■ Microsoft

Microsoft Passwordless Authentication

Passwords are not enough

Password are becoming a relic of the past. The use of passwords leaves us increasingly more vulnerable as we become more predictable in generating them. Trying to combat this with requirements for stronger complexity and frequent updates makes it harder to be productive, drives up already-high costs in password maintenance and support—and still isn't enough to keep up with current cybersecurity threats.

81% of hacking-related breaches used either stolen or weak passwords[1]

Eliminate password theft

People want a highly secure, convenient alternative. Passwordless authentication is a form of multi-factor authentication (MFA) that replaces passwords with two or more verification factors secured and encrypted on a user's device, such as a fingerprint, facial recognition, a device pin, or a cryptographic key. The credentials never leave the device, eliminating the risk of phishing. These alternatives are based on new industry standards developed by members of the Fast ID Online (FIDO) Alliance.

99.9%+ less likely to be compromised when you use MFA[2]

Can't a biometric access system get hacked or spoofed?

Your biometric signature is secured locally on the device, shared with no one but you, and is only ever used to unlock the device or key. It is never used to authenticate over the network. A common biometric attack method involves trying to spoof a person's body part in an attempt to trick the system, but any spoofing would first require that the attacker gains custody of the device.

Password replacements

As biometrics for mobile phones and computers become universal, password replacement options have increased in the modern workplace.

Windows Hello for Business

Windows Hello for Business replaces passwords with strong multi-factor authentication on Windows 10 platforms. Use either a biometric or PIN to authenticate to enterprise apps, content, and resources without a password being stored.

Microsoft Authenticator app

Microsoft Authenticator is a free mobile app on iOS and Android that can replace or augment passwords with push notification approvals, one-time passcodes, and additional verification of a biometric gesture on the device or the device PIN.

FIDO2-compliant security keys

FIDO2-compliant security keys are cryptographic credentials in a variety of form factors, including USB keys or NFC-enabled smartcards. They can be protected with a second factor such as a fingerprint (integrated into the security key) or a device PIN to be entered at sign in.
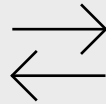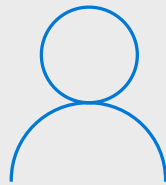
How strong authentication works

Each technology uses the same established cryptographic authentication pattern, with credentials based on the certificate or asymmetrical key pair.
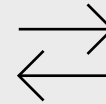
1. Send challenge
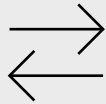
2. Provide user verification
User Auth Gestures

3. Sign and return challenge
FIDO2 Authenticator

4. Verify signed challenge
Relying Party Server

Adoption

Moving to passwordless authentication offers improved security and a better user experience, but requires a growth mindset internally. Start with a low risk group and explain the benefits of eliminating passwords. Deploy MFA with a passwordless authentication option until people are comfortable with it and then start replacing passwords and dependencies on passwords in the background.

"Don't let perfection stand in the way of progress. Every step toward passwordless is a step toward improving your security posture."

Bret Arsenault, CISO for Microsoft

Benefits of eliminating passwords

Sign in to applications and services faster. There are no passwords to create, store, or remember.

Gain a higher degree of trust and security for apps, devices, and service providers.

Dramatically reduce IT support team costs from password resets.

Learn more at aka.ms/gopasswordless