Microsoft Security

Passwordless protection

Reduce your risk exposure with passwordless authentication

Contents

Introduction

IT around the world is entering a new era—one in which passwords are a thing of the past.

Today, IT security is moving toward passwordless authentication using advanced technologies like biometric verification and public/private key cryptography. Open standards like W3C WebAuthn and Fast IDentity Online 2 (FIDO2) CTAP2 are enabling passwordless authentication across platforms. These standards are intended to replace passwords with authenticator devices that are easy to use and may take advantage of investments you've already made—such as laptops, smartphones, fingerprint scanners, and cameras with facial recognition.

Password replacement options can help organizations offer convenience and ease of use without high security risks. With passwordless authentication, you can have an authentication ecosystem that meets the organizational needs of high security and privacy, usability, and interoperability among several authentication devices.

In the future, we should rarely have to deal with passwords in our day-to-day lives—especially at work. For enterprise security and IT departments, implementing intuitive sign-in user experiences will reduce both helpdesk costs and employee frustrations related to frequent password reset requirements.

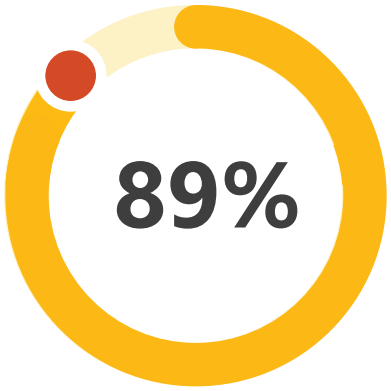
Passwords are the weakest link for security

The cost of using passwords and the associated security risk now outweigh the benefits. Even the strongest passwords are easily phishable and vulnerable to attacks, and user resistance to password requirements is high. The motives to eliminate password authentication are endlessly compelling and all too familiar to enterprise IT organizations today.

For many IT departments, password support and maintenance are often the largest cost. It's common practice to attempt to minimize password theft by encouraging the use of strong, complex passwords and requiring frequent password changes. However, these tactics often result in poor user behavior (easy-to-guess password changes) and can drive up IT helpdesk costs related to frequent password resets. Most importantly, this approach isn't enough to impede current cybersecurity threats, and it doesn't deliver on organizational information security requirements. Focusing on multifactor authentication and great threat detection, rather than password rules, can offer significant security advantages.

> " Your password, in the case of breach, just doesn't matter—unless it's longer than 12 characters and has never been used before."

Alex Weinert
Director of Identity Security
Microsoft
(Your Pa$$word doesn't matter)



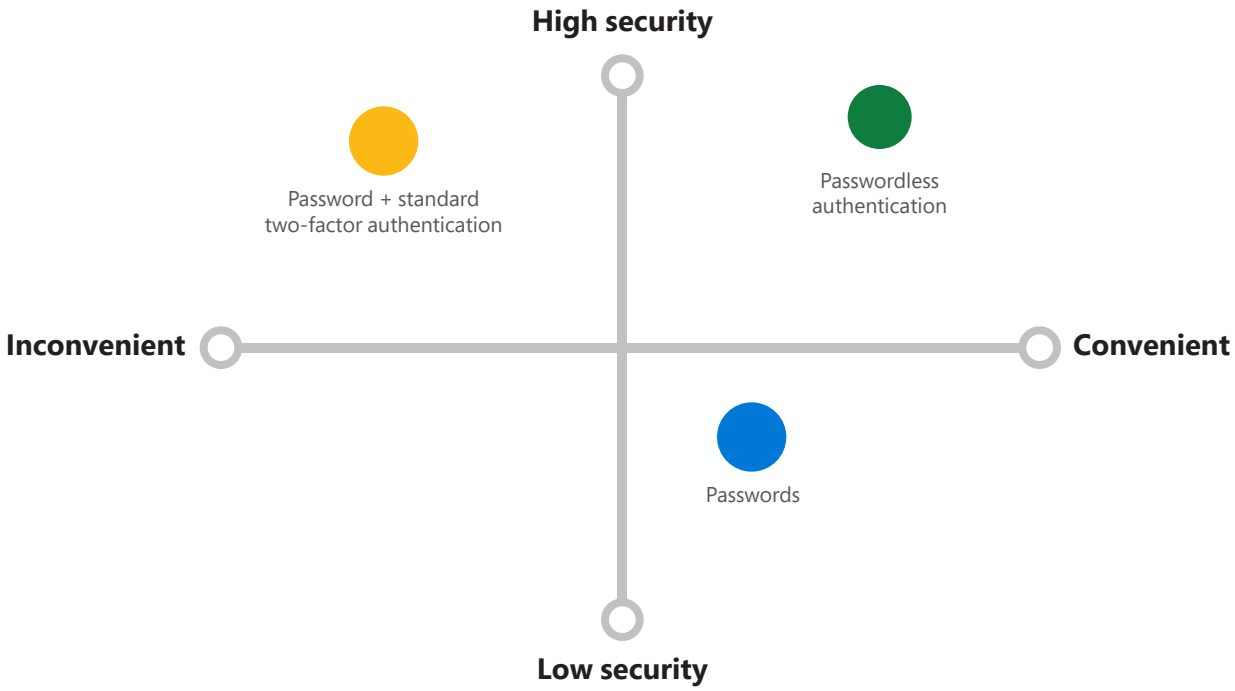
"89% of web application breaches involved some sort of credential abuse (either use of stolen credentials or brute force)."

(Verizon 2021 Data Breach Investigation Report)

Why passwordless authentication?

Passwords are supposed to be both keys used to access accounts and security barriers used to protect those accounts from attackers. To distinguish between an account owner and a potential hacker, organizations must now move beyond using just passwords for account security and protection. At the core of passwordless authentication is multifactor authentication (MFA). With passwordless MFA, you get a familiar, simple to use authentication experience with top industry security that works across a broad set of devices and services.

MFA can reduce the risk of compromise in organizations by 99.9 percent. With remote working becoming a new normal and new regulations to adhere to, IT teams need a variety of MFA options to meet business and user needs. By going beyond passwords while adding assurance, you can make access to your resources more secure. It's imperative for security teams to deliver a seamless user experience while balancing security postures.



Verify first, then trust

To increase account security and provide added protection, many organizations are adopting a Zero Trust approach—a security model which assumes breach and verifies every request for access. Knowing who is requesting access is essential, and that identity must be validated explicitly, not inferred from the environment. Ensure you are secure at the point of access by bringing users into a common identity system with strong passwordless authentication and then using threat intelligence to validate.

Drivers for passwordless authentication

Organizations might adopt passwordless authentication for a variety of reasons, including the following:

- Stronger security to protect against attacks
- Reduced IT support costs
- Support for remote working
- Adoption of a Zero Trust approach to verify each access request
- Productivity and accessibility needs for different workers or partners

Learn more about how to embrace Zero Trust security.

> "Hackers log in, they don't break in, proving your identity is the thing you really have to spend the most amount of time on. It turns out, changing it to 2FA (two-factor authentication) everywhere was a bad way to go, and eliminating passwords is an awesome way to go."

Bret Arsenault
CVP & CISO
Microsoft
(Business Insider)

Ten reasons to love passwordless authentication

1. FIDO2-based[1] credentials developed and adopted by the industry
2. Compliance with NIST[2] Authenticator Assurance Levels 2 and 3 (AAL2 and AAL3)
3. Biometric authentication stored locally to uniquely and securely identify users
4. Faster sign-ins with Windows Hello built into your PC[3]
5. Portable security keys in a variety of form factors that work across platforms
6. Helpdesk savings from password reset requests
7. Convenient sign-ins with Microsoft Authenticator app on your smartphone
8. Phishing-resistant credentials that reduce risk of compromise by over 99.9 percent
9. Easy setup and recovery of passwordless credentials with Temporary Access Pass
10. No passwords needed for end users to be productive and secure

Learn more: aka.ms/passwordless10

[1] Fast IDentity Online 2 (FIDO2) is an open authentication standard based on public key cryptography.
[2] The National Institute of Standards and Technology (NIST) promotes and maintains measurement standards and guidance to help organizations assess risk.
[3] Three times faster sign in based on average time comparison between typing a password respective to detecting a face or fingerprint to authentication success.

Adopting a passwordless strategy

The primary goal of passwordless authentication is to eradicate passwords—and to drain their value for attackers. Moving forward with this approach requires technologies that can support it, as well as time for organizations and their employees to adopt these technologies. Adoption also involves a new mindset. Organizations must first understand how the approach works with their operations flow, and then make the necessary technical and cultural shifts to operate in this new passwordless world.

Before you roll out a passwordless authentication strategy, move your identities to the cloud. Azure Active Directory user behavior analytics and security intelligence can help protect identities, uncover breach patterns, and recover if a breach occurs.

Microsoft has created a passwordless deployment wizard to help you with passwordless authentication strategies. The wizard will ask you to choose personas specific to your organization—and devices that specific roles use—and guide you to the passwordless options available for each case.

Positioning passwordless authentication

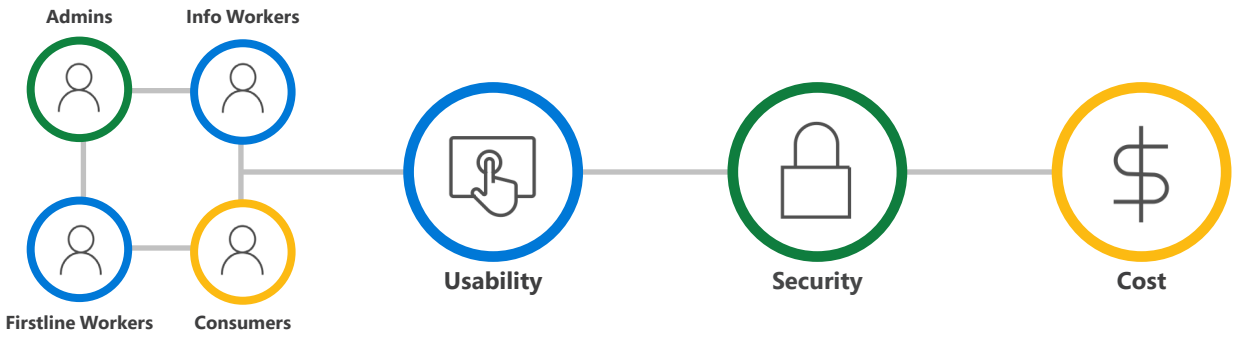
To help make passwordless authentication a success in your organization, consider the following strategies.

Segment your user communities as a journey.

Implementing passwordless authentication doesn't have to be an all-or-nothing approach. You can configure different authentication methods and policies for each segment based on risk. This early stage is about implementing a new sign-in method and getting people acquainted with it. For many, this starts with high-risk communities, such as executives or senior leadership, and those with privileged access, like IT administrators. For others, including mobile or remote workers, this might be a need for high productivity.

Choose the right technologies based on use case.

Determine which passwordless methods will work best for each group, along with your level of flexibility. Allowing more than one type of factor gives people options and helps meet accessibility needs.



Pilot passwordless starting with one or two groups.

Identify a few groups and introduce passwordless to them as an alternative to traditional sign-in methods. Starting small may help ease users into the idea of never typing, changing, or even knowing a password going forward. Plus, these initial users can help promote passwordless as you roll it out to more people.

Measure ROI and make it known.

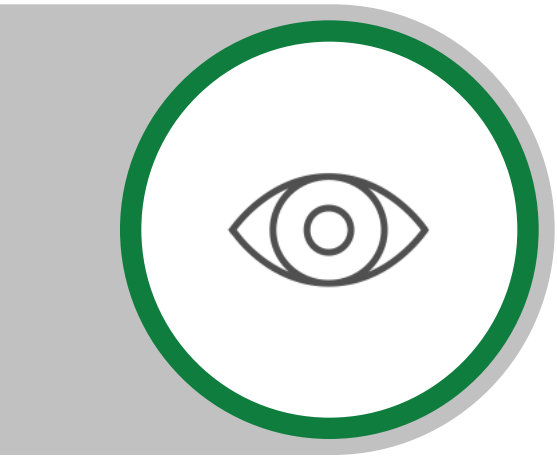
Let leaders in your organization know how passwordless authentication can deliver a high return on their investment. Note that these methods are up to 99.9 percent more secure with MFA and allow three-times faster sign-in, enabling stronger security, greater productivity, and reduced hard and soft costs.

It's about progress, not perfection.

"Everyone has brownfield apps that can't support modern authentication such as biometrics, and so I think what a lot of people should and need to do is take a risk-based approach: First get MFA enforced for high-risk/ value groups like admins, HR, legal, and so on, and then move to all users."

Bret Arsenault
CVP & CISO
Microsoft
(ZDNet)

Choosing the right solutions



Use case 1

Mark is an IT administrator. During the day, he frequently leaves his desk to respond to ticket requests. Because Mark handles sensitive employee information, his workstation must remain secure. Having to spend time remembering extensive passwords—along with required password changes each month—he longs for a solution that provides a fast two-factor authentication to confirm his identity while ensuring secure reliability.

With Windows Hello for Business, Mark uses his face as identification with a portable FIDO2 hardware device. Not only does this authenticate access to his Windows 10 device, but it also authenticates other enterprise applications, giving quick access to resources without the use of a stored password.

Use case 2

Debra is a registered nurse in a regional hospital. Her shifts entail multiple checks on patients, medication distribution, and consistent updates for doctors using secure workstations. Debra needs the flexibility to sign in to multiple computers quickly and efficiently while upholding patient confidentiality. The ability to maintain national standards to protect sensitive patient health information is a constant priority.

Incorporating biometric sensors at each computer, Debra can quickly authenticate her identity using a fingerprint—so she doesn't have to continuously type in a password. Going passwordless speeds up her engagement with patients while maintaining the hospital's security principles.

Use case 3

Dan works from home, which requires him to sign in to his work account. His password has extended characters, and he's required to update it monthly. He has to change—and remember—a new password so frequently that he uses separate programs to retain them. Frustrated with having to store passwords, Dan expressed interest in a more straightforward solution to authenticate his identity while maintaining his job's high security standards.

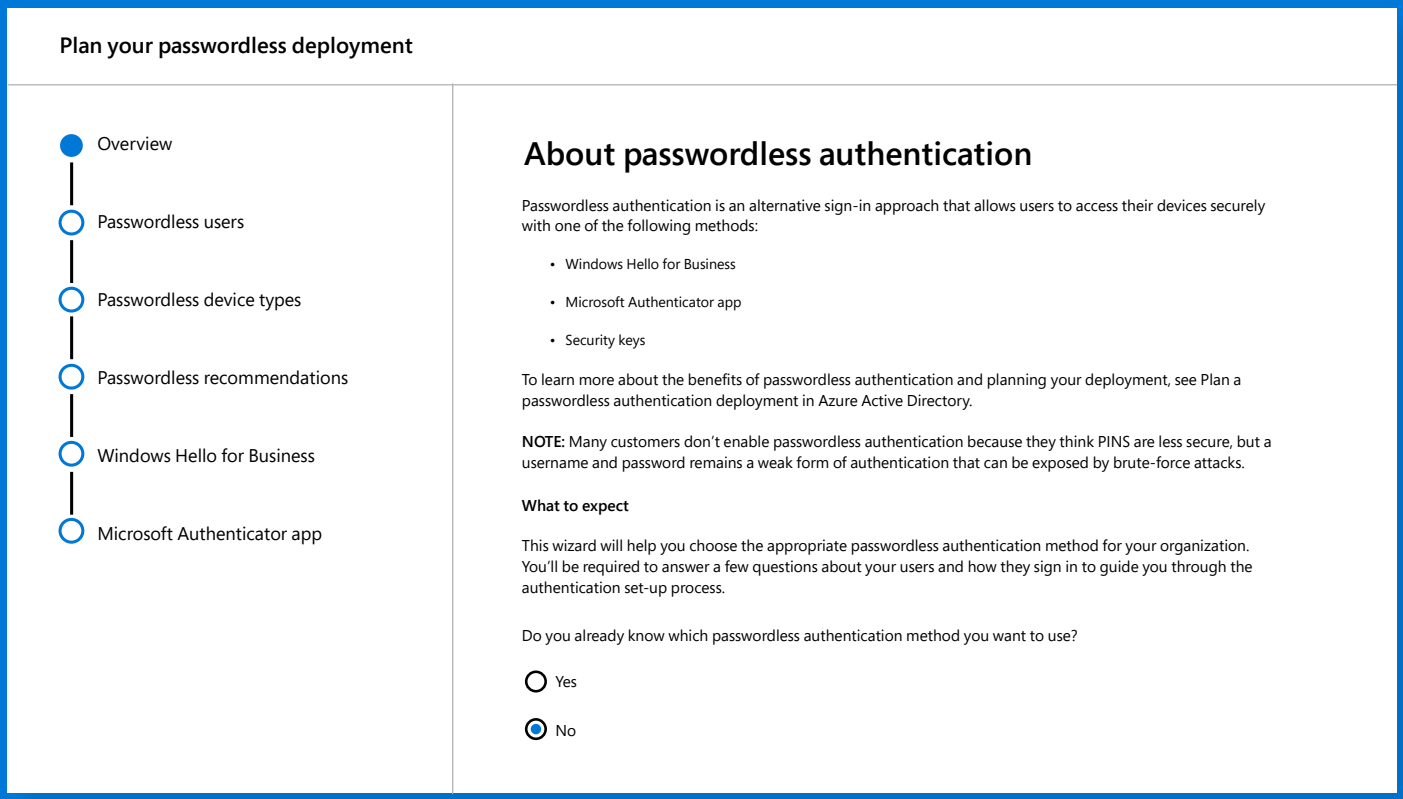
Using the Microsoft Authenticator app, Dan can now sign in to his work account using two-factor authentication on his phone. In the app, he matches the number, chooses to approve, and then provides his PIN to complete the authentication.

Persona	Scenario	Environment	Passwordless Tech
Administrator	Secure access to a device for management tasks	Assigned Windows 10 or 11 device	Windows Hello for Business and/or a FIDO2 security key
Administrator	Management tasks on a non-Windows device	Mobile or non-Windows device	Microsoft Authenticator app and/or a FIDO2 security key
Frontline Worker	Kiosks in a factory, plant, or retail space; data entry	Shared devices, Windows or non-Windows	FIDO2 security keys and/or Microsoft Authenticator app
Information Worker	Productivity work	Assigned Windows 10 or 11 device	Windows Hello for Business and/or a FIDO2 security key
Information Worker	Productivity work	Mobile or non-Windows device	Passwordless sign-in with the Microsoft Authenticator app

Microsoft offers solutions based on platform, hardware, or software that you can try out today and map with your passwordless authentication requirements. For example, introduced by Microsoft in Windows 10, Windows Hello uses biometric sensors or a PIN to verify a person's identity. Similarly, the Microsoft Authenticator app allows people to sign in to their work account, Microsoft account, or Azure Active Directory account from their desktop computer using their phone.

Moreover, Microsoft is continuously collaborating with FIDO Alliance working groups to further the development of passwordless authentication standards and technologies. As a result, Windows Hello works with portable FIDO2 hardware devices that allow for more secure authentication.

To help you identify the right solutions for your organization, the Microsoft 365 admin center offers a setup guide for planning your passwordless deployment.



Learn more about how to set up passwordless authentication.

“ Our numbers show that 99.9 percent of identity attacks have been thwarted by turning on MFA using the Microsoft solution.”

Alex Simons
Corporate VP of Program Management
Microsoft Identity Division
(Azure Active Directory Identity Blog)

Password replacement technology

What do we mean by passwordless authentication?

Passwordless authentication is a form of MFA used to replace passwords with secure alternatives. It requires two or more verification factors to sign in securely with a cryptographic key pair. The device creates a public and private key when registered. The private key can only be unlocked using a local gesture such as a biometric or PIN. Users have the option to either sign in directly via biometric recognition—such as a fingerprint scan, iris scan, or facial recognition system—or with a PIN that's locked and secured on the device.

Windows Hello for Business

Windows Hello for Business replaces passwords with strong two-factor authentication on Windows 10 platforms, including computers and mobile devices. This authentication consists of a new type of user credential linked to a device and uses a biometric or a PIN. It lets you sign in with your face, iris, fingerprint, or a PIN, and enables you to authenticate enterprise applications, content, and resources without storing a password on your device or in a network. Windows stores biometric data that's used to implement Windows Hello securely on the local device only.

How it works

The Windows Hello provisioning process generates a cryptographic key pair bound to the Trusted Platform Module (TPM) on a device. Access to these keys and obtaining a signature to validate the private key's user ownership is enabled only by the PIN or biometric gesture. During Windows Hello enrollment, two-step verification creates a trusted relationship between the identity provider and the user. When a user makes the gesture through the device, the provider can verify the identity from the combination of security keys and the gesture, activating an authentication token that allows Windows 10 or 11 to access resources and services.

Learn more about Windows Hello for Business and Authentication.

"Windows Hello for Business is personal, simple, and provides a brilliant user experience with high security. Our people love logging on with their fingerprint or face."

Peter Scott
Director of Dynamic IT
BT Technology

Microsoft Authenticator app

The Microsoft Authenticator app allows you to authenticate your work account, Microsoft account, or Azure Active Directory account. Instead of using a password, you confirm your identity using your mobile phone through a fingerprint scan, facial or iris recognition, or a PIN. Built on secure technology similar to what Windows Hello uses, this tool is packaged into a simple app that can be used on a mobile device. The Microsoft Authenticator app is available for Android and iOS.

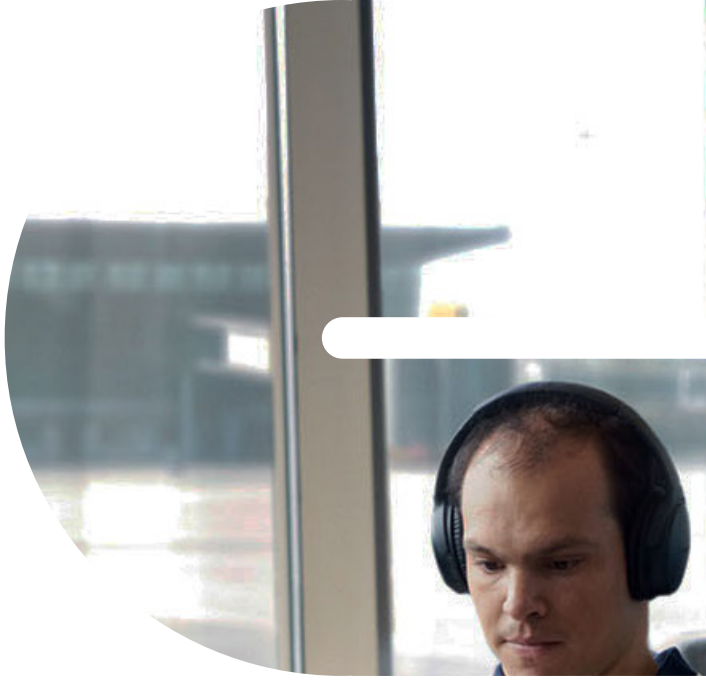
How it works

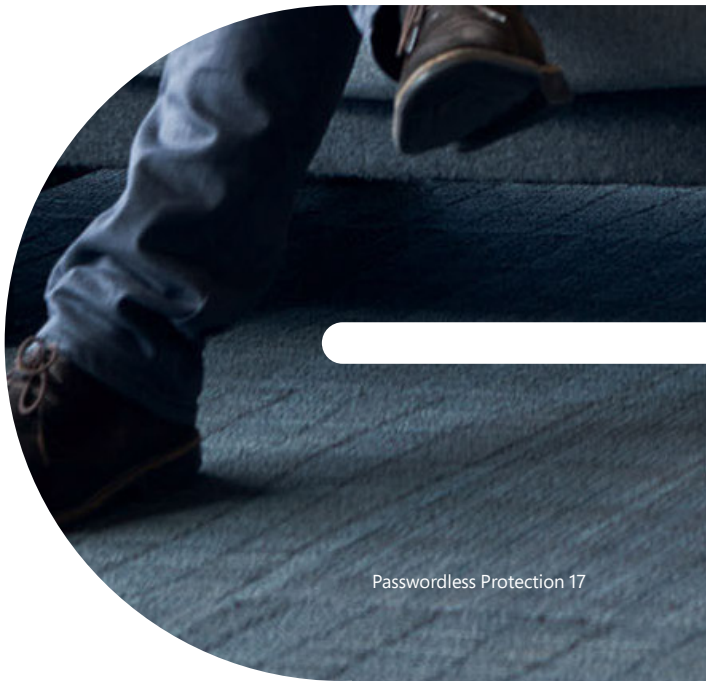
In place of encountering a password prompt after entering a username, a message tells the user to tap a number in their app. In the app, the user must match the number, choose Approve, then provide their PIN or biometric gesture to complete authentication. This two-factor verification method is considered more secure than a single password approach.

Learn more about how Microsoft Authenticator app works.

FIDO2 security keys

FIDO2 is an open authentication standard based on public key cryptography. This standard is intended to solve multiple scenarios, including strong first factor (passwordless authentication), strong second factor, and MFA. With these new capabilities, a security key can entirely replace weak static username/password credentials with strong hardware-backed public/private-key credentials. These credentials cannot be reused, replayed, or shared across services. Devices and tokens that adhere to FIDO2 and WebAuthn protocols bring about a cross-platform solution of strong authentication without the use of passwords. Microsoft partners are working on a variety of security key form factors, including USB security keys and near-field communication (NFC)–enabled smart cards.

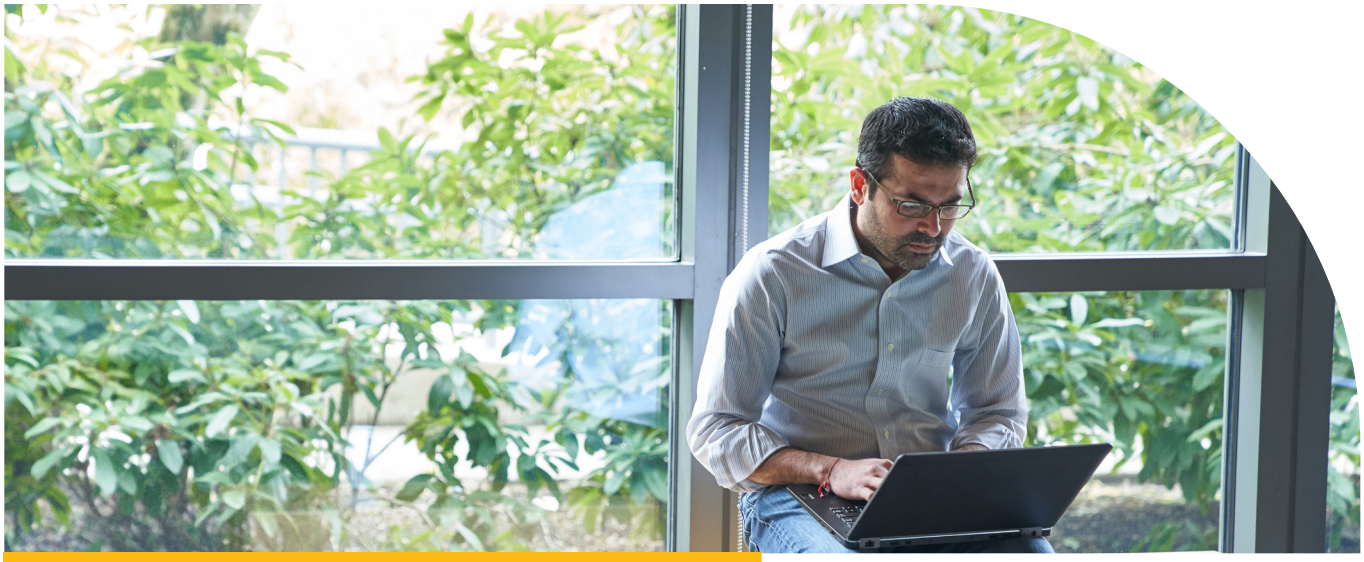




How it works

Microsoft has been working with partners on FIDO2 security devices for Windows Hello to enable secure authentication on shared devices. Security keys allow you to carry your credentials with you and safely authenticate to an Azure Active Directory–joined Windows 10 or 11 device that's part of your organization. You can use any shared Windows device belonging to your organization and authenticate securely—without having to enter a username and password or set up Windows Hello beforehand. Unlike traditional passwords, these keys rely on high-security, public-key cryptography to provide strong authentication. Plus, they have all the benefits of a TPM while also being portable, enabling Firstline and mobile workers to get their jobs done securely.

Learn more about how Windows Hello and FIDO2 security keys enable secure and easy authentication for shared devices.



> “Rather than adding friction with long passwords that create risk for the organization, we turned to biometrics. Now with Windows Hello, security is baked into our ecosystem, and we have better access to information with greater barriers to bad actors. It’s a win-win for our security team, our employees, and the company.”
>
> **Abid Adam**
> **Group Chief Risk and Compliance Officer**
> Axiata Group

Temporary Access Pass

Giving people flexibility when transitioning to passwordless device access can ease worry—but only when fail-safe options are available. For example, new employees in an organization may not have passwords or additional authentication methods for their new work devices. In this case, it’s important to have a different mechanism to create a passwordless credential registration process. Temporary Access Pass gives people a time-limited passcode. This passcode serves as a strong credential and allows people to register their passwordless authentication. It also enables users to gain access to their account when an authentication factor—like a FIDO2 security key or the Microsoft Authenticator app—is lost and a new method needs to be registered.

Temporary Access Pass configuration is available in the Microsoft Azure Active Directory portal and Microsoft Graph.

Comparing Microsoft technologies

The table below lists some key factors for consideration when choosing among Microsoft passwordless technologies.

	Windows Hello for Business	Microsoft Authenticator	FIDO2 security
Pre-requisites	• Windows 10, version 1809 or later, and Windows 11 • Azure Active Directory	• Microsoft Authenticator app • Mobile phone (iOS or Android device running Android 6.0 Marshmellow or above)	• Windows 10, version 1809 or later, and Windows 11 • Azure Active Directory
Mode	Platform	Software	Hardware
Systems and devices	• Computer with a built-in TPM • PIN and biometrics recognition	PIN and biometrics recognition on mobile phone	FIDO2 security devices that are Microsoft compatible
User experience	Sign in using a PIN or biometric recognition (facial, iris, or fingerprint) with a Windows device. Windows Hello authentication is tied to the device—the user needs both the device and a sign-in component such as a PIN or biometric factor to access corporate resources.	Sign in with a mobile phone using biometric recognition or a PIN. Sign in to a work or personal account from your computer or mobile phone.	Sign in using a FIDO2 security device (biometrics, PIN, and NFC). Access your device according to your org's controls and authenticate based on PIN or biometric-using device (USB security keys, and NFC-enabled smart cards, keys, or wearables).
Enabled scenarios	A passwordless experience with a Windows device. Applicable to dedicated work computers with single sign-on (SSO) capabilities for devices and applications.	Passwordless anywhere solution using a mobile phone. Applicable for accessing work or personal applications on the web from any device.	Passwordlesss experience using biometrics, PIN, and NFC. Applicable for shared computers and where a mobile phone is not a viable option (such as for helpdesk personnel, public kiosks, or hospital teams).

Understanding how these technologies work

All three technologies—Windows Hello for Business, the Microsoft Authenticator app, and FIDO2 security keys—use the same proven cryptographic authentication pattern, with credentials based on the certificate or asymmetrical key pair. These credentials, plus the tokens obtained using them, are bound to the device (Windows device or mobile phone).

Secure authentication flow architecture

The authenticator generates a key pair and returns the public key. Optionally, the authenticator also returns an attestation to the identity provider, such as Azure Active Directory.

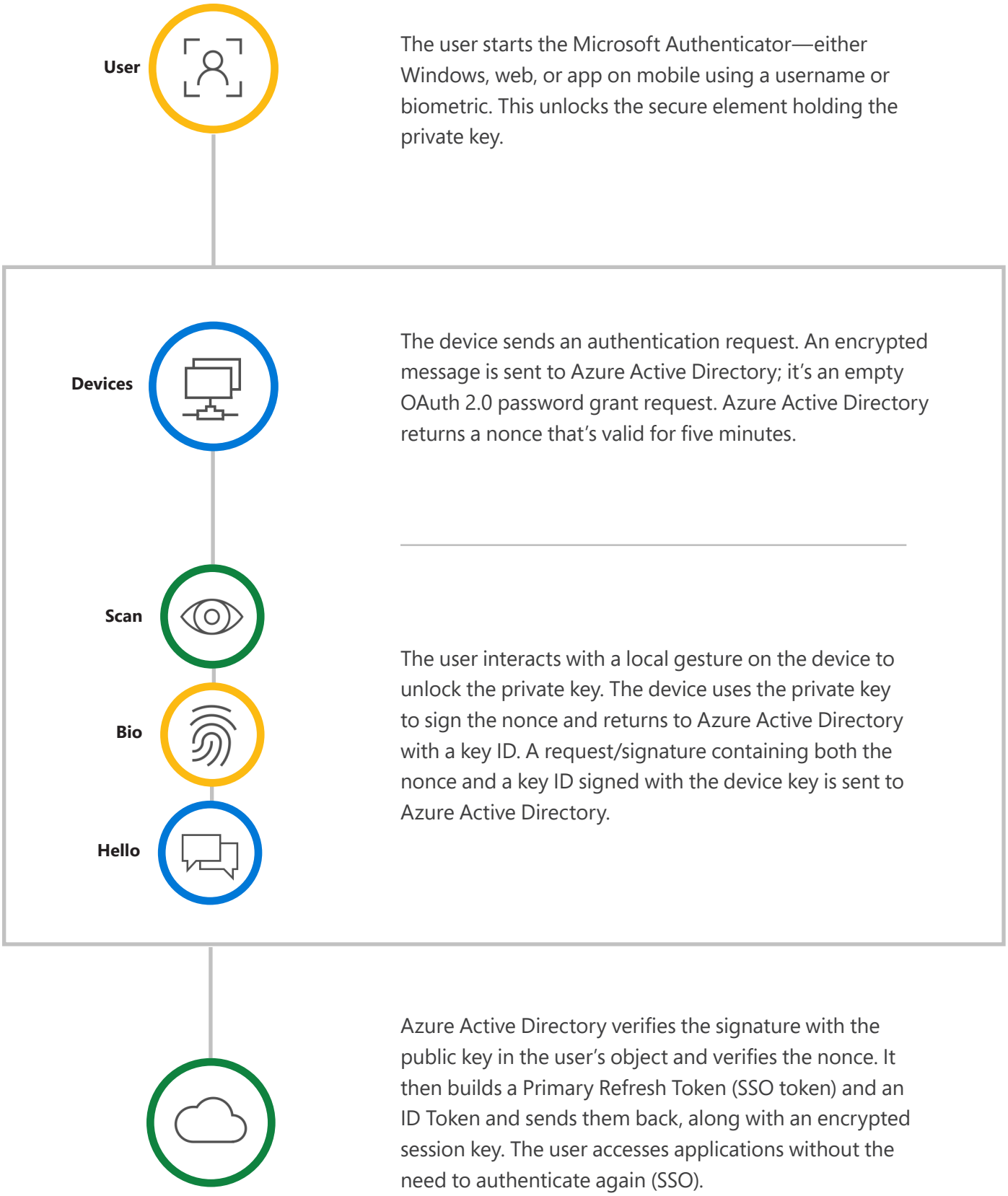
The identity provider validates user identity and maps the public key to a user account during the registration or provisioning step.

Two-factor authentication combines with a key or certificate tied to a device and something that the person knows (a PIN) or something that identifies them (biometrics).

Private keys are bound to a single device or token and never shared. These keys don't roam and are never sent to external devices or servers.

This kind of authentication requires a user gesture (for example, a biometric or PIN), which triggers devices to use the private key to sign data sent to the identity provider cryptographically. The identity provider verifies the user's identity and authenticates the user.

Signing in with secure authentication



The user starts the Microsoft Authenticator—either Windows, web, or app on mobile using a username or biometric. This unlocks the secure element holding the private key.

The device sends an authentication request. An encrypted message is sent to Azure Active Directory; it's an empty OAuth 2.0 password grant request. Azure Active Directory returns a nonce that's valid for five minutes.

The user interacts with a local gesture on the device to unlock the private key. The device uses the private key to sign the nonce and returns to Azure Active Directory with a key ID. A request/signature containing both the nonce and a key ID signed with the device key is sent to Azure Active Directory.

Azure Active Directory verifies the signature with the public key in the user's object and verifies the nonce. It then builds a Primary Refresh Token (SSO token) and an ID Token and sends them back, along with an encrypted session key. The user accesses applications without the need to authenticate again (SSO).

Common misconceptions

There are a few misconceptions associated with passwordless authentication.

Misconception 1

A PIN is the same as a password.

A PIN looks very much like a password—which may lead some people to believe they're the same thing. A PIN can be a set of numbers, but enterprise policy might allow complex PINs that include special characters and letters, both uppercase and lowercase. However, it's not the structure of the PIN (length or complexity) that makes it better than a password—it's how it works. A PIN is tied to the specific device it was set up on. Without the device, the PIN is useless. If someone stole your PIN and wanted to sign in to your account, they'd need your physical device, too.

Misconception 2

Passwordless authentication will impact my legacy apps and protocols.

Adopting passwordless authentication while still using legacy protocols does present challenges. However, Microsoft developed a time-limited password—a kind of one-time password with a current time or a time limit—that you can generate when using legacy authorization. Learn more about Temporary Access Pass.

Misconception 3

Biometric access systems can get hacked or spoofed.

Microsoft understands how critical it is to protect your biometric data from theft. For this reason, your biometric signature is secured locally on

the device and shared with only you. Plus, your signature is only used to unlock your device—and never to authenticate you over the network. Since biometric or PIN identification data is stored on the device, there's no single collection point an attacker can compromise to steal it.

In a typical deployment of FIDO2 and Windows Hello, a person swipes their finger, says a phrase, or looks at a camera on their device to sign in. Behind the scenes, the biometric data is used as an initial factor to unlock a second, more secure factor: a private cryptographic key that works to authenticate a person to the service.

A common biometric attack method involves trying to spoof someone's fingerprint or iris, with the goal of tricking the system into thinking it's real. Any spoofing or hacking attack would first require the attacker to gain custody of the device. Beyond the various layers of protection, many biometric systems today have built-in liveness detection to validate any biometrics presented.

Misconception 4

Without a password, users will get locked out if their devices are lost or stolen.

If the user doesn't have or know their password, they should maintain at least two or more factors for authentication. We recommend using the cloud backup option and biometric lock for the Authenticator app and keeping a back-up FIDO2 security key in the event that devices are lost. A Temporary Access Pass could also be used for account recovery, which is distributed to them from IT for one-time use. Monitoring for threats and using Azure AD Identity Protection can help to alert if suspicious activity is happening.

Leading the change to passwordless

Change isn't always easy. As organizations adopt passwordless authentication methods, cultural and technological challenges follow. Every organization is complex; while passwordless authentication offers improved security and user experience, most organizations need to fix fundamental facets before embarking on this journey—but it's an effort that pays off. From a technological standpoint, passwordless authentication seems to be a promising way to overcome security challenges.

Organizations can pass the benefits of passwordless authentication to their employees:

- Employees can sign up and use services faster with the improved user experience. They don't need to ever see or use a password.
- Passwordless authentication delivers a higher degree of trust and security for apps, devices, and service providers than passwords. There aren't any passwords to store, and there's nothing to hack or guess at.
- Passwordless authentication is cost-effective for IT, freeing support teams from endless password resets and reducing loss in productivity.

Progress over perfection

When trying to drive a culture shift, make it about the user outcome. Understand that you're encouraging people to switch from a widely adopted security system—passwords, which are familiar and conventional—to a modern one. People might think that this new technology is going to be hard or complicated, but you need to help them realize that it's simpler and better—and that a password isn't the key to their world. Put simply, passwords aren't enough—and it's time to evolve to the next level of authentication.

The importance of educating users

For passwordless authentication to succeed as it evolves, user acceptance is an absolute necessity. Launching an awareness drive about passwordless authentication can help people understand and affirm these new ways to authenticate their devices, whether by using Windows Hello for Business, Azure Active Directory-based apps, or other methods.

Organizations need to educate their employees about these topics and points:

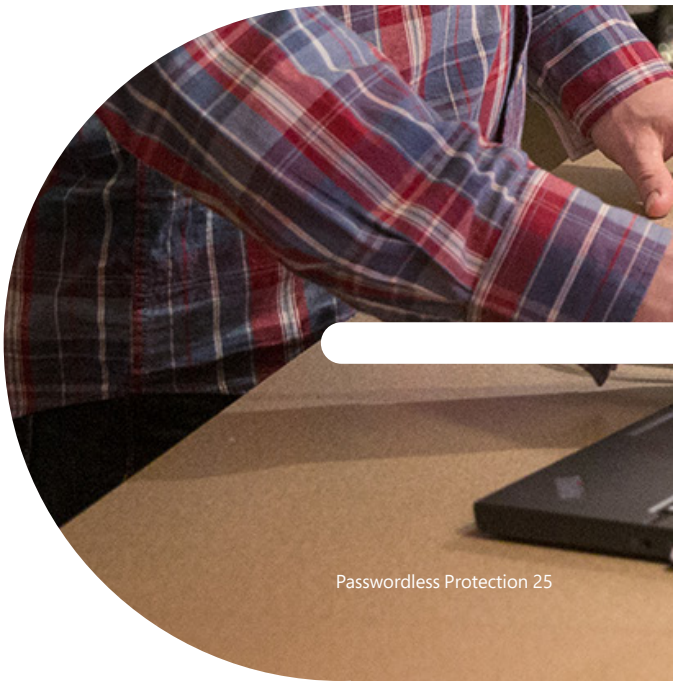
- Nobody likes passwords, except for bad actors. Passwordless technology not only makes authentication safer and stronger, but also easier and faster!

- Reusing passwords across work and personal accounts can have implications for your organization. Bad actors who obtain user information can use it in attacks like password spray. It only takes one person's account to compromise the organization. When passwords are no longer used, you're helping to protect your company.

- Phishing efforts often lead people to sign in to fake sites, consequently giving their usernames and passwords away. With passwordless authentication, physical keys are bound to the devices being used.

- A FIDO2 key won't authenticate with a website it doesn't trust.

Building awareness can help you answer objections, encourage questions and feedback, and explain the value of switching to passwordless authentication. By educating people, you can enable and inspire them to try passwordless authentication for themselves.



Summary

With a Zero Trust mindset, you must assume a breach could happen. However, the adoption of technologies like passwordless MFA is one of the best ways for organizations to lower the risk of an identity being compromised. To stay ahead of such threats, organizations can prepare by moving to password-free methods.

Passwordless authentication is the right approach—now and for the future—but it's still evolving. Understand that it takes time to transition and know what your options are for moving forward, given your organization's specific requirements. Consider starting small, with a pilot of one or two groups. Or, if you can't go passwordless right now, think about registering for MFA with Conditional Access, which helps to minimize user prompts and detect suspicious activity. Likewise, you can use intelligent password policies with Azure AD Password Protection and enable self-service password reset to help increase security.

Learn more

Learn how Microsoft can help you get started with passwordless authentication.

- Forget passwords, go passwordless
- Enable a remote workforce by embracing Zero Trust security
- Learn more with the passwordless deployment guide