PingIdentity x identIT

Passwordless Authentication

Getting Started on Your Passwordless Journey

WHITE PAPER

Table of Contents

Introduction

Passwords are problematic. They're arguably the weakest link in security, a leading cause of breaches, and difficult to manage. Passwords are just bad—bad for security and bad for user experiences. Yet, despite their shortcomings, passwords remain ubiquitous. Adopting passwordless authentication can solve the inherent problems of passwords to deliver stronger security and better user experience.

For customers, passwordless improves engagement, lowers abandonment rates and ultimately drives higher revenues. For employees, less time entering and resetting passwords means higher productivity and significantly less strain on helpdesks. The security benefits are also clear: 80% of breaches involve brute force attacks or the use of lost or stolen credentials.[1] Passwordless provides a clear long-term solution to better security and user experience.

Passwordless technology is readily available today and many organizations want to pursue it. But, adoption is still low. That's because passwordless is not a single solution per se, but rather one that requires integrations of multiple products and technologies. Also, it's not simply an IT or security decision but rather requires buy-in from various leaders throughout an organization.

Lastly, every organization has its own unique technology and use case requirements that must be addressed.

As a result, businesses are often confused about where to start and how to increase passwordless adoption amongst their users.

Read on to learn more about the challenges that come with passwords, why we're still using them and what passwordless authentication is. Finally, we'll offer guidance on how organizations can navigate their passwordless journeys from start to finish and the various options available to them.

80% of breaches involve brute force attacks or the use of lost or stolen credentials.

Source: Verizon 2020 Data Breach Investigations Report

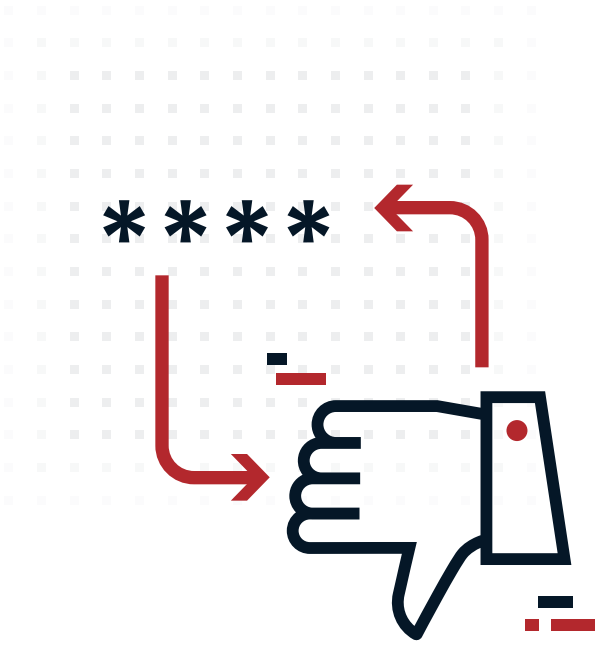
1 Verizon 2020 Data Breach Investigations Report; Source

The Problem With Passwords

No matter how you slice it, passwords present usability and security problems. They are an accepted inconvenience that we've become numb to. Here are some of the common problems:

Passwords Aren't User Friendly

The average person uses roughly 191 services that require them to enter passwords or other credentials.[2] And that number is growing. As employees and customers have way more passwords to keep track of than ever before, their frustration will only continue to grow.



While short and simple passwords are easy to remember, they are weak and easy to crack. Organizations have forced users to create long and complex passwords in the name of security. But all this has done is make users more frustrated, while also increasing the likelihood that they will reuse the same passwords across multiple websites. This can actually have the opposite effect when it comes to securing these users.

Passwords Aren't Secure

Why? 70% of people use the same usernames and passwords across various sites, which presents an easy target for criminals.[3] If credentials are compromised through phishing or brute force attacks, hackers may try those same username and password combinations elsewhere. With over 15 billion compromised credentials in circulation on dark web forums,[4] it's no wonder the majority of today's breaches involve compromised credentials.

2 From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover, Digital Shadows, 2020; Source
3 Griffith, Eric, "Stop Using the Same Password on Multiple Sites! No. Really" PCMag, Sept 21, 2021; Source
4 From Exposure to Takeover, Digital Shadows, 2020; Source

Why Are We Still Using Passwords

This begs the question: why are we still using passwords? And why is passwordless adoption so slow? The truth is that most security teams realize passwords offer weak security. But with the use of passwords dating back to the invention of computers, old habits die hard.

There are a few reasons why passwords remain prevalent. Common roadblocks include:

1 Technical debt

Today's enterprises still depend on legacy systems, applications, and registration flows that are built around passwords. Critical day-to-day operations run on them and reverse engineering them for passwordless is difficult. Despite the obvious long-term benefits of passwordless authentication, re-wiring legacy infrastructure with the potential for downtime is a high risk endeavor. Compatibility concerns are also a deterrent to adopting passwordless. Organizations need full confidence that their systems will be compatible with passwordless solutions. This is a significant obstacle that feeds into the next hurdle to adopting passwordless.

2 Fear of change

Passwords have been ingrained in our mindset and provide us with a false sense of comfort. They are also relatively easy for organizations to implement. Using passwords is the path of least resistance for many organizations, despite their shortcomings. In contrast, pursuing passwordless authentication may require some near-term user adoption and education challenges.

3 Various user scenarios

Every organization is different. There is no one size fits all approach for passwordless and there are a wide range use cases that must be considered. A passwordless solution needs to have flexibility and scale.

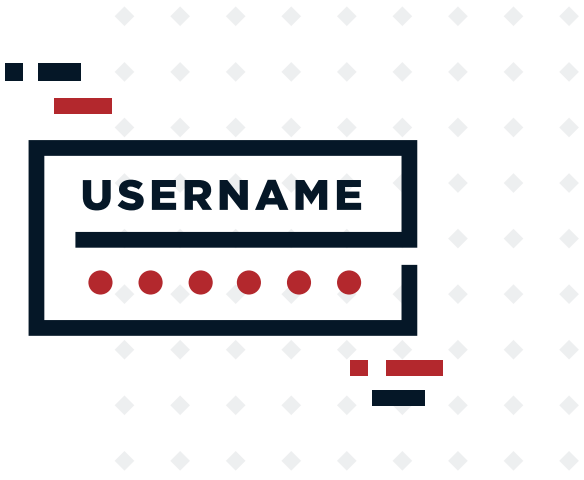
For example, a manufacturer will have different types of workers in both offices and factories. These workers have different requirements. An office worker behind the scenes may be able to login using a thumbprint on their own device, while a worker on the factory floor may be using a shared device with gloves on and will need to authenticate via retina scan.

The diverse set of user scenarios and use cases combined with the lack of out-of-the-box, plug-and-play passwordless solutions can block passwordless adoption. The key is to take inventory of all your existing technologies and define the various authentication use cases you have. Then start small and expand.

4 Terminology

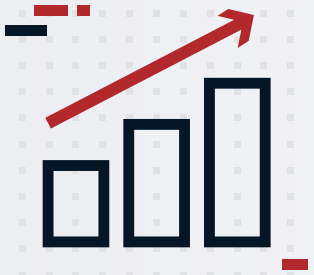
Another problem is that the term itself, "passwordless" can be interpreted as less secure despite it actually being the opposite and offering stronger security. This raises an important question: is "passwordless" the proper term and could this be holding up adoption?

The ultimate goal is frictionless, secure authentication. Given that the term passwordless literally means "no passwords"—which the average person associates with a layer of security—perhaps "Passwordless" erroneously infers less protection to some audiences. The misunderstanding about what passwordless truly means may discourage organizations from adoption.



Why Go Passwordless

By 2025, more than **50%** of the workforce and more than **20%** of customer authentication transactions will be passwordless, up from less than **10%** today.[5]



For Customers

The frustration of creating and keeping track of multiple different passwords comes at a cost. 56% of consumers have abandoned an online service when logging in was too frustrating.[6] If your customers can't remember their password, their next step is often to abandon their shopping cart rather than go through the password recovery flow. While using passwords is inexpensive, the ultimate cost in terms of lost revenue can be significant.

Passwordless significantly improves user experience by making online access seamless and secure. 46% of consumers prefer sites that offer alternatives to passwords and 53% feel better when using MFA to sign into sites or services.[7] Customers are already familiar with passwordless biometric logins on their smartphones. By offering passwordless authentication, businesses can not only improve customer experiences, but also reduce abandonment rates and improve their bottom lines.

56% of consumers have abandoned an online service when logging in was too frustrating.

46% of consumers prefer services or sites that offer alternatives to passwords and 53% feel better when using MFA to sign into sites or services."

Source: Ping Identity "2021 Consumer Survey: Brand Loyalty is Earned at Login"

5 Gartner, "Take 3 Steps Toward Passwordless Authentication"; Source
6 Ping Identity, "2021 Consumer Survey: Brand Loyalty is Earned at Login"; Source
7 Ping Identity, "2021 Consumer Survey: Brand Loyalty is Earned at Login"; Source

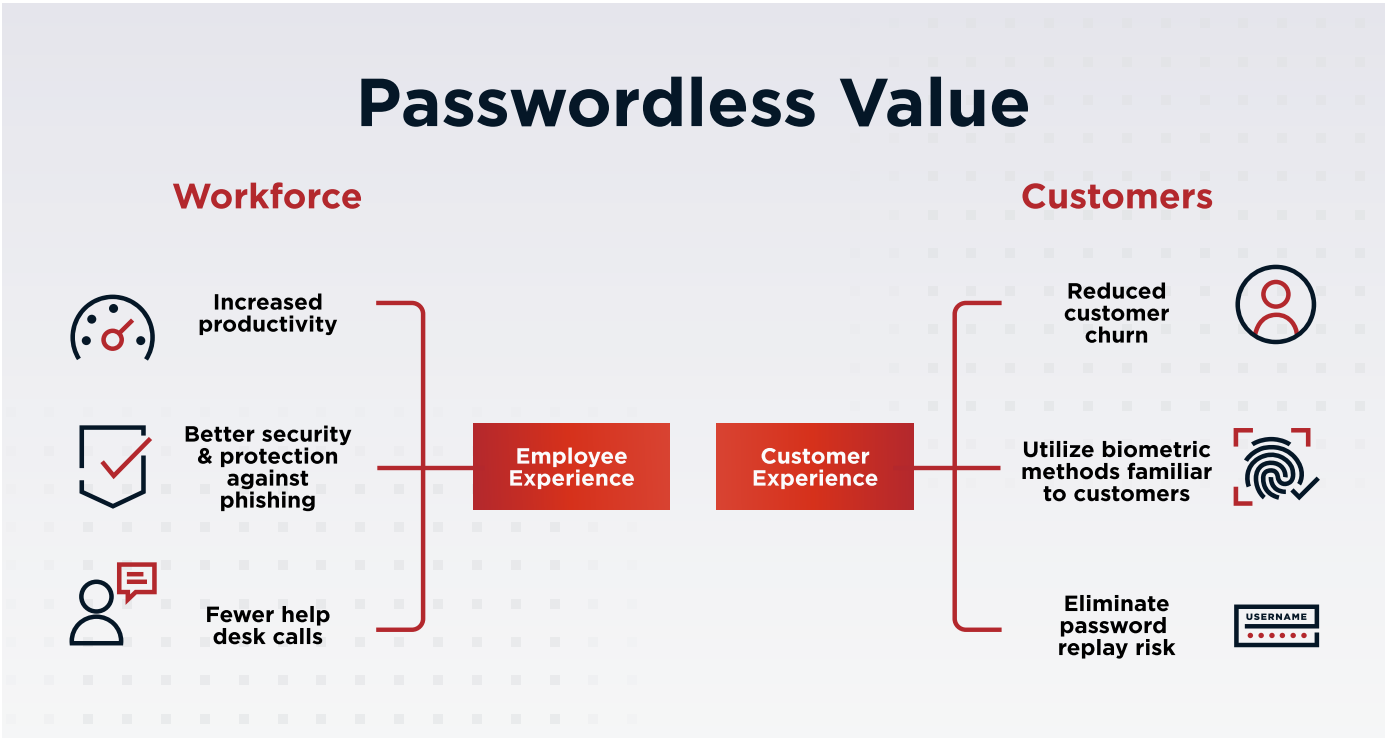
Workforce

When it comes to employee identities, passwords are very expensive for organizations. On average, 11 hours are lost annually from password resets, 12 minutes are spent daily entering and resetting passwords[8], and 33% of IT department's tickets are related to passwords.[9] For a company of 15,000 employees, the estimated cost of lost productivity per organization averages $5.2 million annually.[10]

The average cost of a data breach is $4.24 million.

Source: 2021 Cost of a Data Breach Report, IBM Security.

Passwords increase your risk of a breach too. Credential stuffing, also known as "credential recycling" or "replay attacks," is a genre of brute force attacks where an attacker tests username and password combinations that have been leaked or stolen from the dark web and other websites. This technique works for attacks against users who have reused their login credentials across multiple online accounts. These types of attacks are successful up to 2% of the time.[11] This statistic might not seem that threatening, but if you have 1,000 employees or customers and rely on passwords, it can translate to as many as 20 compromised accounts. Organizations that adopt passwordless authentication for their employees will dramatically lower their security risks and enhance worker productivity and satisfaction.



8 "Up to 11 hours spent every year resetting passwords"; Source
9 Ping Identity, "Our Passwordless Future: A New Era of Security"; Source
10 "Up to 11 hours spent every year resetting passwords"; Source
11 Soverson, Jarrod. "What Your Login Success Rate Says About Your Credential Stuffing Threat", Source

Preparing to go Passwordless

The path to passwordless can lead to more questions than answers. “Passwordless” can have different definitions depending on who you ask. It can mean replacing passwords with another primary authentication method, such as a fingerprint or facial scan. Or it can mean removing passwords completely.

Passwordless is not a specific product or capability but rather a technology-agnostic end goal or future state. Most likely it will leverage multiple technologies to improve experiences and security by minimizing your reliance on passwords. Ultimately, you will want to remove passwords altogether and replace them with stronger methods of authentication.

83% of those with no plans for passwordless authentication admit their organization is unsure how to implement this, and **33%** say a lack of experience is a barrier to adoption.[12]

Passwordless Stages

Going passwordless has two main stages:

- **Use fewer passwords:** First reduce your password footprint with SSO. Then, strengthen password security with MFA. Finally, use alternative factors as the primary method of authentication, such as biometrics. For example, when a customer wants to access their bank account, they are often given the option of authenticating via a biometric or an authenticator app. In this case, a password was required during initial account registration and already exists on the back end. Password replacement often comes earlier on in an organization’s passwordless journey.
- **Get rid of passwords altogether:** Ultimately, your organization’s goal is for users to be able to register accounts without ever needing to use a password at all. This can involve using digital ID proofing and using a standards-based approach like FIDO to authenticate while layering in risk signals to continuously authenticate a user’s session. In this use case, users can create accounts firmly bound to their identities through a biometric factor, such as a selfie or a fingerprint scan plus their mobile device, without ever needing to create a password.

Never having passwords at all to begin with offers multiple benefits. One is that users and businesses never have to store passwords, thereby eliminating the risk of a password database being leaked or stolen. Another is that users no longer must go through the cumbersome process of creating passwords and keeping track of them. This saves time, reduces registration friction, and frees up resources.

12 Ping Identity, “Our Passwordless Future: A New Era of Security”; Source

Evaluating Authentication Factors

Every authentication factor other than a password is—by definition—passwordless. But not all authentication methods are created equally. To determine which options will be best for you, you need to first be familiar with the different passwordless authentication categories and methods and their relative strengths and weaknesses.

Weak authentication factors:

- **Something you know:** Passwordless boils down to eliminating the weakest factor, which is usually "something you know," otherwise known as knowledge-based questions (KBAs). Examples include passwords, PINs, and challenge questions such as "What is your mother's maiden name?" These can easily be guessed, stolen or cracked.

Alternate and stronger authentication methods include push notifications, SMS or email OTPs (one-time passcodes), QR codes, security keys or biometric factors like fingerprint scans and facial recognition.

How the journey to passwordless will look for your business ultimately depends on assessing where you are in these stages. These more robust authentication methods fall into two categories:

Strong authentication factors:

- **Something you have:** Authentication factors in this category verify that you are in possession of a specific item. Examples include a phone on which you could receive a text message or an ATM card.
- **Something you are or do:** This usually refers to biometrics, with the most common verification methods being a fingerprint scan, facial recognition or voice recognition.

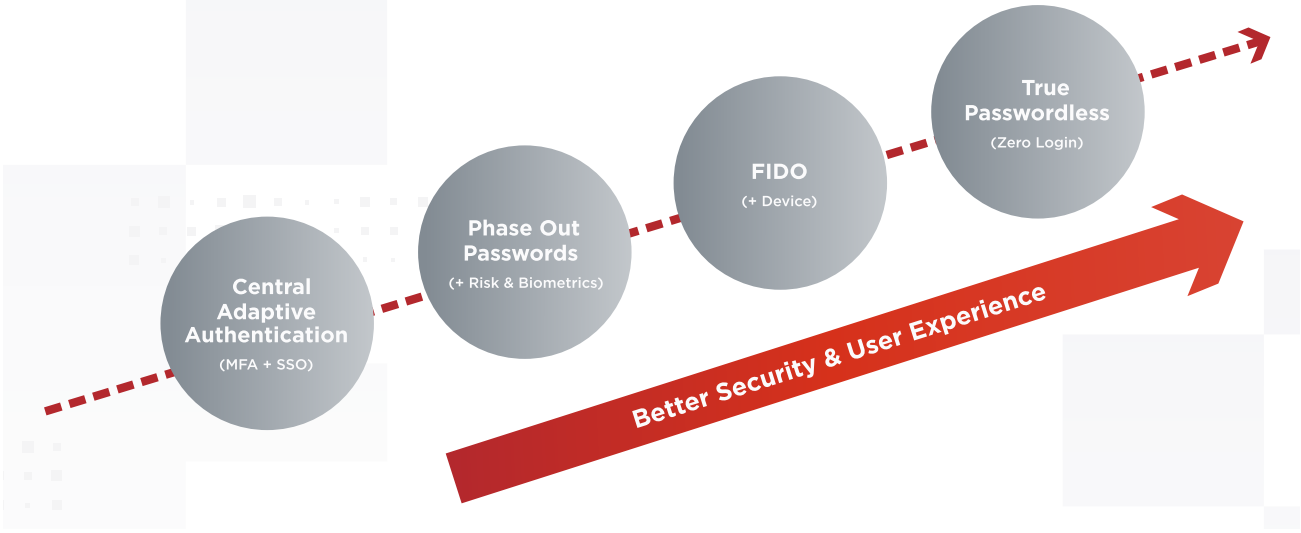
Authentication Methods: Pros & Cons

One-Time Passcodes	• Easy to Implement • Inexpensive	• Security Risks • Add Friction
Authenticator Apps	• Customizable • Strong Security	• Requires Enrollment • Add Friction
Biometrics	• Built-In to Device • User Friendly	• Expensive • Use-Case Specific
Security Keys	• Strong Security • FIDO	• Expensive • Add Friction

The Passwordless Journey

At Ping, we work with some of the largest enterprises in the world, who have the most complex passwordless use cases and goals. As a result, we've created the following journey, a phased approach for organizations to realize their passwordless visions. Of course, organizations can skip or reorder steps to address their specific applications, users and business needs.

Passwordless Maturity Scale



Phase 1: Central Adaptive Authentication

The first step on your passwordless journey is to centralize single sign-on (SSO) and multi-factor authentication (MFA) in order to centralize and standardize authentication for all of your applications. This will provide a consistent user experience and give you a convenient control plane for determining which applications your users can access. This phase comes in two subsequent flavors of use cases.

Extended Session

The first and most basic use case is "extended session". Users login with a username and password at predetermined time intervals as determined by an administrator—for example, once per day during the first week, once per week during the second week and then once per month, as long as they demonstrate normal usage and behavioral patterns. During extended sessions, users are only required to authenticate with a username plus MFA, thus offering a passwordless experience and only have to use full credentials sporadically.

This use case is similar to what users experience when loading their personal or work email accounts or websites such as Google or Amazon. This authentication scenario offers faster and more seamless experiences through fewer password prompts. After all, you are more likely to use a service if you don't constantly have to enter credentials.

Policy-Based Authentication With Risk Signals

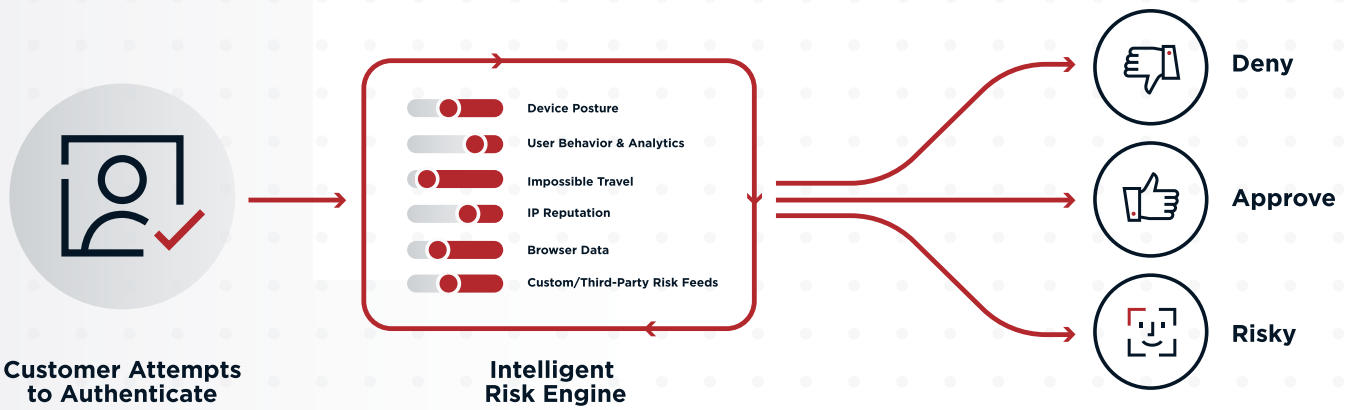
Also known as risk-based authentication, this scenario is policy-based and introduces risk signals to facilitate more flexible adaptive authentication to combat modern threats. With remote work growing, organizations face new challenges related to monitoring and securing their attack surface as users connect to the network from anywhere and on anything. Risk signals provide an effective way to move some of the authentication process into the background and make it invisible for the user.

Risk signals are a foundational piece of the passwordless puzzle. They are evaluated as customers and employees interact with an organization's online channels to enable more intelligent authentication decisions. As a result, users are only prompted for MFA when there is elevated risk or during a high-value transaction.

Multiple risk predictors can be used to establish baselines of normal user behavior and detect anomalies, thereby helping organizations make more intelligent risk decisions:

- **User behavior analytics:** Use machine learning to distinguish behavioral patterns of humans versus bots and illegitimate users.
- **Device profiling & reputation:** A method of acquiring device characteristics to determine any association with prior fraudulent activity.
- **Anonymous network detection:** Bad actors will commonly use VPNs, Tor and proxies to mask their actual IP addresses.
- **IP reputation:** Prevent users who emanate from malicious domains from accessing applications and services.
- **Impossible travel:** Prevent logins from locations the device could not have traveled to since its most recent login.

Risk-based authentication can be applied to both workforce and customer use cases. From a user experience perspective, if you have ever attempted to log into your mobile banking application while traveling abroad and had to perform a step-up authentication factor such as an OTP or a push notification, this was likely due to a risk score having been triggered. Risk-based authentication provides greater assurance that a user is who they say they are without introducing unnecessary friction.



Phase 2: Phase Out Passwords

Once you have those basic building blocks in place, you can begin to focus on replacing passwords with more robust and convenient authentication factors. The scenarios below require users to register with a password once initially. They can log into applications and services without passwords from then on. This phase has a wide range of use cases.

Username + MFA

The first step in this stage is to implement username plus MFA. A user fills out a username form without entering a password and is then prompted with an additional authentication factor from one of their known, trusted and pre-enrolled devices that the authentication authority has seen before. This second factor can be an application-based OTP, biometric scan or push notification, any of which will enhance both security and reduce friction by eliminating passwords from the authentication flow.

Email Magic Link

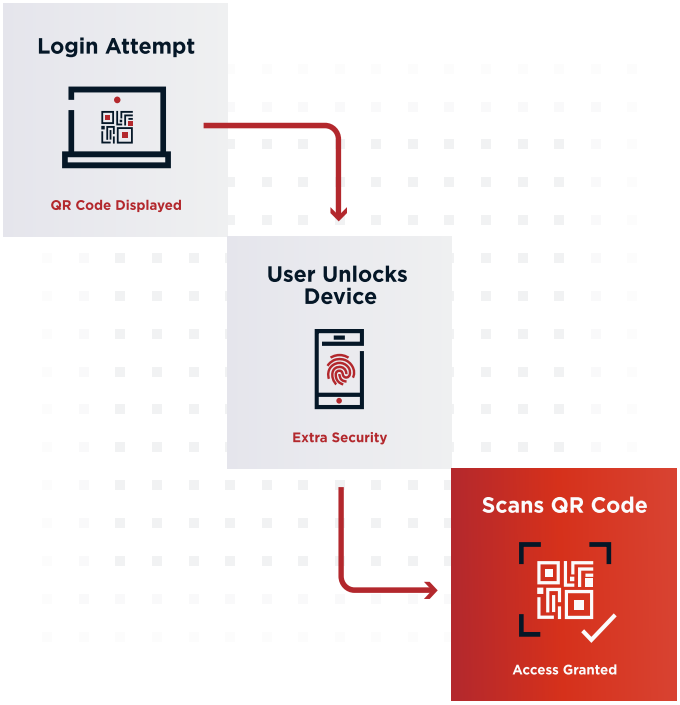
Another way to reduce password use is through email magic links. Users are prompted with a username form and then presented with a message that they have received an email with a link to the resource they want to access. Once the user clicks the link in their inbox, this completes the authentication flow and they are then granted access to the resource. This replaces "something you know" (a password) with "something you have" (an email address). As of now, it has not been widely adopted in workforce environments and is strictly a customer identity use case.

QR Codes

Also, strictly a customer use case, QR codes can save time and reduce frustration by leveraging users' smartphone cameras to facilitate fast and frictionless authentication across devices. QR code authentication is particularly useful when authenticating to publically accessible devices (like a kiosk) or devices with limited options for controls (like a TV). Authentication via QR codes is both username-less and passwordless and can be application-based or app-less:

Application-based QR codes

Application-based QR codes enable users to leverage their mobile devices as authenticators with minimal friction. Users can access customer applications on new devices by scanning QR codes directly from within the same providers' applications that they are already logged into on their smartphones.

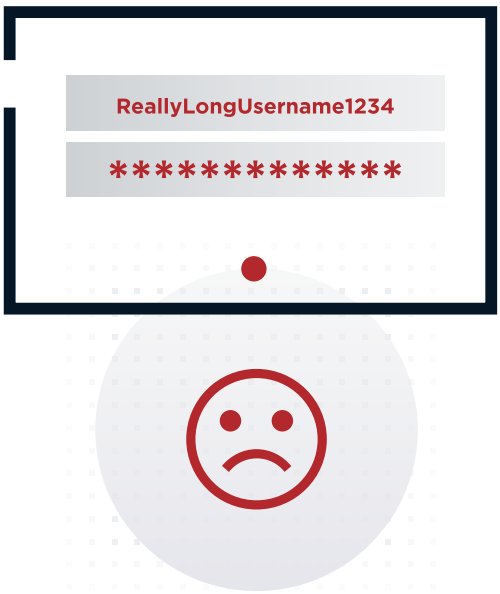


Take the following example: a user is already logged into their favorite streaming service on their smartphone and wants to access the same service on their new smart TV. Two login options appear: 1) Login with two sets of credentials or 2) Login with a QR code. Rather than going through the painstakingly frustrating process of clicking their TV remote to enter their username and password, they can instead simply scan the QR code on their TV screen from within the streaming service application that they are already logged into on their phone and presto! A usernameless and passwordless transfer of the users' login information is relayed from one device to another, instantly logging them in on their TV.

App-less QR codes

With app-less QR codes, the experience is similar but differs in that the user doesn't have to have an application installed on their phone. Rather they could navigate to the streaming service on a TV and scan a QR code on the TV screen directly from their phone camera to access the service via their phone's browser. For this to work, the user must have already enabled passwordless authentication on both their phone and with the streaming service.

Each of these use cases replaces "something you know" (passwords) with either "something you have" (a smartphone) and/or "something you are" (biometrics) to deliver a seamless login experience that completely bypasses any usernames or passwords. They also prevent the risk of a user falling victim to password replay attacks.



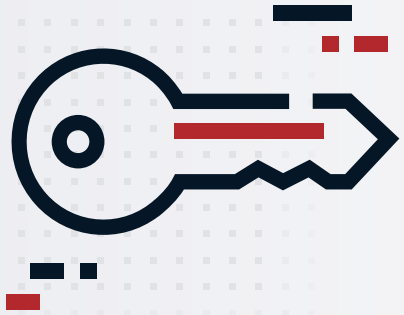
Phase 3: FIDO

The next step is to standardize FIDO (Fast Identity Online) wherever possible. FIDO is an open standard that is designed to protect user privacy and store biometric data on users' devices rather than on a server in the cloud. Biometric data never leaves the user's device, enabling them to authenticate locally without their data traversing the internet. FIDO authentication requires users to register their device's authenticator application with each website they want to authenticate with. The authenticator then generates a public/private key pair for each site and returns the public key.

Understanding the technological underpinnings of how FIDO works can be complicated. To briefly summarize its value, FIDO simplifies the management of passwordless environments for IT departments by removing the need for credentials to be shared by pairing devices with specific applications and websites. It is also the greatest defense against phishing attacks. This is because phishing attacks that are designed to steal credentials by routing users to fake websites are rendered obsolete since the attackers' bogus sites were never paired with the user's device.

By 2025, **more than 25%** of multifactor authentication (MFA) transactions using a token will be based on FIDO authentication protocols, up from less than 5% today.

Source: Gartner, "Take 3 Steps Toward Passwordless Authentication".

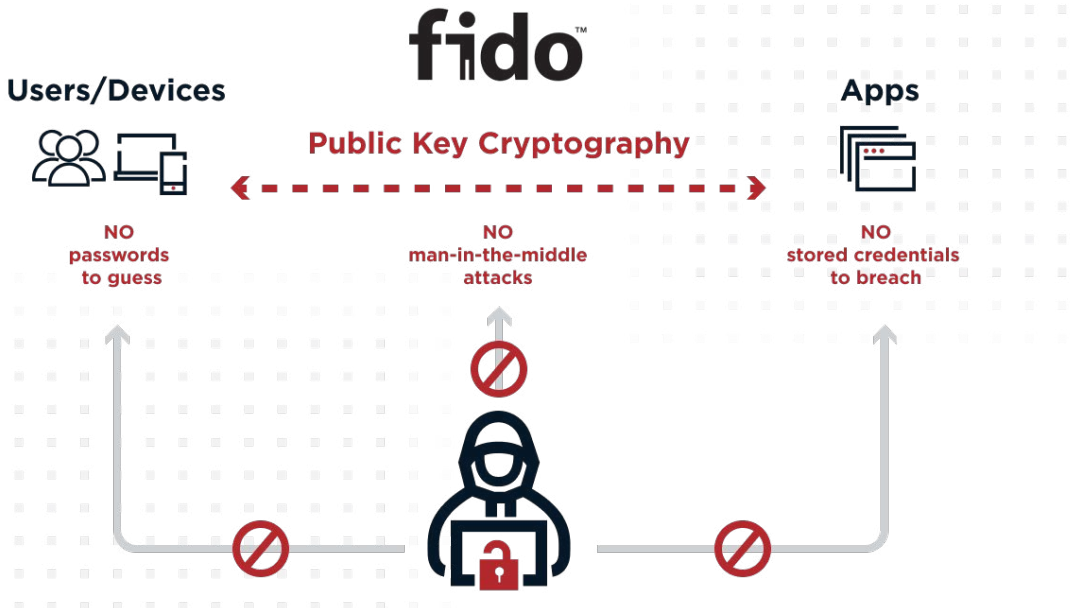


FIDO Security Keys

Also referred to as cross-platform authenticators, FIDO security keys are external hardware devices—like a YubiKey—that plug into a user's device via USB. Upon visiting a registered site, the user is prompted with a form button that wakes up any of the connected physical security keys. The user must then plug the key into their device and tap it to complete authentication.

FIDO Device (Platform)

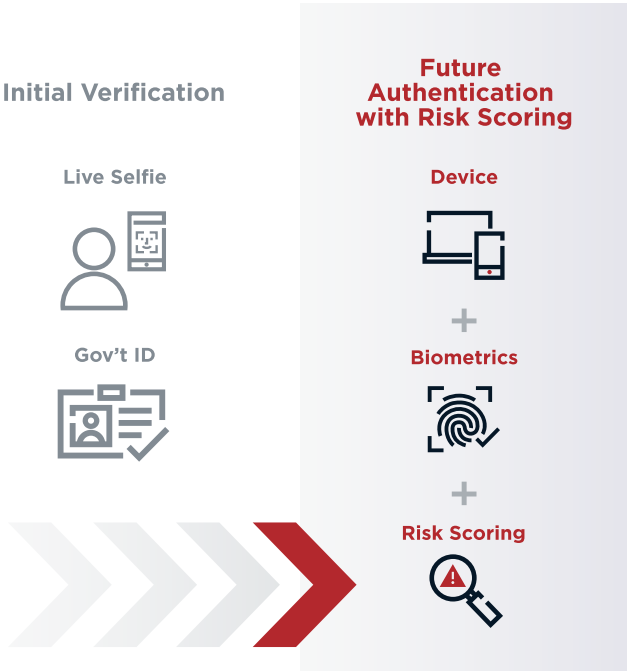
Platform authenticators contain an embedded cryptographic key tied to a single user device. Users attempting to gain access to the device or registered applications or sites on that device are prompted with a biometric factor such as a fingerprint or facial scan to complete authentication. Common FIDO compatible platform authenticators include Windows Hello, Apple FaceID and Android. These serve a variety of use cases such as web authentication, Windows and Mac login, and more.



FIDO replaces something you know (passwords) with something you possess (the FIDO security key).

Phase 4: Zero Login

Also referred to as “true passwordless,” zero login reflects scenarios in which no passwords exist. Zero login combines device enrollment with the passive collection of other contextual authentication signals to optimize both security and user experiences via minimal logins.
During initial registration, the user is verified without needing a password or username, for example, by taking a selfie and providing additional identity-supporting documentation, along with the traditional device pairing process. Then, future logins are done via the user’s trusted device with a passwordless medium like a QR code or a biometric scan to authenticate regularly.
Zero login also relies on risk signals to optimize security and convenience. Most of a user’s authentication is done in the background, and only when a risk score alarm fires do they have to perform a step-up authentication. Also, in the event of a user having lost their device and requiring an account recovery, a selfie could be used to expedite the recovery process.



An Example of Zero Login

A user can have a certificate for a private key like a digital wallet on their phone and also have bluetooth on. The user biometrically unlocks their phone with a face scan. Then, by leveraging bluetooth—as the user approaches a device that they would normally have to authenticate on to access, such as a laptop—it will automatically unlock. Under this scenario, when a user is within proximity of a resource that they have permission to use, they will be granted instant access.

To summarize the above example, a biometric scan of the user’s face unlocks the user’s phone, which in turn, unlocks the FIDO security key that is physically close to or embedded in a resource the user needs to access. This resource could be a laptop or—hypothetically—even a door to a building. This example reflects true “zero login”. After initial registration, users never have to login at all. Instead, the user’s phone leverages bluetooth to project their identity wherever they go. As a result, whenever a user is in physical proximity of the secured devices in question, the bluetooth from their phone recognizes the presence of their known and trusted device and immediately grants them access.

Zero login is by far the most mature passwordless scenario. As such, few if any organizations have implemented it.

Passwordless Journey Cheatsheet

Use the checkboxes below to determine where you are on the passwordless journey and help to map out your next steps.

Phase 1: Central Adaptive Authentication

- [ ] **Single Sign-On**
  Include social login and/or third-party IdPs (if applicable).
- [ ] **Add MFA Method/s**
  Try to provide multiple ways to authenticate, but prioritize adoption of more secure methods.
- [ ] **Implement Extended User Sessions**
  Require only MFA (no passwords) during extended sections.
- [ ] **Add Risk Signals**
  To continuously authenticate users via user behavior analytics, IP reputation, device profiling, anonymous network detection, impossible travel, and more.

Phase 2: Phase Out Passwords

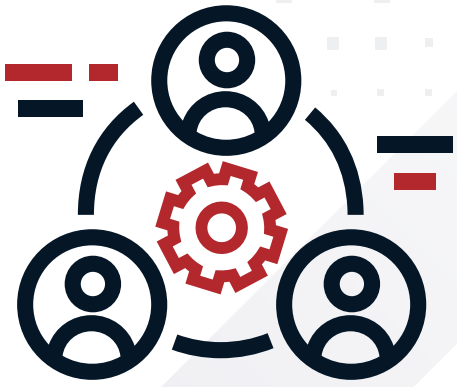
- [ ] **Username + MFA**
  Users fill out a username form without entering a password and are then prompted with an additional authentication factor such as an OTP, biometric scan or push notification.
- [ ] **Email Magic Link**
  Users fill out a username form and then receive an email with a link to the resource they want to access.
- [ ] **QR Codes**
  Strictly for customer use cases, QR codes enable a username-less and passwordless way for users to login to applications and services by scanning a QR code on another device on which they are already logged in.

Phase 3: Embrace FIDO

- [ ] **FIDO Security Keys**
  Users can connect a physical key such as a Yubikey to their device to allow for quick login with a tap.
- [ ] **FIDO Device (Platform) Authenticators**
  A cryptographic key is tied to a single user device to enable users to login to that device or registered applications and sites on that device via a biometric factor.

Phase 4: Zero Login

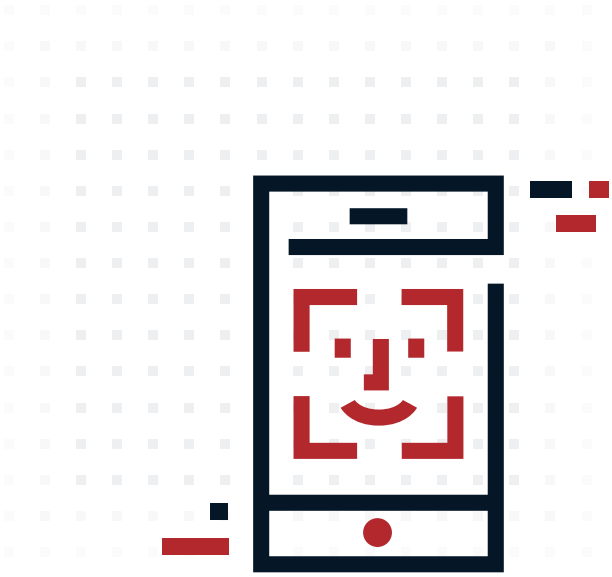
- [ ] **Eliminate Passwords Entirely**
  Users no longer ever need to use passwords or usernames to complete the initial registration process or for future logins through a combination of the above passwordless options



Passwordless Best Practices

Each organization has unique technology investments and user scenarios. There is no "one-size-fits-all approach" to passwordless. There are, however, common themes and best practices that organizations should adhere to. Best-in-class passwordless solutions should offer the following capabilities:

1. **Identity Verification (Identity Proofing):** Although eliminating the need for passwords offers a more secure way to authenticate, a common drawback is account recovery. Specifically, the challenge that arises when users lose the only device that their identity is paired to authenticate. Whereas many providers enable recovery solely via less secure mediums such as SMS OTPs, vendors that offer identity proofing as a capability can more quickly and securely enable account recovery through a selfie and/or other identity-supporting documentation.
2. **Central Adaptive Authentication:** Pairing MFA with SSO and risk signals offers more security through more adaptive authentication. With risk scoring continuously being done in the background, users experience minimal interruption. Step-up authentication is only triggered when absolutely necessary (i.e., when an alarm fires due to an increased risk score, an unusual policy violation, etc.).
3. **Hybrid Requirements:** A hybrid passwordless solution that offers both SaaS and traditional on-premises capabilities is more flexible, can accommodate hybrid environments and will better position organizations to scale over time than those that offer only on-premises.
4. **Coverage Across All Identities:** Identity types are diverse and can include employees, customers, partners and more. The same goes for use cases. For example, picture an organization with retail workers with different devices that might not be FIDO enabled, as well as corporate workers who need FIDO keys. Providers that can accommodate a diverse array of user and use case scenarios may be better suited to cover all of your organization's needs.
5. **Orchestration:** You need the ability to create different passwordless journeys across various applications and services. Orchestration allows you to easily create and optimize passwordless authentication flows in a no-code manner. Most importantly, it lets you test out the actual user experiences in quick succession.



Conclusion

Going passwordless is critical to ensuring that customers have secure, fast and frictionless digital experiences that drive engagement instead of frustration and abandonment. Likewise, going passwordless is also crucial to optimizing employee productivity, lowering password-reset related expenses and protecting your organization against a costly data breach. Thankfully, passwordless technology is currently readily available for mainstream adoption, but organizations will need to make it a strategic priority if they are serious about reducing security risk and improving customer and employee experience.

Choosing which passwordless authentication methods are best for your organization will vary based on your own unique user scenarios. Also, because passwordless use cases and requirements are so complex, organizations should strongly consider identity orchestration to implement it. Identity orchestration enables organizations to continuously iterate on the passwordless experiences that they deliver by testing different risk signals, authentication factors, and even MFA solutions from different providers.

The bottom line is that designing, testing, and optimizing the passwordless experiences that you want your users to have requires the ability to iterate quickly and test various options. Identity providers that empower you to continuously experiment with different passwordless flows through orchestration capabilities will deliver the fastest realization of time-to-value.

To learn more about best practices related to deploying passwordless in your organization, check out **Ping Identity's Passwordless Solution.**

Here at Ping, we offer a no-code, drag-and-drop identity orchestration platform that works across many different passwordless scenarios, incorporates different risk signals, and allows users to create flows with different identity vendors. To learn more about identity orchestration, check out **PingOne DaVinci.**

About IdentIT

Make It Happen with the Experts in Digital Identity

Going passwordless isn't just about technology — it's about enabling secure, seamless user experiences across every touchpoint. At IdentIT, we help organizations make passwordless a reality by designing and implementing future-proof authentication strategies powered by Ping Identity.

We don't just understand digital identity challenges — we solve them, from strategy to implementation and beyond.

At IdentIT, we specialize in end-to-end digital identity services designed to empower your business through every stage of your digital identity journey:

ADVISE

- Current State Audits & Architecture Reviews
- Business Case Development & Roadmap Design
- Vendor Selection & RFI/RFP Guidance

BUILD

- Tailored Architecture Design
- Seamless Implementation Of Digital Identity Solutions
- Knowledge Transfer & Team Enablement

RUN & EVOLVE

- 24/7 and 8/18 Support Services
- Proactive Monitoring & Optimization
- Continuous Improvement & Future-Proofing

We work with enterprises across sectors to deliver secure, scalable identity solutions. Our team combines deep technical knowledge with hands-on experience.

Ready to future-proof your digital identity strategy?

Let's turn your vision into action. Contact us and start building secure, scalable identity solutions that grow with your business.

www.identit.eu

identIT