to authenticate via biometrics or PIN to gain entry. Biometrics are only used locally on your device and are never sent to the website.

What is the process to set up a passkey? How does that process change when I go to a site or app in the future?

When a website or app that previously used a traditional username/password enables support for passkeys, it's often enough with a click of a button to create your first passkey. The process is as easy as unlocking your device. In the background, when you create a passkey, it will generate a pair of cryptographic keys. The first is the public key, which is stored on the website for which you are creating the account. The second is the private key, which is stored on your device or your Bitwarden Vault. This key pair is protected on your device by your biometric fingerprint or face scan.

What information is required when setting up a passkey?

When you create a passkey for a site, you will have to first log in with your existing username and password. The server will then push a request to your browser to provide specific encryption information. You will then have to approve the request using e.g. biometrics (fingerprint scanner or face unlock) or your device PIN code. Upon successful verification, your device will generate the key pair and send the public key to the site. And that's all the information you'll be required to provide when setting up a passkey.

Where are my passkeys stored?

The public key is stored on the website and the private key is stored on your device or in your passkey provider, e.g. your Bitwarden Vault.

Table of Contents

Additional Resources

Page: Innovating in passwordless

Blog: Bitwarden launches passkey management

Blog: Log into Bitwarden with a passkey

Blog: What are passkeys?

Blog: How do passkeys work?

Product: Passwordless.dev

Webcast: Passkeys and Bitwarden

Webcast: Passkeys & you

Passkey security

From a security perspective, how do passwords and passkeys compare?

Passkeys are more secure than the traditional username/password authentication method for a number of reasons. First and foremost, you won't be able to use easy-to-crack passwords, such as "*password*." Also, 2FA is built into the passkey and the only way someone could access your account would be to have both the private key and your biometric login or device pin code.

Do I need 2FA with my passkey?

No, because 2FA is built into the passkey that is provided to the website during the login process. Each website may choose to include an additional step for logging in, though most do not.

Can my passkey be hacked?

Nothing is 100% foolproof. However, hacking a passkey would require considerable effort to not only gain access to the device where the private key is stored but to also break into your device, e.g. recreating your biometric login (fingerprint or face) or device pin code. Because of this, passkeys are far more secure than traditional methods.

What happens if I lose my phone? How do I recover my passkey with nothing like a password to identify myself?

Passkeys are often able to sync across your devices, however not all platforms support this yet. Bitwarden will allow you to store your passkeys in your vault that is backed up and syncs between all your devices. Should you somehow lose your passkeys, most sites should have recovery options, so you can create a new passkey for your account. This will, of course, be on a site-by-site basis.

What happens if my device is stolen? Can a thief gain access to passkeys in that way?

The only way a thief could successfully use your passkeys on your device is if they can also unlock your device, effectively gaining full access to your data. However, each use of a passkey often requires user verification such as biometrics or re-entry of your device pin, so stealing your device while unlocked would not be enough.

Using passkeys with Bitwarden

Google recently announced passkey support. Is this the same thing that Bitwarden is announcing?

Partly. Google announced that it has added support for passkey authentication for Workspaces accounts, meaning users can sign into their Google Workspace with a passkey instead of their usual password. Similarly, Bitwarden users will be able to access their Bitwarden accounts with a passkey instead of their master password.

Bitwarden also announced that users will be able to save, store, and manage registered passkeys associated with the websites and applications they use right within their vaults. So, Google now makes it possible to use passkeys for accounts and Bitwarden is capable of storing passkeys in vaults.

Do I use the same passkey regardless of the browser I'm on or will each site require a different passkey depending on the browser or device?

The passkeys stored in Bitwarden are synced passkeys, meaning that any browser where you are logged into the Bitwarden extension or where you have the Bitwarden mobile app installed, you can access your accounts using the same passkeys without needing to create new ones. If you don't store your passkeys in Bitwarden it will depend on how well the browser integrates with your device OS (where the passkeys are stored).

What are some examples of sites that support passkeys?

The growing list of sites that support passkeys at the moment include Best Buy, Cloudflare, eBay, Google, Kayak, PayPal, and GitHub. A community-sourced Passkey Index is available on GitHub.

How will I use passkeys with Bitwarden? Do I still need a master password?

Users can use a passkey to access their accounts without a master password for the web app using supported browsers. Passkeys can also be created and stored in Bitwarden vaults for accessing sites supporting passkeys.

Can passkeys be used across platforms? If not, are there any issues with having different passkeys depending on the platform you're using?

There are two types of passkeys, device-bound passkeys and synced passkeys. Device-bound passkeys are limited to the device where they were created. Synced passkeys can be stored inside a passkey provider like Bitwarden, and used wherever they are logged in.

Will I be locked into using passkeys if I adopt it?

That will depend on the site or the account. Some sites may only choose to offer passkey authentication, while others may offer traditional username/password authentication, username/password/2FA authentication.

Can passkeys be shared with other trusted individuals?

That depends on the platform. Some platforms, including Bitwarden, make it possible to share passkeys with trusted individuals.

Is there support, such as a live chat representative to speak with if I'm having trouble with my passkey?

That will depend on the site. If a site supports passkey authentication and they offer support, they will be able to answer your questions regarding passkey authentication for that particular site.

If I no longer want to use my passkey, can I remove it?

Yes. This will be done in the same way you would remove a password on your device.