Microsoft

Password-less protection

Reduce your risk exposure with password alternatives

Contents

Passwords are no longer enough

IT around the world see the beginning of a new era, where passwords are considered as a relic of the past. The costs now outweigh the benefits of using passwords, which increasingly become predictable and leave users vulnerable to theft. Even the strongest passwords are easily phishable. The motives to eliminate authentication systems using passwords are endlessly compelling and all too familiar to every enterprise IT organization. But how do you get there?

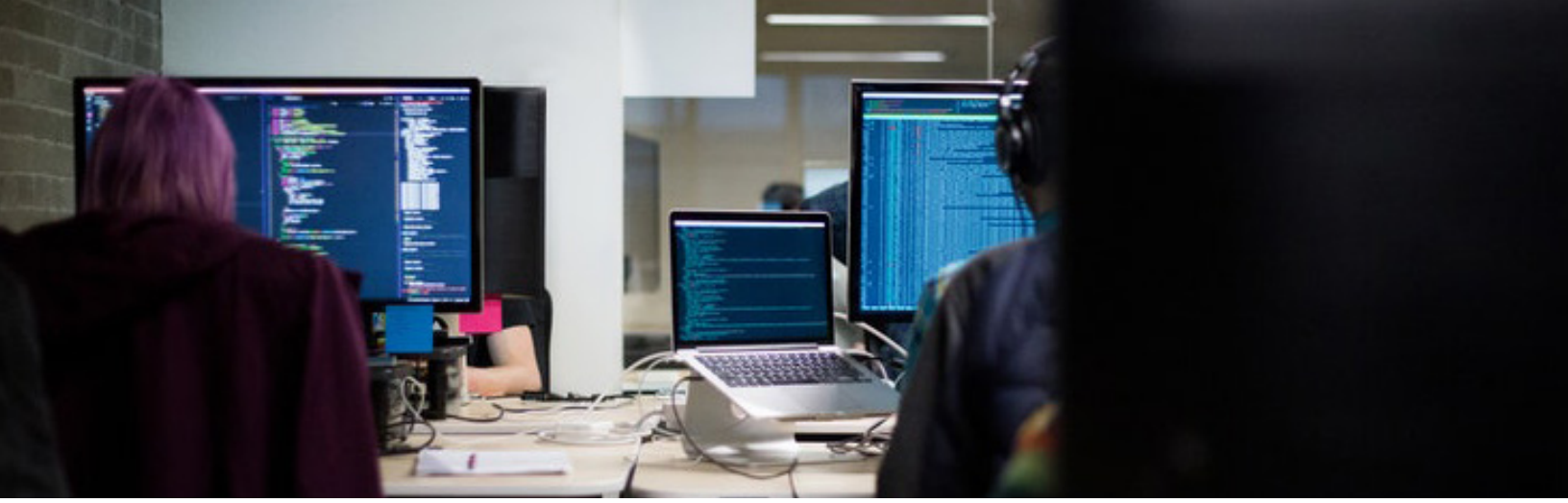
For enterprise IT departments, nothing costs more than password support and maintenance. It's common practice for IT to attempt lessening password risk by employing stronger password complexity and demanding more frequent password changes. However, these tactics drive up IT help desk costs while leading to poor user experiences related to password-reset requirements. Most importantly, this approach isn't enough for current cybersecurity threats and doesn't deliver on organizational information security needs.

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

Source: Verizon 2017 Data Breach Investigations Report

You can reduce your odds of being compromised by up to 99.9% by implementing multi-factor authentication (MFA).

Source: Microsoft 2018 Security Research



Why eliminate passwords?

Password authentication has always been challenging throughout the evolving enterprise security landscape. A password is supposed to provide a key to accessing an account and a security barrier to protect the account from the attackers. To distinguish between the account owner and the attacker, organizations have needed to move beyond using just passwords for protection.

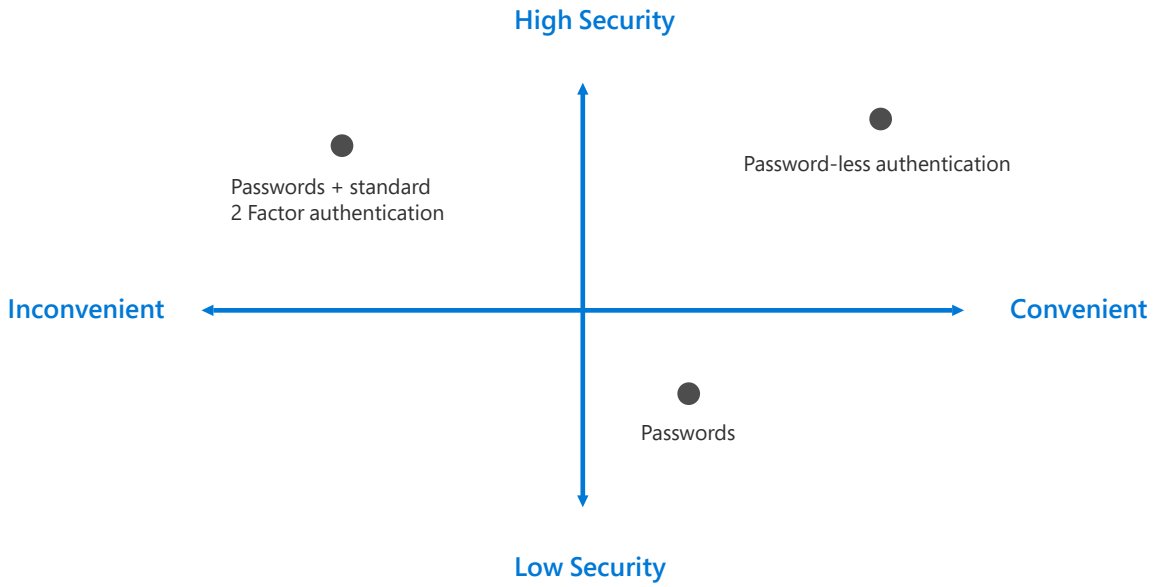
Multi-factor authentication (MFA)—for instance, a pin and password, or biometrics—has presented a more secure method for organizations. With increasingly complex access environments and more access points than ever before, IT teams have every reason to add multi-factor authentication options such as smart-cards, hard and soft tokens, SMS, and more—wherever users connect to resources. By going beyond passwords to add authentication steps, you can make user access to your resources more secure.

However, depending on the implementation, MFA can also lead to increasing complexity regarding the user experience. It's imperative for for IT teams to deliver a seamless user experience while balancing security risk.

Many years ago, we started multi-factor authentication with smart-cards to secure the identity of our employees. Initially, we used physical smart-cards to secure, but it didn't give people a smooth user experience. Additionally, this also requires a card reader in each hardware device which can be challenging to implement and also smart-cards are prone to be lost or forgotten. Then we focused on a nearly-friction-free experience, from using biometrics that allows people to use fingerprints, iris scans, facial recognition, and even heartbeats to authenticate their identity. These technologies are easier to use, more accessible to the needs and preferences of the person, and are significantly harder for criminals to exploit.

–Bret Arsenault, CVP & CISO, Microsoft

Source: Enterprise Security magazine



Today, IT security are moving toward password-less authentication using advanced technologies like biometrics, PIN, and public/private key cryptography. Plus, new standards like Web Authentication API (WebAuthN) and Fast Identity Online (FIDO2) are enabling password-less authentication across platforms. These standards are designed to replace passwords with biometrics and devices that people in your organization already use, such as security keys, smartphones, fingerprint scanners, or webcams.

Password replacement options can help organizations provide convenience and ease-of-use without high-security risks. Ideally, with password-less authentication, you can have a future ecosystem of authentication that meets the organizational needs of high security and privacy, usability, and interoperability among different authentication devices.

Moving forward, end-users should never have to deal with passwords in their day-to-day lives. And with an intuitive sign-in/sign-up user experience, help desk costs can be reduced.

Introduction to password replacement technology

What do we mean by password-less authentication?

Password-less authentication, as we refer to it in this brief, is a form of multi-factor authentication that replaces the password with a secure alternative. This type of authentication requires two or more verification factors to sign in that are secured 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 fingerprint scan, facial recognition, or iris scan—or with a PIN that's locked and secured on the device.

Adopting a password-less strategy

At its core, the underlying principle of password-less authentication is to eradicate the use of passwords and thereby drain their value for attackers. Moving forward with this approach requires technologies that can support it—and time for organizations and users to adopt these technologies. Adoption also involves a new mindset. Organizations have to understand how the approach works with their flow of operations and make the necessary technical and cultural shift, so that users can operate in this new password-less world.

Here are the key considerations for implementing password-less authentication into your MFA strategy:

1. Choosing the right technology – Develop password-replacement offerings with a new set of alternatives that address the shortcomings of passwords while embracing their positive attributes. This early stage is about implementing an alternative and getting users acquainted with it.

2. Understanding how it works – Get to know how password-less technologies overcome security challenges and reduce the user-visible password-surface area. Adopting these technologies means upgrading experiences related to the life-cycle of a user's identity—including provisioning of an account, setting up a brand-new device, using the account/device to access apps and websites, and enacting recovery. It also means deconditioning users from providing a password any time a password prompt shows on their computer.

3. Increasing user adoption – Simulate a password-less world—that is, enable end users and IT admins to replicate the approach in a test environment and transition into a password-less world with confidence. This simulation should encourage a cultural shift within the organization—getting users comfortable with the idea of never typing, changing, or even knowing a password going forward.

Choosing the right technology

With biometrics on mobile phones and computers becoming more ubiquitous, the number of password replacement technologies has increased.

Microsoft offers solutions based on platform, hardware, or software that you can try out today and map with your password-less authentication requirements. Introduced by Microsoft in Windows 10, Windows Hello uses biometric sensors or a PIN to verify a user's identity. The Microsoft Authenticator app is a software token that allows users to verify their identity with a built-in biometric or a PIN when signing into their work or personal accounts from a mobile phone.

As a member of the FIDO Alliance, Microsoft has been working with other alliance members to develop open standards for the next generation of credentials. As a result, you can now use portable FIDO2 hardware devices to log into a work machine or cloud services on supported devices and browsers.

Let's go into more detail on each of these technology options.

Windows Hello for Business

Windows Hello for Business replaces passwords with strong multi-factor authentication on Windows 10 platforms, including PCs and mobile devices. This authentication consists of a new type of user credential that's linked to a device and uses a biometric or PIN. It lets you sign in with your face, iris scan, fingerprint, or a PIN, and enables you to authenticate to enterprise applications, content, and resources without a password being stored on your device or in a network at all. The biometric data is only used locally and never leaves the device.

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 user ownership of the private key is enabled only by the PIN or biometric gesture. Taking place during Windows Hello enrollment, the 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 is able to verify the identity from the combination of Hello keys and the gesture. This activates an authentication token that allows Windows 10 to access resources and services. For further information, go to 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, British Telecom Technology

As of October 2018 there are 89 million active Windows Hello users worldwide. More than 6,500 organizations have deployed Windows Hello for Business. Major PC vendors are shipping devices that have integrated Windows Hello-compatible cameras or fingerprint readers.

Microsoft Authenticator app

Millions of people are using the Microsoft Authenticator app every day to better secure their sign-ins.

The Microsoft Authenticator app enables users to verify their identity and authenticate to their work or personal account. Microsoft Authenticator can be used to augment a password with a one-time passcode or push notification. The app can also be used to verify multiple factors and replace the need for a password. Instead of using a password, users confirm their identity using your mobile phone through fingerprint scan, facial or iris recognition, or PIN. Built on secure technology similar to what Windows Hello uses, this tool is packaged into a simple app on a mobile device making it a convenient option for users. The Microsoft Authenticator app is available for Android and iOS.

How it works

In place of encountering a password prompt after entering a username, users get a push notification to verify presence. In the app, users confirm their presence by matching a number on the sign-in screen, then providing a face scan, fingerprint, or PIN to unlock the private key and complete the authentication. This multi-factor verification method is more secure than a password and more convenient then entering a password and a code. In some cases it doesn't require any typing at all! For further information, go to How to use the Microsoft Authenticator app.

FIDO2 security keys

FIDO2 is an evolution of the U2F open authentication standard based on public key cryptography using hardware devices. This standard is intended to solve multiple user scenarios including strong first factor (password-less) and multi-factor authentication. 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, WebAuthN, and CTAP protocols bring about a cross-platform solution of strong authentication without using passwords. Microsoft partners are working on a variety of security key form factors, such as USB security keys and NFC-enabled smart cards.

How it works

Microsoft has been working with partners to ensure FIDO2 security devices work on Windows, the Microsoft Edge browser, and online Microsoft accounts, to enabling strong password-less authentication. For shared device scenarios, security keys allow you to carry your credential with you and safely authenticate to an Azure AD joined Windows 10 device that's part of your organization. You can use any shared Windows device belonging to your organization and authenticate securely—without needing 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, these keys have all the benefits of a secured enclave to store credentials while also being portable, enabling more use cases for deskless and kiosk workers.

Security devices fit nicely with our current scenarios. They are simple to deploy and easy to use. We see value in rolling FIDO2-enabled HID badges to all 110,000+ Emirates Group staff in the future.

–Emirates IT

Microsoft has been aligned with the FIDO Alliance from the start; the alliance represents 250 organizations from various industries on a joint mission to replace passwords with an easy-to-use, strong credential.

Comparing the Microsoft technologies for password-less authentication

Here are some factors for you to consider when choosing Microsoft password-less technology:

	Windows Hello for Business	**Microsoft Authenticator app**	**Fast Identity Online (FIDO) 2 security devices**
Pre-Requisite	Windows 10, version 1511 or later Azure Active Directory	Microsoft Authenticator app Phone (iOS and Android devices running Android 6.0 or above.)	Windows 10, version 1809 or later Azure Active Directory
Mode	Platform	Software	Hardware
Systems and devices	PC with a built-in Trusted Platform Module (TPM) PIN and biometrics recognition	PIN and biometrics recognition on phone	FIDO2 security devices that are Microsoft compatible
User experience	Sign in using a PIN or biometric recognition (facial, iris, or fingerprint) with Windows devices. 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 using a mobile phone with fingerprint scan, facial or iris recognition, or PIN. Users sign in to work or personal account from their PC or mobile phone.	Sign in using FIDO2 security device (biometrics, PIN, and NFC). User can access device based on organization controls and authenticate based on PIN, biometrics using devices such as USB security keys and NFC-enabled smartcards, keys, or wearables.
Enabled scenarios	Password-less experience with Windows device. Applicable for dedicated work PC with ability for single sign-on to device and applications.	Password-less anywhere solution using mobile phone. Applicable for accessing work or personal applications on the web from any device.	Password-less experience for workers using biometrics, PIN, and NFC. Applicable for shared PCs and where a mobile phone is not a viable option (such as for help desk personnel, public kiosk, or hospital team).

Understanding how strong authentication works

Secure authentication flow architecture

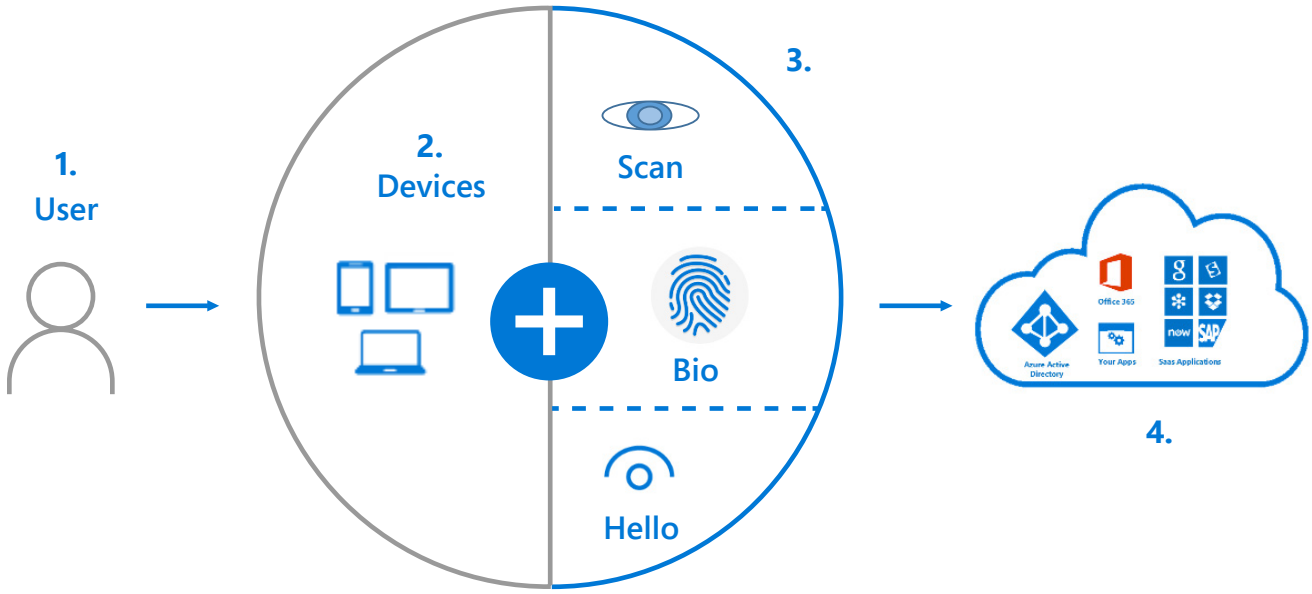
All three technologies use the same proven cryptographic authentication pattern, with credentials based on the certificate or asymmetrical key pair. These credentials—plus the token that is obtained using the credential—are bound to the device (Windows or FIDO2 device, or mobile phone).

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.

Identity provider validates user identity and maps the public key to a user account during the registration or provisioning step. Authentication requires multiple factors, combining a key or certificate tied to a device and something that the person knows (a PIN) or something that the person is (biometrics). Private keys are securely stored on the device. Private keys are bound to a single device and never shared. These keys don't roam and are never sent to external devices or servers.

This kind of authentication requires a local gesture. PIN entry and biometric gesture both trigger devices to use the private key to sign data that's sent to the identity provider cryptographically. The identity provider verifies the user's identity and authenticates the user.

Secure authentication flow architecture



1. The user attempts to sign into their account from a device. The device sends an authentication request. The identity system (for example, Azure AD) requests validation.

2. The user interacts with a local gesture (for example, biometric, PIN) from its device. The device uses the private key to sign nonce and returns to Azure AD with key ID. A request/ signature containing both the nonce + the key ID signed with the device key sent to Azure AD

3. Azure AD verifies the signature with the public key in the user object and verifies nonce. Builds a Primary Refresh Token (SSO token) and an ID token and send them back along with an encrypted session key. The user accesses applications without the need of authenticating again (SSO).

Common misconceptions

Misconception 1:

Isn't a PIN the same as a password?

A PIN looks much like a password, which may lead people to equate them. 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 that makes it better (length, complexity), but rather how it works. A PIN is tied to the specific hardware 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:

If I use password-less authentication, doesn't that impact my legacy app and protocols?

Adopting password-less authentication when still using legacy protocols does present challenges. However, for this purpose, Microsoft is developing a time-limited password—a kind of one-time password with a current time or a time limit that the user could generate when using legacy authorization.

Misconception 3:

Can't a biometric access system 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 no one but you. Plus, your signature is only used to unlock your device and never to authenticate you over the network. As it just stores biometric or PIN identification data on the device, there's no single collection point an attacker can compromise to steal biometric data.

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

A common biometric attack method involves trying to spoof a person's body part, with the goal of tricking the system into thinking that a fake is real. Any spoofing or hacking attack would first require that the attacker gains custody of the device. Beyond the various layers of protection, many biometric systems today are building in "liveness detection" to validate that a biometric presented is real.

User adoption

No change is easy. Cultural and technical challenges follow organizations as they proceed with password-less authentication methods.

Every organization is complex; while password-less authentication offers improved security and user experience, most organizations need to fix many fundamental facets to start on this journey. These fixes can be implemented over time to additional groups to reduce your risk of attacks and security breaches. That effort offers rewards, however. From a technological viewpoint, reducing the use of passwords and eventually eliminating them can help you make a sea change in both security and productivity for your organization.

Getting rid of passwords can help you enjoy these benefits:

As a user, you can sign in faster to use applications and services. There are no passwords to create, store, or remember.

Password-less authentication delivers a higher degree of trust and security for apps, devices, and service providers. You don't have to store passwords.

It's cost-effective for IT. IT support teams can be freed from endless password problems.

Old-school mentality

It's nearly impossible for an organization to visualize how different individuals go about their day-to-day activities, or to validate this password-less change accurately. It's crucial for organizations to do just that. Understand that you're encouraging people, including many in IT leadership, to switch from a widely adopted security system, like passwords, that's very familiar, comfortable, and conventional. And don't forget: change for most people is hard. Yet, in this case, once users experience password replacements, they'll forget that they even needed to enter passwords on a day-to-day basis or reset passwords on their own in a self-service portal. You need to make them realize it's simpler, better, and help them erase the mentality that a password is the key to their world. Passwords are not enough anymore. It's time to go to the next level of authentication.

Educating users on new authentication methods

The successful evolution of password-less authentication heavily relies on user acceptance. An awareness drive on these new password-less authentication methods can help users understand and affirm the new way of authenticating to their devices, such as using Windows Hello for Business or Microsoft Authenticator-based applications.

Organizations need to educate their users that:

1. Hackers easily guess passwords. One encouragement could be that MFA is simply making their password authentication better and stronger.

2. Companies that have experienced data breaches may have leaked user data to the web. Hackers that obtain user information can use that information to guess further passwords because users often use the same, or a derivative password, for several sites or services.

3. Phishing efforts often lead users to sign in to fake sites, giving their usernames and passwords away. With password-less authentication, this is an issue of the past because the physical keys are bound to the machines they use and FIDO2 tokens will not authenticate with a website it doesn't trust.

This awareness practice can answer some of the objections, encourage questions and feedback, and explain the value of this change. The user education enables and inspires users to try the experience out.

Summary

The adoption of modern multi-factor authentication technologies—like biometrics and public key cryptography in widely accessible devices—is one of the most impactful steps that can meaningfully reduce a company's identity risk. Given emerging requirements, organizations can prepare themselves by making a plan to start moving to to password-less technologies.

Going password-less is a long-term approach for secure authentication, and it's still evolving. It can take time to transition. You can start with a pilot of one or more options. For users that can't go password-less, turn on MFA to validate users and minimize prompts based on the risk of the sign-in with conditional access capabilities. Use a password filter to block leaked credentials and common passwords from being used with password protection policies.

For more information, here are some resources that can help you get started:

Overview of Microsoft password-less technologies

Windows Hello for Business documentation

About the Microsoft Authenticator app