ForgeRock®

7 Steps to Passwordless Authentication

Best practices and questions to ask IAM providers

Passwords have become an obstacle for enterprises and their users and customers. It's no secret passwords are a security risk, as they provide a huge attack surface for data breaches. Why? Because they are easy to guess and obtain, and humans make mistakes, including inadvertently exposing their passwords. But there's more than just security to think about. From forgotten passwords to complex requirements, passwords are a pain, causing customers to go elsewhere and employees to lose time. They lead to a decrease in workforce productivity due to account lockouts and an increase in call center and help-desk operational costs. In fact, Forrester estimates that the average large enterprise allocates more than $1 million annually to password-related support costs.[1]

By eliminating the need for users to interact with passwords, you can increase security and customer satisfaction. You can also reduce operational costs for your call center while boosting revenue by removing barriers that drive customers away. It's no wonder going passwordless is a top initiative for many organizations. However, getting there has proven to be difficult in the past, as the process has been riddled with confusion. Luckily, there are many ways to get to passwordless today, but there are also multiple factors to consider when planning for a passwordless implementation. How will you enable passwordless for customers accessing web services? Do you want to eliminate the use of passwords for your workforce? Can your legacy software and infrastructure support passwordless? How will you support users when they lose their devices or they have devices that aren't equipped for passwordless?

To help you map out a passwordless strategy, we've outlined key steps to consider and questions to ask identity access and management (IAM) providers to help ensure that your passwordless project succeeds.

1 Assess use cases, expected outcomes, and requirements

Assess your organization's business goals, user needs, security considerations, and requirements. You will likely gain organizational support if you're able to demonstrate the value of passwordless authentication with desired business outcomes. Examples of desired outcomes may include the need to increase customer adoption rates, improve customer journeys across channels, reduce fraud and security incidents, meet regulatory requirements, and lower costs associated with call centers. Aligning business outcomes with your use cases early on will also help answer how successful the project is.

Use cases include:

Enterprise authentication

Strengthen security and improve workforce experiences. Employees and partners can use biometrics, security keys, or other passwordless methods to access corporate networks, applications, and systems. These methods reduce the risk of password-related breaches and improve productivity by eliminating the need for password resets.

Mobile applications

Passwordless authentication is particularly useful for mobile applications, where convenience and security are critical. Most mobile devices have built-in biometric sensors, such as fingerprint or facial recognition, that can be used to authenticate. This makes it easy for users to access their apps without entering passwords and improves the overall user experience.

Consumer and citizen authentication

Provide a seamless and secure login experience. By using biometrics or one-time passcodes (OTPs), organizations can eliminate the need for users to remember and manage passwords when accessing online services, e-commerce platforms, or financial applications.

IoT devices

Many internet-of-things (IoT) devices are delivered with default passwords and basic security in place, making them vulnerable to unauthorized access and cyberattacks. Passwordless authentication can be applied to secure access to IoT devices by using device-based authentication, such as secure pairing or unique cryptographic keys. Organizations can ensure that only authorized individuals or devices are able to interact with IoT devices, minimizing the risk of unauthorized access or control.

Take inventory of all user repositories that maintain passwords, and determine the appropriate level of security, user experience goals, and compliance requirements. Some passwordless authentication methods, such as biometrics, rely on collecting and storing personal data. Address any privacy concerns and ensure compliance with applicable data protection regulations.

2 Develop an organizational migration strategy

Going passwordless doesn't happen overnight. Organizations can move to passwordless at a pace that is right for the business and its users. Develop a strategy that aligns with your organization's goals and timelines. Identify stakeholders, such as security, marketing, compliance, developers, and product teams, upfront. Choose authentication methods that suit your organization's needs and users by considering security, user experience, device compatibility, scalability, and available resources.

Passwordless implementations can vary, with strategies that include:

Passwordless as a second factor

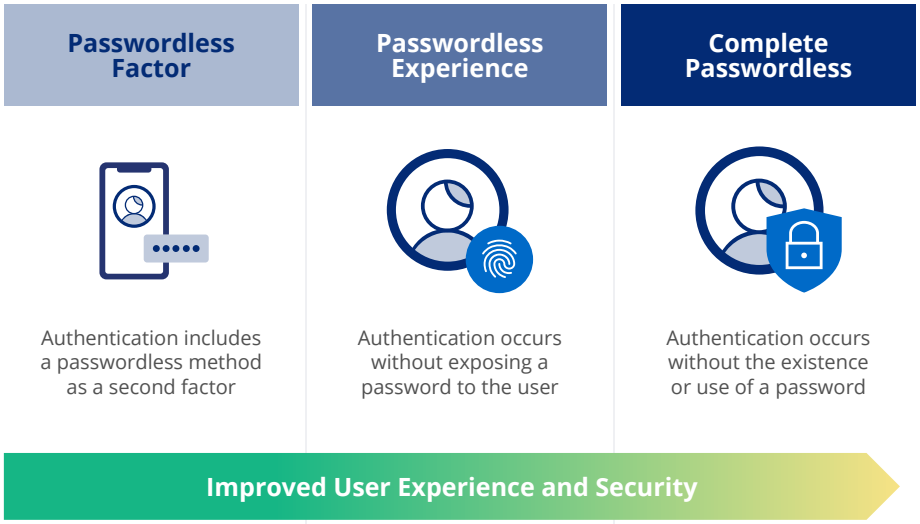
Passwordless authentication methods can be used as a second multi-factor authentication (MFA) factor, such as push notification, one time passcode (OTP), or emailed magic links. A passwordless factor is the most common offering of IAM vendors. It reduces friction and improves on the security of a standard login, but cannot be characterized as passwordless because it relies on usernames and passwords.

Passwordless experience

Provide a seamless and secure login experience. By using biometrics or one-time passcodes (OTPs), organizations can eliminate the need for users to remember and manage passwords when accessing online services, e-commerce platforms, or financial applications.

Complete passwordless

In this scenario, authentication occurs without the use of passwords. Instead, users can employ biometrics and private-key cryptography. Passkeys give users a simple and secure way to sign in without passwords by relying on Face ID or Touch ID. Since the user doesn't have a password — no password even exists — you eliminate all of its security risks and usability issues.



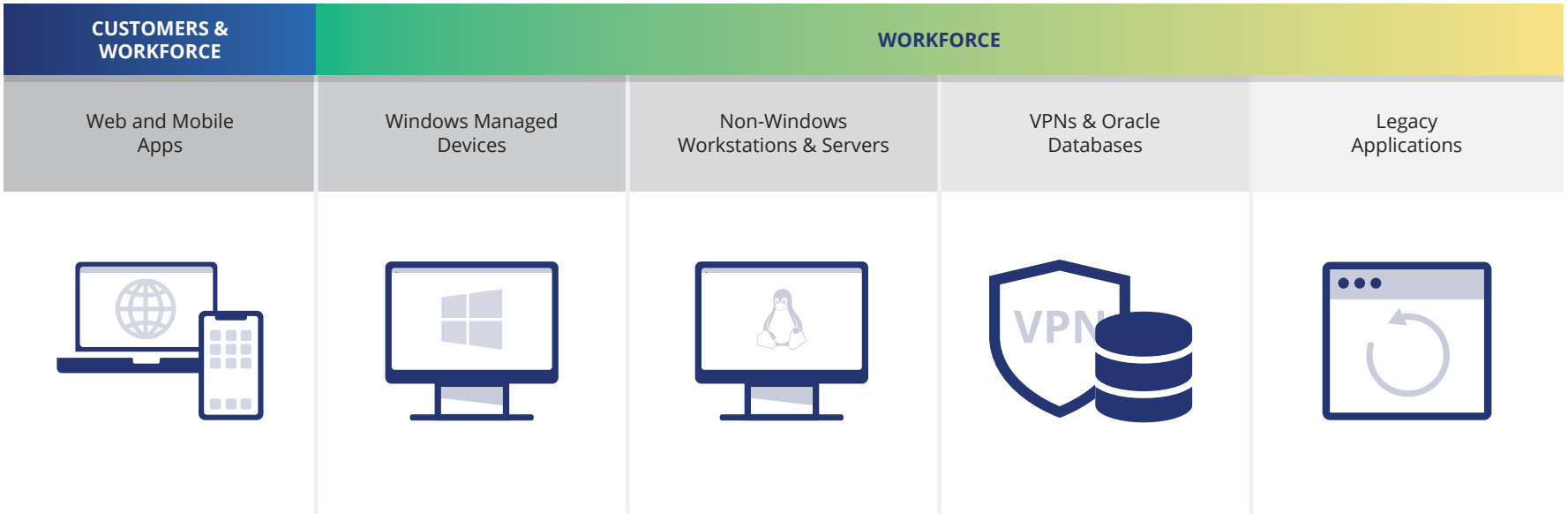
3

Identify integration requirements

Implementing passwordless authentication may involve integrating new systems, application programming interfaces (APIs), or protocols with existing infrastructure. This can be complex, requiring careful planning, development resources, and potential adjustments to ensure seamless integration. Identify and plan for integration requirements with existing systems, devices, applications, and infrastructure.

It is important at this stage to take a complete technological inventory in order to properly assess what integrations will be required to enable passwordless authentication throughout your organization. Standards like WebAuthn/FIDO2 help enable passwordless web-based applications and mobile devices. Other integrations that build on top of the FIDO2 standard or use stand-alone technology to achieve the “passwordless experience” may be needed for infrastructure and non-browser applications that are still being used in your organization.

Examples of enabling passwordless include web and mobile applications, legacy applications, Windows and Mac workstations and servers, RADIUS-based authentication, virtual and Windows Remote Desktop, desktop SSO, VPNs, databases, mainframes, LDAP, REST, Unix/Linux servers, and more. Ensure compatibility and seamless integration between your passwordless authentication solution, as well as your user management and access control systems. It’s important to choose a solution that works across all enterprise software as a service (SaaS), on-premises applications, and device logins, and that requires minimal custom coding and consulting fees.



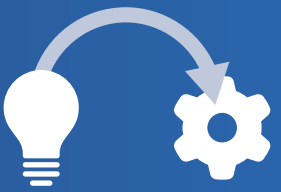
4 Plan for secure backup and recovery options

In the event of device loss or failure, users may need backup options to regain access to their accounts. Enterprises should provide alternative authentication methods or recovery mechanisms to prevent account lockout. Strengthen the recovery process for use cases where security is the primary consideration by leveraging contextual signals (location, device, suspicious IP, and more), and pinpoint verification processes to gain a high level of assurance about the identity of the user. Where possible, leverage orchestration and fraud management solutions as part of the authentication experience.

5 Develop an implementation plan

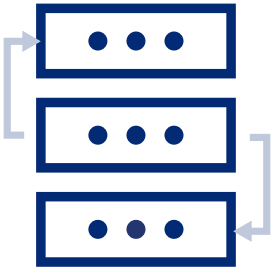
Develop an implementation plan, including timelines, resource allocation, communication strategies, and any necessary training or education for your workforce, customers, and administrators. Your organization can start with passwordless authentication methods (FIDO2 WebAuthn passkeys, OATH, push, OTP, biometrics, and QR codes) that complement your existing password-based MFA where it makes sense for specific browsers, applications, services, and risk levels.

You can also phase in passwordless as part of your employee onboarding and customer acquisition initiatives. To support this journey, it is highly recommended that you leverage standards such as SAML, OAuth, and OpenID Connect with secure single sign-on (SSO). SSO helps reduce the number of applications that need to be enabled, making the journey to passwordless easier.



6 Deploy passwordless in phases

A successful passwordless implementation will involve input from many parts of the organization. First, conduct a pilot test to evaluate the selected authentication methods in a controlled environment. Gather feedback from a subset of users, and assess the performance, usability, and security of the chosen methods. Then, implement passwordless authentication starting with a subset of users, authentication methods, and specific applications or systems. This phased approach allows for controlled deployment, monitoring, and adjustment based on user feedback and system performance.



It's important to communicate and educate users about the security benefits of passwordless authentication and the enhanced user experience they can expect, starting with clear instructions on how to use the new authentication methods. Lastly, do not disable existing methods until you've collected enough telemetry to identify any lingering issues.

7 Monitor performance and success

By continuously monitoring and evaluating the performance, user experience, and security of passwordless authentication journeys, you'll be in a better position to demonstrate how successful passwordless is for your organization. Conduct A/B orchestration journey testing to monitor the percentage of users who adopt passwordless, engagement rates, authentication success and fail rates, journey times, and risk levels. Collect feedback from users, and make adjustments to improve business outcomes. Lastly, it's important to stay up to date with emerging passwordless authentication technologies, open standards, and industry best practices for innovation. Regularly assess your authentication methods, and make improvements based on advancements and evolving security threats.

What was once a concept is now achievable. Aligning passwordless initiatives with business outcomes brings significant benefits to IAM leaders and organizations overall. From better security to reduced costs and increased revenues, the elimination of passwords should be a board-level priority for every organization in order to remain competitive in today's digital economy. Ready to get started? We've prepared a sample of the most important questions to ask IAM providers to help you along your journey.

Questions to ask IAM providers

Implementing passwordless authentication requires careful planning, user engagement, and ongoing innovation in alignment with standards. It's essential to strike a balance between security and usability, ensuring a seamless and secure authentication experience for all your users. Additionally, implementing passwordless authentication may involve upfront costs for hardware tokens, biometric sensors, or software licenses. Organizations need to ensure that the solution they choose can scale to accommodate a growing user base without compromising performance or security. Below are some sample questions you should consider asking identity access and management providers:

Solution functionality

1. Do you offer passwordless solutions that support the workforce, external consumers/citizens (CIAM), or both? Please explain how you would deploy a passwordless solution to each of those use cases.
2. What authentication methods does your solution support: biometrics, FIDO2, email magic links, or other?
3. How does your solution integrate with existing IAM systems?
4. Does your solution support MFA? If so, please explain how MFA is implemented.
5. Explain how your passwordless solution supports an organization with a Microsoft Windows Hello for Business (WHfB) desktop infrastructure. How does it differ?
6. How have organizations like mine deployed your solution and what challenges did they face?

Security and privacy

1. What security measures are in place to protect user identities and sensitive data?
2. How does your solution help ensure user data privacy and compliance with relevant regulations, such as GDPR and CCPA?
3. Describe your solution's encryption methods and key-management practices?
4. How does your solution support passkeys?
5. How does your solution integrate with fraud detection solutions? Does it have the ability to gather intelligence from external sources to help make real-time access decisions?
6. What alternative authentication methods or recovery mechanisms do you offer to prevent users from being locked out of their accounts?

Integration and scalability

1. What passwordless standards and protocols does your solution follow: FIDO2, WebAuthn, OATH, passkeys, or others? If none, please provide an explanation of how your solution deviates or adds to the standards and protocols and why.
2. How does your solution integrate into modern web applications and services?
3. How does your solution integrate with legacy on-premises applications and services like VPNs, databases, LDAP, servers? What about existing infrastructure such as Windows and Mac workstations and servers, remote desktop (virtual and Windows), desktop SSO, mainframes, and Unix/Linux servers?
4. Does your solution support passwordless capability for both SSO and MFA?
5. What is the scalability of your solution, especially in terms of handling a large number of users?
6. How does your solution secure applications running on premises and in the cloud?

Questions to ask IAM providers

User experience

1. What makes your solution easy for users to embrace?
2. How does your solution provide self-service options for users to manage their authentication preferences?
3. Explain the typical user registration process for both device enrollment and MFA selection.
4. How does your solution support emergency access for: lost or unavailable device, no network access, or kiosk mode, with many users accessing the same workstation?

Pricing and Support

1. How do you license and charge for users? Please provide detailed pricing information for your passwordless authentication solution, including any additional costs or licensing fees.
2. What level of ongoing maintenance and support do you provide for your passwordless authentication solution?
3. What is your service level agreement (SLA) regarding response times and issue resolution?
4. What training and documentation do you offer for administrators and end-users?

Go passwordless with ForgeRock

Move your users from password dependency to a passwordless experience or to complete passwordless authentication without having to rewrite your business applications and resources. With ForgeRock, you can move to passwordless at your own pace without it being an all-or-nothing experience. Find out how you can create a wide range of passwordless authentication user journeys using no-code orchestration based on the security and user experience needs of your business.

Start your passwordless planning today

Get a guided demo for **Passwordless at your Pace**.

Read the white paper: **Go Passwordless. Authenticate Securely.**

Watch the on-demand webinar: **How Your Organization Can Eliminate Passwords Faster.**

Contact us to discuss your passwordless journey.

[1] https://www.forrester.com/report/best-practices-selecting-deploying-and-managing-enterprise-password-managers/RES139333

About ForgeRock

ForgeRock® (NYSE: FORG) is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. For more information, visit: **www.forgerock.com**.

FOLLOW US

ForgeRock