

PREPARING FOR MICROSOFT'S PASSKEY TRANSITION

Microsoft's decision to retire its own SMS and voice-based authentication services from early 2027 marks a significant shift towards phishing-resistant authentication.



FAQ

1. What is changing in Microsoft authentication?

Microsoft is making passkeys the default authentication experience and retiring Microsoft-provided SMS and voice authentication services. From 1 September 2026, users enabled for SMS or voice authentication will be prompted to register passkeys. From 1 February 2027, Microsoft-provided SMS and voice authentication will be retired.

2. What is a passkey?

A passkey is a phishing-resistant authentication method that uses cryptographic credentials stored securely on a trusted device. Users authenticate with a fingerprint, face recognition, PIN, or security key rather than entering a password and one-time code.

3. Why is Microsoft moving away from SMS and voice authentication?

SMS and voice calls are vulnerable to phishing, interception, and SIM-swap attacks. Passkeys provide significantly stronger protection against modern identity threats.

4. Will passwords disappear completely?

Not immediately. While passkeys are designed to support passwordless authentication, organisations may continue to use passwords during their transition. However, the long-term industry direction is towards passwordless authentication.

5. What happens if we do nothing before February 2027?

Users relying solely on SMS or voice authentication will be required to register a passkey before they can continue signing in. Microsoft states this will be a mandatory, blocking experience.

littlefish
GROUP



Want to know more?

We can take you through security best practice and identify where risk may be creeping in... **Get in touch today.**



Call: 0330 390 2002



email: info@littlefish.co.uk



HQ: Price House, 37 Stoney St, Nottingham NG1 1LS

[littlefish.co.uk](https://www.littlefish.co.uk)

6. Do users need to buy security keys?

Usually not. Most users can create passkeys using Microsoft Authenticator, Windows Hello for Business, or supported mobile devices. Hardware security keys remain an option for specific scenarios.

7. Can passkeys work on company and personal devices?

Yes. Passkeys can be used on managed corporate devices and supported personal devices, depending on organisational policy and security requirements. Cross-device authentication is also supported.

8. Can users use synced passkeys from Google Password Manager or iCloud Keychain?

Potentially – depending on organisational policy and the passkey providers enabled in your environment. Synced passkeys can improve user convenience across supported devices, but IT teams should define whether they are approved for corporate access, especially where personal devices, consumer cloud accounts, recovery, auditability, and device trust are involved.

9. What happens if someone loses their mobile phone?

Organisations should implement recovery processes such as Temporary Access Pass (TAP), secondary authentication methods, and identity verification procedures.

10. Will this affect self-service password reset (SSPR)?

Yes. The retirement of Microsoft-provided SMS and voice services applies across Entra services, including self-service password reset. Organisations should review their recovery and account recovery processes.

11. How will users register a passkey?

Microsoft will begin prompting eligible users to register passkeys during sign-in. Users can typically create a passkey through Microsoft Authenticator or another supported passkey provider.

12. How do I know if my organisation is affected?

If your organisation uses SMS codes or voice calls for MFA or password reset, you should assess which users and groups are still dependent on these methods. Microsoft recommends identifying these users as part of your migration planning.

Want to know more?

We can take you through security best practice and identify where risk may be creeping in... **Get in touch today.**



Call: 0330 390 2002



email: info@littlefish.co.uk



HQ: Price House, 37 Stoney St, Nottingham NG1 1LS

[littlefish.co.uk](https://www.littlefish.co.uk)

13. Are passkeys more secure than Microsoft Authenticator notifications?

Passkeys are considered phishing-resistant because there is no code or approval that can be intercepted or entered into a fraudulent website. They provide a higher level of protection than traditional MFA methods.

14. What should IT teams be doing now?

- Identify users still using SMS or voice MFA.
- Review Entra Authentication Methods policies.
- Pilot passkeys and Windows Hello for Business.
- Update onboarding and account recovery processes.
- Launch user awareness and adoption campaigns.

15. Will SMS authentication disappear completely?

Not necessarily. Organisations with a business requirement for SMS or voice authentication will be able to use customer-managed telecom providers through the Microsoft Security Store after Microsoft's native service is retired.

16. What are the business benefits of moving to passkeys?

- Reduced risk of phishing and account compromise.
- Faster and simpler user sign-in experience.
- Lower password reset and service desk volumes.
- Alignment with Zero Trust and cybersecurity best practice.
- Better readiness for future Microsoft security capabilities.

17. What is the single most important message for organisations?

Start planning now. Organisations that identify SMS and voice dependencies early will have a smoother migration, lower risk, and better user adoption before the February 2027 deadline.

IF YOU'D LIKE TO UNDERSTAND WHAT MICROSOFT'S MOVE AWAY FROM SMS AND VOICE-BASED MFA COULD MEAN FOR YOUR ORGANISATION, OR NEED HELP PLANNING AND IMPLEMENTING A PASSKEY STRATEGY, PLEASE FEEL FREE TO GET IN TOUCH.



Want to know more?

We can take you through security best practice and identify where risk may be creeping in... **Get in touch today.**



Call: 0330 390 2002



email: info@littlefish.co.uk



HQ: Price House, 37 Stoney St, Nottingham NG1 1LS

[littlefish.co.uk](https://www.littlefish.co.uk)