Passkeys and MFA: which sign-in methods are still good enough?

Require phishing-resistant sign-in (security keys, passkeys, Windows Hello for Business or certificates) for every admin first, and secure account recovery before you enforce it. Then move each remaining group to the strongest method its devices support, and give SMS, voice and email codes an end date.

Reviewed	Next review	Version	Written for	Latest version
5 Nov 2026	**5 Dec 2026**	**1.1**	**IT and security teams, especially on Microsoft 365 and Microsoft Entra ID**	**sheets.einblick.dev/passkeys-mfa/**

If you only do five things

1. **Move admins to phishing-resistant sign-in first.**
   Give every privileged account a security key or device-bound passkey and require it at each sign-in. CISA suggests starting with administrators and help desk staff[1].
2. **Secure account recovery before you enforce.**
   Once sign-in is phishing-resistant, attackers target onboarding and recovery, which often still use SMS or email codes[2]. Decide who may reset a method and how they verify identity, and notify the user whenever a method is added or an account is recovered, as NIST requires[3].
3. **Move everyone else off phishable methods.**
   Adversary-in-the-middle phishing relays passwords and MFA codes to the real sign-in page and captures the session cookie. It made up 44.6% of the phishing techniques Microsoft identified from July 2025 to June 2026[2]. Retire SMS, voice and email codes first, then push and app codes.
4. **Block legacy authentication.**
   Legacy protocols don't support MFA, so a stolen password is enough to sign in. Microsoft reports that more than 99% of password spray attacks use legacy authentication[4]. Find the clients that still use it, then block it with Conditional Access, or with security defaults if your licenses don't include Conditional Access[4].
5. **Protect sessions after sign-in.**
   A stolen session token works without the passkey. Require compliant devices, bind tokens to the device where supported and enforce phishing-resistant reauthentication for risky sign-ins and sensitive actions[5].

Move a group to phishing-resistant sign-in

1. **Check the group's devices.**
   List the operating systems each person signs in from. Microsoft's minimum versions are Windows 10 22H2, macOS 13, iOS 17 and Android 14; older devices may need a security key[6].
2. **Create the Conditional Access policy in report-only mode.**
   Do this before registration starts, so the sign-in logs show who would be blocked and on which device[6].
3. **Plan how each person registers.**
   Existing users register with the MFA they already have. New hires and users without MFA get a Temporary Access Pass after an identity check and register with it[6].
4. **Register a portable credential, then a local one.**
   A passkey or security key works across devices; Windows Hello for Business or Platform Credential for macOS speeds up daily sign-in on each computer. Microsoft recommends at least two methods per user, so a lost phone doesn't lock anyone out[6].
5. **Enforce in waves, then remove the old methods.**
   Add users to the policy in waves and slow down when help desk tickets rise[6]. Then remove SMS, voice and one-time code methods from their accounts so attackers can't fall back on them[2].

Which methods to keep

A method is phishing-resistant when it is bound to the site's domain or to the TLS channel[3]. NIST doesn't count any method where the user types a code[3].

Phishing-resistant

- **Security keys (FIDO2).** They suit admins, shared PCs and computers too old for passkeys.
- **Device-bound passkeys.** The private key never leaves one device, such as a phone running Microsoft Authenticator[7]. They suit admins without a separate security key.
- **Synced passkeys.** NIST allows them at AAL2 but not AAL3. Where you can, keep them in company-managed accounts on managed devices that block sharing, as NIST requires for federal agencies[3].
- **Windows Hello for Business.** It is bound to one computer and suits daily sign-in there.
- **Certificate-based authentication.** CISA counts it as phishing-resistant[1]. Keep it where you already issue smart cards.

Acceptable for now

- **Push approval with number matching.** CISA rates it resistant to push bombing but still vulnerable to phishing[1].
- **One-time codes from an app or hardware token.** SIM swapping doesn't affect them, but a phishing page can relay them[1].
- **Phone sign-in in Microsoft Authenticator.** Entra ID counts it as passwordless MFA, but the built-in Phishing-resistant MFA strength excludes it[8].

Retire

- **SMS and voice codes.** NIST classes phone-network codes as restricted and requires a migration plan in case they stop being acceptable[3].
- **Email codes.** NIST doesn't allow email for out-of-band authentication[3]. CISA's SCuBA baseline for Entra ID requires disabling email, SMS and voice codes[9].
- **Push approval without number matching.** A single tap approves the sign-in, which push bombing relies on[1].

If you run Microsoft Entra ID

- **Require an authentication strength.** The built-in Phishing-resistant MFA strength needs Entra ID P1 and accepts passkeys (FIDO2), Windows Hello for Business and multifactor certificate-based authentication[8].
- **Use passkey profiles.** Allow synced passkeys for most users and require attested device-bound passkeys, such as security keys or Microsoft Authenticator, for admins. Passkeys work in every Entra ID edition, including Free[7].
- **Keep Temporary Access Passes short-lived.** Make them one-time use, keep the lifetime near the 1-hour default and limit their sessions with sign-in frequency[10].
- **Check VPNs that use the NPS extension.** It doesn't support number matching, so users without a registered one-time code method still get a plain Approve or Deny prompt[11].
- **Pilot token protection.** It binds sign-in tokens to the device for Exchange, SharePoint and Teams in native apps[12].

Accounts that need their own rules

- **Admin accounts.** Microsoft requires MFA for its admin portals and Azure management, and users who already sign in with MFA see no change[13]. Require phishing-resistant methods in your own policy.
- **Service accounts.** Move scripts that sign in as users to managed identities or service principals, which mandatory MFA doesn't cover[13].
- **Emergency access accounts.** Keep at least two, with security keys or certificates that differ from your normal admin methods. Exclude them from blocking policies, alert on every sign-in and test them at least every 90 days[14].
- **Shared devices and mailboxes.** Use security keys on shared PCs, since Windows Hello for Business isn't meant for kiosks with a shared account[6]. Block sign-in for shared mailbox accounts.
- **Guests.** They can't register passkeys in your tenant[7], so require MFA and decide in cross-tenant access settings which home tenants' MFA you trust.

What changed in 2026

- **Synced passkeys are generally available in Entra ID.** Since March 2026, passkey profiles set the allowed passkey types, attestation and authenticator models per group[15].
- **Account recovery with Verified ID is generally available in Entra ID.** Since May 2026[16], users who have lost every method can recover their account through a government ID check[17].
- **The UK NCSC now recommends passkeys wherever a service supports them.** It announced the change in April 2026 and counts FIDO2 sign-in with user verification as MFA[18].
- **Azure requires MFA for changes made from scripts and tools.** Enforcement for Azure CLI, PowerShell, SDKs and REST APIs began rolling out in October 2025, and tenants could postpone it until 1 July 2026[13].

What you can skip

- **Periodic password changes and composition rules.** NIST SP 800-63B-4 prohibits both; force a change only on evidence of compromise[3].
- **Short session timeouts for everyone.** The NCSC warns that frequent reauthentication desensitizes users to entering their credentials[19].
- **Security keys for every user.** Microsoft recommends synced passkeys for users without admin rights[6].
- **A new PKI for certificate-based sign-in.** Microsoft calls it more complicated to configure than passkeys[6].

Mistakes that cost the most

- **Resetting MFA for unverified callers.** Scattered Spider talked help desks into resetting passwords and moving MFA to attacker devices[20].
- **Letting anyone with the password register MFA.** Attackers add their own method to keep access[2], so require a managed device to register[9].
- **Excluding accounts from MFA and forgetting them.** The NCSC calls them a backdoor[19]. Give each exclusion an owner and an end date.
- **Leaving device code flow open.** Attackers use it in phishing, and Microsoft recommends blocking it wherever possible[5].
- **Stopping at a password reset.** Also revoke sessions and remove the MFA methods, app secrets and consent grants the attacker added[2].

Version history

5 Nov 2026, version 1.1	Reviewed for company readers: synced passkeys should live in company-managed accounts on managed devices that block sharing where possible, as NIST requires for federal agencies, rather than in staff's personal accounts.

Sources

1. Implementing Phishing-Resistant MFA. CISA, Oct 2022. cisa.gov
2. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
3. SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management. NIST, 31 Jul 2025. pages.nist.gov
4. Block legacy authentication with Conditional Access. Microsoft Learn, 24 Mar 2026. learn.microsoft.com
5. Protecting Tokens in Microsoft Entra ID. Microsoft Learn, 24 Apr 2025. learn.microsoft.com
6. Plan a phishing-resistant passwordless authentication deployment in Microsoft Entra ID. Microsoft Learn, 26 Mar 2026. learn.microsoft.com
7. How to enable passkeys (FIDO2) in Microsoft Entra ID. Microsoft Learn, 8 Mar 2026. learn.microsoft.com
8. Overview of Conditional Access Authentication Strengths. Microsoft Learn, 4 Mar 2025. learn.microsoft.com
9. CISA M365 Secure Configuration Baseline for Microsoft Entra ID. CISA (ScubaGear), ScubaGear v2.0.0, Oct 2026. github.com
10. Configure a Temporary Access Pass in Microsoft Entra ID to register passwordless authentication methods. Microsoft Learn, 4 Mar 2026. learn.microsoft.com
11. How number matching works in MFA push notifications for Authenticator. Microsoft Learn, 6 Nov 2025. learn.microsoft.com
12. How Token Protection Enhances Conditional Access Policies. Microsoft Learn, 14 Aug 2026. learn.microsoft.com
13. Plan for mandatory Microsoft Entra multifactor authentication (MFA). Microsoft Learn, 3 Apr 2026. learn.microsoft.com
14. Manage emergency access admin accounts. Microsoft Learn, 4 Jun 2026. learn.microsoft.com
15. Microsoft Entra releases and announcements. Microsoft Learn, 26 Jun 2026. learn.microsoft.com
16. What's new for Microsoft Entra Verified ID. Microsoft Learn, 8 Oct 2026. learn.microsoft.com
17. Verified ID identity verification overview in Microsoft Entra ID. Microsoft Learn, 30 Apr 2026. learn.microsoft.com
18. Passkeys are more secure than traditional ways to log in. NCSC (UK), 23 Apr 2026. ncsc.gov.uk
19. Avoiding MFA anti-patterns. NCSC (UK), version 2.0, 26 Sep 2024. ncsc.gov.uk
20. Scattered Spider (AA23-320A). CISA, FBI and partners, updated 29 Jul 2025. cisa.gov