



Using a Password manager to hold passkeys

You can safely use a modern password manager to store and use passkeys, provided it explicitly supports them and you protect the vault with a strong master password (and ideally hardware-backed 2FA). For most people this is currently the most practical way to sync passkeys across different devices and operating systems. [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#)

What passkeys are

Passkeys are a replacement for passwords that use public-key cryptography instead of something you remember. The website holds a public key, while your device (or password manager) stores the private key and proves possession when you sign in, so there is nothing reusable for attackers to steal in a database breach. [\[5\]](#) [\[1\]](#)

How password managers handle passkeys

Several password managers (1Password, Dashlane, Keeper, Bitwarden, Google Password Manager, etc.) can now create, store and autofill passkeys in the same vault as your passwords. They encrypt the private key in your vault, sync it across your signed-in devices, and then present it to the site when you choose the relevant account during login. [\[2\]](#) [\[3\]](#) [\[6\]](#) [\[7\]](#) [\[1\]](#)

Security pros of using a manager

Using a password manager for passkeys gives you cross-device portability, so you are not locked to a single platform's ecosystem. It also lets you manage both passwords and passkeys in one place, including sharing specific credentials with family or team members where supported. [\[3\]](#) [\[4\]](#) [\[1\]](#) [\[2\]](#)

Security considerations and limitations

The trade-off is that your passkeys are now protected by the same factors as your password vault, so your master password, device security and second factor become critical. Some security experts argue that leaving passkeys bound to a hardware authenticator or platform (like iCloud Keychain or a hardware security key) can reduce attack surface further, at the cost of convenience. [\[8\]](#) [\[9\]](#) [\[4\]](#) [\[3\]](#) [\[5\]](#)

Practical setup tips (for your situation)

Given you already use tools like 1Password and multiple Apple and Windows devices, the most straightforward approach is to enable passkey support in your existing manager and use it as the primary store. You can still keep platform stores (iCloud Keychain, Google Password

Manager) on for redundancy, but be deliberate about which one you treat as the “source of truth” to avoid confusion. [6] [7] [9] [4] [1]

Would you like a step-by-step for enabling and testing passkeys in the specific password manager you’re using now (e.g. 1Password, Bitwarden, or another)?

✱✱

1. <https://1password.com/product/passkeys>
2. <https://www.dashlane.com/blog/how-to-manage-passkeys>
3. <https://www.keepersecurity.com/blog/2023/10/05/how-to-manage-passkeys/>
4. <https://maketechesasier.com/passkeys-in-password-manager/>
5. <https://www.wired.com/story/what-is-a-passkey-and-how-to-use-them/>
6. <https://support.google.com/accounts/answer/6197437?hl=en&co=GENIE.Platform%3DAndroid>
7. <https://support.google.com/accounts/answer/6197437?hl=en&co=GENIE.Platform%3DDesktop>
8. https://www.reddit.com/r/Passkeys/comments/1p5nnoo/storing_passkeys_in_ones_password_manager_is_not/
9. <https://support.google.com/chrome/answer/13168025?hl=en&co=GENIE.Platform%3DDesktop>
10. <https://www.wired.com/story/how-to-use-google-passkeys/>