Getting Started With Passkeys, One Service at a Time

Passkeys help do away with passwords for logging into websites and cloud services. This Tech Tip outlines ways to get started.

Robert Lemos, Contributing Writer

January 3, 2024

6 Min Read

Latest Articles in DR Technology

Beazley Security Launches With MXDR Offering

JUNE 27, 2024 | 1 MIN READ

SOURCE: ARTEMIS DIANA VIA ALAMY

Passkeys gained momentum in 2023.

In addition to the major three technology firms supporting passkeys — Apple, Google, and Microsoft — third-party password providers, such as 1Password and Bitwarden, implemented their own support for managing the credentials. Dozens, and likely hundreds, of major websites have followed suit, implementing the necessary support for passkey authentication.

Overall, more than 7 billion accounts could be using passkeys, according to the FIDO Alliance, whose technical specifications power the authentication standard. Left unsaid: The vast majority of users are not.

The whole point of passkeys is to make passwordless authentication as convenient and secure as passwords, says Andrew Shikiar, executive director of the FIDO Alliance.

"Passwords are a clear and present danger to everything we do online right now," he says. "To take on passwords, you need to be able to prove the same characteristics as passwords — ubiquity and convenience."

For those who want an easier and more secure way to sign into cloud services and websites, this Tech Tip is for you.

What Are Passkeys?

Passkeys are the answer to the question: "Why should we memorize passwords for websites when our devices have more secure ways of authentication?" Windows systems, Macs, iPhones, and Android devices all have ways of securely storing keys via an encrypted hardware enclave and authenticating the user through biometrics.

Apple, Google, and Microsoft worked with the FIDO Alliance to establish the passkey standard using certificates for authentication that are WebAuthn-compliant. Various ecosystems — such as Apple, Bitwarden, Google, 1Password, and Microsoft — manage passkeys in different ways, but they all support standardized passkeys.

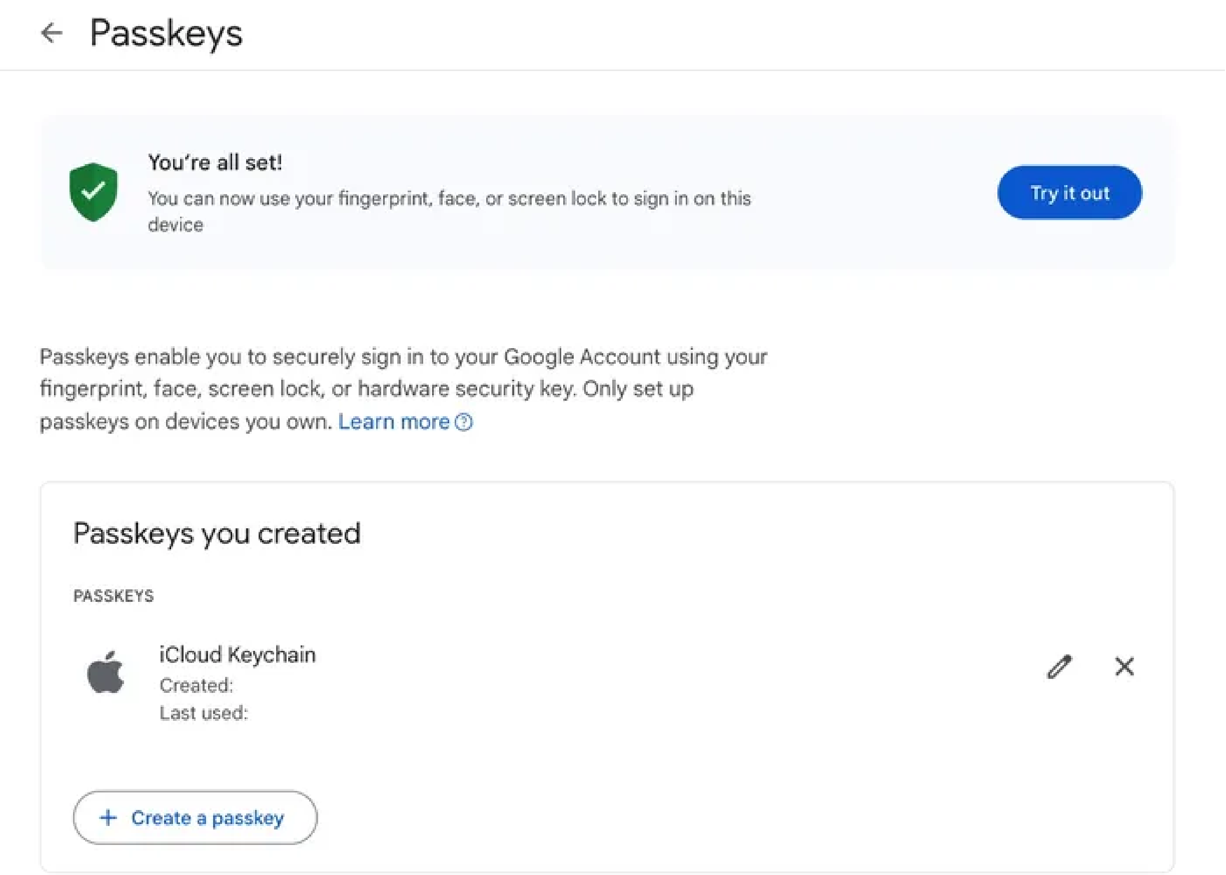
Google, which by default now asks users if they want to use passkeys, has not released data on the number of accounts that have opted into using the technology, but it does say that 60% of users believe passkeys are easier to use than traditional login methods.

"Similar to any new innovation, it's going to take time for people to get used to passkeys," says Arnar Birgisson, a software engineer for Google. "Passwords are all we've known for countless years."

A Passel of Passkeys

The first question that users should consider is whether they want to consolidate their keys under a single ecosystem or provider. For users who have exclusively bought into the Apple ecosystem, for example, using the passkey support in the iCloud Keychain feature of Macs, iPads, and iOS devices might be completely acceptable. Similarly, users of Google Chrome can use the password capabilities of the browser across different platforms to manage passkeys by signing into their Google accounts.

To avoid being locked into a specific ecosystem of hardware or browsers, however, users could instead turn to a third-party service. 1Password, Bitwarden, Dashlane, Enpass, and LastPass all support — or are working on support for — passkeys through their application and browser extensions, which will allow passkeys to be accessed across major device types and browsers. Using a single ecosystem can make passkeys simpler for the user, especially when it comes to the critical issue of key recovery.



← Passkeys

You're all set!

You can now use your fingerprint, face, or screen lock to sign in on this device

Passkeys enable you to securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. Only set up passkeys on devices you own. Learn more

Passkeys you created

PASSKEYS

iCloud Keychain
Created:
Last used:

Generating a passkey for Google on the Chrome browser using Apple'"s iCloud Keychain to store the passkeys. Source: Author

Creating a Passkey: Google Account Using Chrome

For personal Google accounts, or if you are the administrator of Google Workspace accounts, you can set up passkeys for your users. (The Google Workspace support is currently in beta.) Google supports setting up passkeys on Windows 10 and up, MacOS Ventura and later, or ChromeOS 109 and up, although users are recommended to update to the most current version of their operating systems.

For Google accounts, go to the company's passkey site and click the "Get passkeys" button. Google will ask you to sign into the account you want to associate with a passkey, create the passkey, and then have you test access to the system.

To use Chrome to store passkeys, you need to have Chrome Sync enabled:

1. Open the Chrome browser.
2. Click on the hamburger button (three stacked dots in the upper right) and select Passwords & Autofill -> Google Password Manager.
3. Enable "Use passkeys across your X devices," where X is your type of devices (Windows, Apple, etc.). You will likely have a choice to use your Google account to sync data or the operating system's native syncing mechanism (Microsoft OneDrive or Apple iCloud, for example).

Creating a Passkey: Microsoft 365 on Windows

Microsoft's passwordless technology is a little less integrated than Google's or Apple's passkey support. On Windows, logging into a site using passkeys through Windows Hello is seamless, with passkeys handled in the background. On non-Windows systems, users must download the Microsoft Authenticator app to a supported device (such as an Android phone or iPhone) to log into Microsoft services using a second factor.

To use Windows to store passkeys:

1. Download and install the Microsoft Authenticator app to your mobile device.
2. Log into your Microsoft account (such as Microsoft Live or Microsoft 365) and go to Accounts -> Security. Under "Additional security," turn on Passwordless account.
3. To manage passkeys on Windows, go to Settings -> Accounts -> Passkey settings. All passkeys saved will be listed here.

Creating a Passkey: PayPal on 1Password for Apple

Apple users can manage their passkeys through iCloud Keychain, which synchronizes across all Apple platforms. However, third-party apps are another option. For users of the 1Password password manager, for example, passkeys are now integrated into the information for each account and easily accessible from a browser extension.

To use 1Password to store passkeys and access PayPal, for example:

1. Download and install the 1Password application and the 1Password extension for your current browser(s).
2. Use your credentials to login to PayPal, saving the account to 1Password. Then log out. (If you already have the PayPal credentials in 1Password, you can skip this step.)
3. Go to PayPal, look for a link to "Create a passkey," and click the link. Or go to PayPal and open the 1Password extension, which should have a purple

notification stating "Passkey available." Click on the notification and then on "Use passkey."

4. You will have to log in again to have a passkey assigned to your account.

Recovering From a Lost Device

The problem with tying online-account access to a device is that if the device is lost, damaged, or stolen, the user has lost access to those accounts. This critical problem is why Apple, Google, and Microsoft collaborated on the passkey standard. By allowing passkeys to be synchronized through their cloud infrastructure, the companies can provide account recovery services — as can third-party providers, such as 1Password and others.

Still, a lost briefcase or backpack that has a person's entire cloud-access stack — a laptop, phone, and table, for example — could lead to a loss of access to their services. For that reason, the different ecosystems have different methods of recovering accounts and the keys associated with those accounts. Apple has iCloud Keychain escrow, Google allows users to default to two-step verification through backup codes or a hardware security key, and 1Password allows account recovery through its Emergency Kit process.

Users should also consider purchasing a hardware token. Some passkey service providers allow the backing up of keys — such as the iCloud Keychain — to a security device, such as a hardware token. In addition, hardware tokens that support device-bound passkeys can be a backup method of accessing an account.

Passkeys users should run through the mental exercise of recovering their critical cloud accounts in the case of a lost device to ensure that they understand the process and know all the information necessary for recovery.

About the Author(s)

Robert Lemos, Contributing Writer

Veteran technology journalist of more than 20 years. Former research engineer. Written for more than two dozen publications, including CNET News.com, Dark Reading, MIT's Technolo...

You May Also Like

More Insights

Events

Black Hat USA - Aug 3-8 - The Premier Technical Cybersecurity Conference - Learn More

Black Hat Europe - December 9-12 - Learn More

SecTor - Canada's IT Security Conference Oct 22-24 - Learn More

More Events