

Setting Up Your Passkey

A more secure way to sign in: no codes, no approvals

What is a passkey?

A passkey replaces your password and one-time codes with a single biometric check: your fingerprint, face, or device PIN. When you sign in, your device confirms it's really you and automatically proves it to Microsoft. No codes to copy, no approval requests to tap.

Passkeys are also phishing-resistant. Because the passkey is tied to the exact website you registered it on, a fake login page can never steal it; it simply won't work anywhere except the real Microsoft sign-in.

Where your passkey will be stored

Your passkeys will be stored in the Microsoft Authenticator app on your phone and in Windows Hello on your work laptop. You don't need to remember or manage them - your device handles that automatically.

Device	Stored In	Unlock Method
iPhone / Android phone	Microsoft Authenticator app	Face ID, Touch ID, or fingerprint
Windows laptop (work)	Windows Hello	Fingerprint / Face / PIN



Note

You will be asked to set up two passkeys: one in the Microsoft Authenticator app on your phone, and one on your work laptop via Windows Hello. This means you always have a backup if one device is unavailable.

Before you start

Make sure you have:

- Your current Microsoft account password (you'll need it to log in once)
- Your existing MFA method (Authenticator app, SMS, or email) ready (used only this one time)
- Your phone charged and with you
- Access to mysignins.microsoft.com (open in a browser on your computer)

Step 1: Set up a passkey in Microsoft Authenticator

The Microsoft Authenticator app stores your passkey securely on your phone. These steps are the same whether you use iPhone or Android.

1. Make sure you have the Microsoft Authenticator app installed on your phone. If not, download it from the App Store (iPhone) or Google Play (Android).
2. Open a browser on your computer and go to mysignins.microsoft.com.
3. Sign in with your work email and password, then approve using your current MFA method.
4. Tap Security info, then tap Add sign-in method.
5. Choose Passkey.
6. When asked where to save it, choose Microsoft Authenticator.
7. A QR code will appear on screen. Open the Authenticator app on your phone, tap the + icon or the menu, and choose Scan QR code.
8. Scan the QR code shown on your computer screen.
9. Your phone will prompt you to confirm with your fingerprint, Face ID, or PIN.
10. Once confirmed, you should see: Passkey added successfully.



Tip

If you already use Microsoft Authenticator for MFA approvals, the passkey is added alongside your existing account. You don't need to remove or re-add the account.

Step 2: Set up a passkey on your work computer

Your work laptop already uses Windows Hello (the fingerprint reader or camera you use to log in to Windows). This automatically works as a passkey — you just need to register it with Microsoft.

1. On your work computer, open a browser and go to <https://mysignins.microsoft.com/security-info>
2. Sign in using your password or the phone passkey you just created.
3. Go to Security info and tap Add sign-in method.
4. Choose Passkey.
5. Windows will prompt you to use Windows Hello. Confirm with your fingerprint, face, or PIN.
6. You should see: Passkey added successfully.



Tip

If Windows Hello isn't set up on your laptop yet, go to Settings > Accounts > Sign-in options and follow the prompts to add a fingerprint or face before continuing.

Step 3: Test your passkey

Once both passkeys are registered, try signing in with a passkey:

1. Open a private/incognito browser window.
2. Go to portal.office.com and enter your work email.
3. When prompted, choose Sign in with a passkey (or use your fingerprint/face when asked).
4. Your device will ask you to confirm with biometrics or PIN and a one time code is not required.
5. You should be signed in. Done!

Troubleshooting

Problem	What to try
I don't see a Passkey option	Make sure you're signed in to mysignins.microsoft.com with your work account. Try refreshing the page.
The QR code isn't working	Make sure you're scanning the code from the Authenticator app (tap + or the menu, then Scan QR code). The code expires after a short time - refresh the page to get a new one if needed.
Face/fingerprint not recognised on my phone	Make sure biometrics are set up on your phone first (Settings > Face ID & Passcode on iPhone; Settings > Biometrics on Android), then try again.
Passkey registration fails or times out	Try Edge or Chrome on your computer. Disable browser extensions and try again. Make sure your Authenticator app is up to date.
I lost or replaced my phone	Contact the IT helpdesk. They can issue a temporary access pass so you can register a new passkey on your new phone.
I still want to use the Authenticator app push approvals	You can keep using push approvals during this transition period. However, passkeys provide stronger protection against phishing and we encourage you to complete setup as soon as possible.

Need help?

If you run into any issues, contact the IT helpdesk. You don't need to figure this out alone. Passkey setup takes most users under five minutes and we're here if you get stuck.