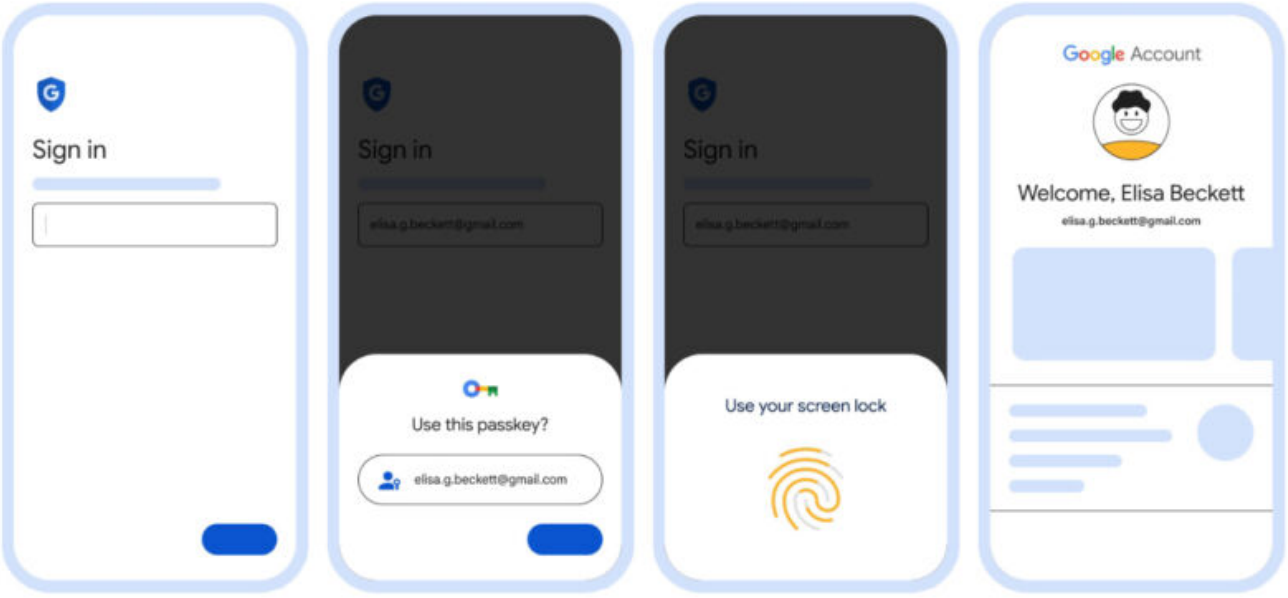
Passwordless Google accounts are here—you can now switch to passkey-only



Enlarge / Google says the login flow will go something like this, from left to right: type in your username, pick a passkey, scan a finger. Hopefully your device has biometrics.

reader comments

106 with

Google is taking a big step toward our supposedly passwordless future by enabling passkey-only Google accounts. In the blog post, titled “The beginning of the end of the password,” Google says: “We’ve begun rolling out support for passkeys across Google Accounts on all major platforms. They’ll be an additional option that people can use to sign in, alongside passwords, 2-Step Verification (2SV), etc.” Previously, you’ve been able to use a passkey with a Google account as part of two-factor authentication, but that was always *in addition to* a password. Now it’s possible to use a Google account with a passkey *instead of* a password.

A passkey, if you haven’t heard of the new authentication method, is a new way to log in to apps and websites and may someday replace a password. Password entry began as a simple text box for humans, and those text boxes slowly had automation and complication bolted onto them as the desire for higher security arrived. While you used to type a remembered word into a password field, today, the right way to use a password is to have a password manager paste a random string of characters into the password box. Since few of us physically type in our passwords, passkeys remove the password box.

Passkeys have your operating system directly swap public-private keypairs—the “WebAuthn” standard—with a website, and that’s how you get authenticated. Google’s demo of how this will work on a phone looks great—the usual box asks for your Google username, then instead of a password, it asks for a fingerprint, which unlocks the passkey system, and you’re logged in.

Google’s passwordless support is headed for consumer devices right now, while business Google Workspace accounts will “soon” have the option to enable passkeys for end users.

Passkeys still aren’t ready for prime time

Even with Google going all-in on passkeys, that doesn’t mean they’re ready for widespread adoption. First, some platforms (Windows/Linux/Chrome OS) are not as far along as others (macOS/iOS/Android). The official passkeys.dev site has a helpful page that tracks platform-by-platform readiness, and there’s still a long way to go. It would be terrible to be unable to access your passkey Google account on Chrome OS, which presumably would lock you out until you switch back to a password.

Advertisement
The second issue does not seem like it’s going to be fixed any time soon, and that’s that passkeys sync via your *operating system ecosystem*, not via a browser, which represents a major regression over the way passwords work. Today if I add a password to Chrome on Windows, that password will instantly be available everywhere I have Chrome installed, like an Android phone, a MacBook, an iPhone, a Chromebook, etc., but passkeys don’t work like that.

To quote the FIDO Alliance page, passkeys are “synced to all the user’s other devices running **the same OS platform**” [emphasis ours]. That means if I add a passkey to Chrome on Windows, that passkey goes into the OS vendor’s passkey store—Microsoft’s—and will only sync with other Microsoft operating systems. If you exclusively use Apple devices, everything will sync, and you won’t notice a difference. The rest of us will need to go through a QR-code and Bluetooth-driven transfer process to get our credentials working across Windows and Android or Android and Linux, or any other cross-OS-vendor combination. The Big Tech companies in charge of passkeys don’t seem interested in making them as seamless and convenient as passwords, and that will be a major hurdle for their ubiquity.

1Password confirms this whole syncing mess, “Currently, passkeys on other platforms require you to use a device from the same ecosystem to authenticate. Syncing with other operating systems or sharing passkeys requires tedious work-arounds, like QR codes, resulting in a more complicated and less secure experience.” It’s unclear whether apps like 1Password have been invited to the Big Tech passkey party. 1Password says it has joined the FIDO Alliance, but 1Password’s passkey page also has a video saying that passkeys weren’t open enough. The video says, “Today’s solutions don’t deliver on that promise of openness and interoperability. If you create a password on your iPhone or Android device today,

it’s pretty much trapped. It’s not easy to share, move it to another platform or sync with your preferred password manager. We can do better. And that’s why we’re excited to show you what the future could look like, if passwordless technology were more open.”

1Password’s passkey page contains a lot of “could” and “should” language, but the company is working on some kind of solution that will be out “this summer.” Even if the company manages to crack the problem of passkey syncing for its own app, having such a major cross-platform regression in the default setup—which is what most people will use—will seriously limit the appeal of passkeys.

Listing image by Google

https://arstechnica.com/?p=1936276