The Passkey Playbook

A Practical Guide to Passwordless Authentication in Enterprises

fido ALLIANCE

EBOOK

Solving the Problem of Passwords

Passwords remain one of the most significant — and targeted — security vulnerabilities in modern enterprises. In the spring of 2025, **16 billion passwords were exposed** in a record-breaking data breach. Yet passwords are still the most common authentication method in businesses large and small.

Passkeys have emerged as a robust and widely accepted alternative, eliminating phishing risks while simplifying the user experience. No passwords to remember; no log-in details to compromise or steal. The challenge? Moving fast without introducing risk — or disruption — along the way.

In this playbook, we'll present a practical, phased approach for implementing enterprise passkeys. Rooted in business value, end-user experience and long-term risk reduction, it offers straightforward guidance for strengthening authentication and reducing organizational complexity.

What's a passkey?

A passkey is a credential that's based on **FIDO standards** and enables users to unlock a digital account not with passwords, but with a physical device — like a security key or smart card — or directly on your mobile phone, tablet, or computer. Each passkey can only be used for a single account; if you can prove that you own your passkey, you'll be able to access your account.

fido ALLIANCE

HID

1

Why: Overview of Phased Approach

The Importance of a Phased Approach

Transitioning to passkeys isn't about flipping a switch. It's about building the trust and the infrastructure to drive adoption in manageable stages. Embracing a phased approach to passkeys is more flexible, cost-efficient and user-friendly than the alternative — and, ultimately, it's faster. **Here's why.**

A phased approach enables organizations to:

Increase Flexibility

Passkeys aren't one-size-fits-all. A phased approach makes it easier to adopt solutions that best align with your existing environment, user and business needs and compliance mandates.

Boost Cost-Efficiency

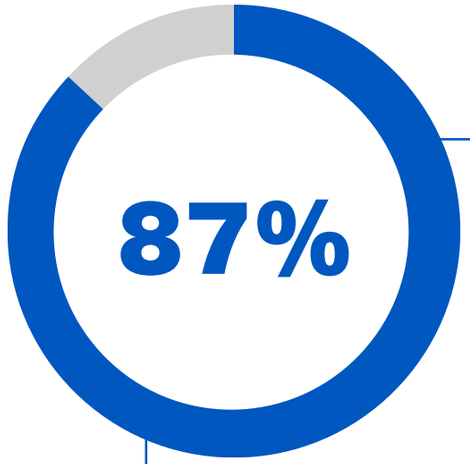
Going passwordless doesn't always require a huge, upfront hardware investment. A phased approach enables you to start with the infrastructure you already have, like ID badges, then build momentum with more targeted investments over time.

Minimize Business Disruption

Most people don't like passwords, but they may nonetheless be resistant to adopting a new approach. If you start small (users that are more sophisticated or features that are more important to protect), it will be easier to win them over to the advantages of the new method.

Speed Time-to-Value

Small steps can make a big difference when it comes to protecting your organization. Working one step at a time helps you iron out the kinks and improve the process as you move forward, rather than taking on a huge chunk all at once. And you'll be in good company.



*Compared to data from a 2022 FIDO Alliance survey

of surveyed organizations have successfully deployed or are deploying passkeys — a growth by 14 percentage points since 2022*

Source: The State of Passkey Deployment in the Enterprise survey, 2024

What: Understanding Passkey Options

2

Designing the Best Solution

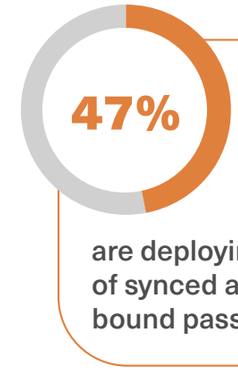
To customize a passkey plan that works for your organization, you'll need to understand what's possible. In this section, we'll assess the options — and review what other organizations are doing.

Passkeys can be stored and delivered in two primary ways, each with different security and usability trade-offs.

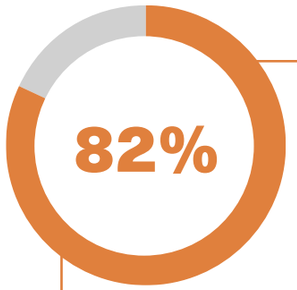
	Synced Passkeys	Device-Bound Passkeys
	Synced passkeys are stored in a cloud account (e.g., Apple iCloud, Google, or even a third-party Password Manager) and synced across multiple devices. This enables users to access one account on multiple devices without having to re-enroll each device.	Device-bound passkeys are stored locally on a specific device, such as a smart card, security key, or mobile device. They are not transferrable, so users must have the device that stores the passkey in order to access their account.
Best For	Mobile-first users, BYOD environments and customer-facing applications.	Regulated industries as well as workforce identity and high-assurance applications that require proof of possession as an authentication factor.
Risks	Synced passkeys can be shared (e.g., via AirDrop), threatening account integrity if they inadvertently fall into the wrong hands. Phishing a synced passkey is more difficult than cracking a password, but the risk, though small, is still real.	Device-bound passkeys require robust credential recovery planning in case users forget or lose their device. Many organizations enroll more than one key as a backup. Another option is selecting a passkey management solution that enables security teams to provision keys and remotely unlock devices and reset PINs.

According to our research, **device-bound passkeys are most popular** for enterprise settings — though nearly half of the 400 UK and US executives we surveyed with the FIDO Alliance are deploying a mix of synced and device-bound passkeys.

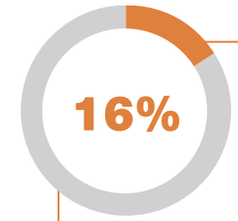
Surveyed companies reported implementing or considering a mix of device-bound and synced passkeys



are deploying a mix of synced and device bound passkeys



are deploying device-bound passkeys



are deploying synced passkeys only

Source: The State of Passkey Deployment in the Enterprise survey, 2024

HID

Understanding Where Passkeys Fit

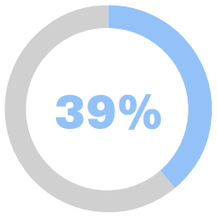
Passkeys reframe both how users authenticate and how security teams manage identity recovery — requiring new playbooks for troubleshooting and support.

That's why successful deployments typically begin with:

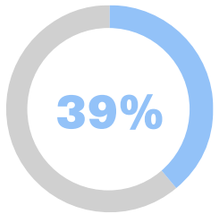
- Technically proficient users like IT administrators and engineers — providing IT staff with the insight and education required to help end users
- High-risk roles in finance, HR and compliance — ensuring the quickest wins from a security perspective
- Existing smart card or MFA users — who are already used to the experience of using a high security credential

Only **21% of enterprises deploying passkeys** roll them out to the entire organization at once. Instead, most prioritize departments or workflows with access to sensitive data and applications.

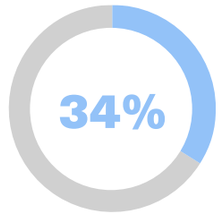
Organizations are prioritizing specific users groups for passkeys, with the top three cited user groups being:



those requiring access to IP



users with admin accounts



users at the executive level

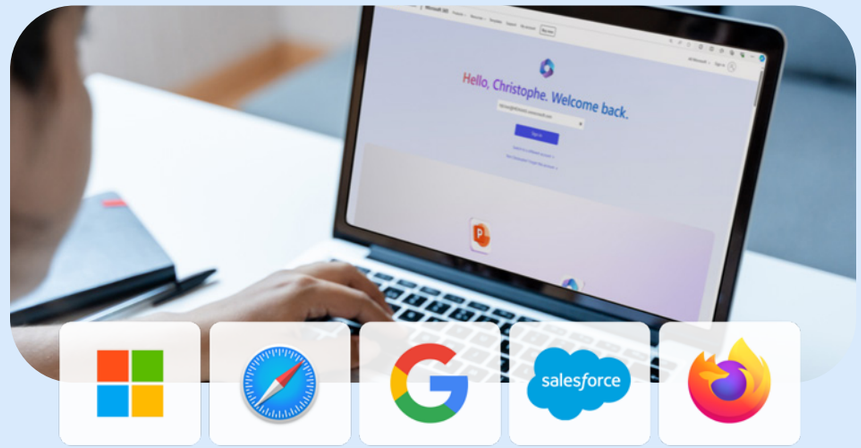
*Only 21% said they are targeting all of the users in their organization.

Source: The State of Passkey Deployment in the Enterprise survey, 2024

Compatibility is no longer a barrier. Passkeys are already supported across:

- Microsoft 365 and Microsoft Entra ID
- Google Workspace and Chrome
- All major web browsers — including Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari — support FIDO authentication standards
- Salesforce, Dropbox, Box, Zoom and other major Software-as-a-Service (SaaS) platforms

This broad ecosystem support simplifies staged deployment — starting small and expanding strategically.



How: The Phased Approach, Step by Step

3

Planning Your Passkey Rollout

Successful passkey deployments often start with existing infrastructure, then scale and evolve with time. The most capable solutions integrate seamlessly with identity platforms like Microsoft Entra, Google Workspace, Ping Identity, Okta and others. This makes it easy for organizations to tailor authentication journeys that fit each situation.

The goal is not to find a technology that fits all needs and use cases. It's to build an adaptable authentication strategy that aligns with your users, infrastructure and regulatory obligations — at a pace that works for your business.

We've broken down the process into three distinct steps: start, scale and standardize. Let's tackle each in turn.

1. Start: Use What You Have

The first step is finding solutions that increase security now while building momentum for the future. Many business environments support strong authentication with minimal disruption. To identify the best place to start, ask yourself:

- Which user groups are ready for change?
- What devices and systems already support FIDO2 or passkey login?
- Where can we get a quick win with minimal friction?

This is your pilot phase, designed to validate assumptions, capture feedback and demonstrate value early. What it looks like will depend on your specific needs and goals, but examples might include:

Reusing Physical Access Cards

Many times, phishing-resistant authentication (that is, cryptographic key pairs) can be configured on the ID badges that are used for physical access — a move top solutions support without additional hardware upgrades. This reduces friction by enabling employees to authenticate securely using a form factor they are already comfortable with. Once users have adjusted to the transition, these cards can be replaced with FIDO2-certified cards or keys that support passkey technology.

Starting With Sophisticated Users

Most organizations that are deploying enterprise passkeys have prioritized specific user groups. Departments that are already familiar with MFA or security keys are an excellent place to start, because they'll have an easier time with the transition.

Prioritizing Critical Infrastructure

Business-critical applications like email, desktop login, Microsoft Office 365, Salesforce, and HR systems are ideal candidates for passkey authentication. That's not just because they already support the technology, but because they offer a portal to some of the highest-value data in your business — information that, if compromised, could cost you millions of dollars.

2. Scale: Expand With Strategy and Feedback

Once your pilot goals are achieved, you can scale your deployment to include more users and applications. Many organizations use a hybrid approach in this phase — deploying synced passkeys for convenience and device-bound passkeys where higher assurance is required.

Focus on broadening usage, formalizing workflows and improving support while addressing key areas like:

Expanding Access

Create plans for addressing other groups of internal users who are ready for passkey authentication, prioritizing critical workflows and access to sensitive data.

Addressing Device Readiness

The solution that's right for one user group may not be best for the others. Platform authenticators like biometrics might work for one user group, for instance, while those who access high-security applications will be safer with device-bound credentials.

Driving Adoption

Successful passkey deployment requires effective change management strategies. Drive adoption with targeted onboarding and user awareness campaigns along with clear messages about what's behind the change — then keep in touch to solicit feedback and answer questions.

Improving Support

Even sophisticated users can struggle with a new workflow. Monitor helpdesk trends and feedback to identify areas that need to be tweaked or improved as you expand to new user groups.

3. Standardize: Operationalize and Enforce

Once successful adoption is underway, it's time to standardize authentication policies across the organization. How well does authentication align with your broader security posture? What steps might decrease the risk posed by legacy systems?

Steps to consider include:

Enforcing Passkey Usage

As adoption grows, you can start applyingtechniques like conditional access, where you can enforce passkey use for specific roles, devices or risk scenarios.

Decommissioning Passwords

Eventually, you can decommission passwords and one-time codes — and, in areas where that's not feasible, implement additional security controls like threat detection and enhanced monitoring to mitigate potential risks.

Expanding Access

Continue expanding coverage to new business units, cloud applications and device types.

Streamlining FIDO Management

Establish lifecycle and recovery processes for FIDO management. IT administrators often choose to enroll more than one key as a backup for device-bound passkey users. Enterprise Passkey Management solutions make things even easier by enabling security teams to create and register passkey credentials remotely, and unlock the device is case the PIN is forgotten, increasing visibility and decreasing help desk tickets.

Implementing Procurement Strategy

IT Security Departments should work with procurement to ensure future IT investments support the organization's passwordless strategy. Ideally, all IT software should be compatible with the organization's IDP (or relying party); if not, applications should be FIDO compliant and able to use users' FIDO authenticators.

At this point, passkeys will become the default authentication method, rather than an exception — and will be fully integrated into the enterprise's security model.

4

Return On Investment (ROI)

The ROI of Passkeys

Sometimes, it's hard to quantify the value of security investments until your organization experiences — or is able to deter — a data breach. That's not the case with passkeys, which generate measurable benefits across security, operations and user experience. In fact, 77% of organizations that implemented passkeys said the technology has reduced helpdesk calls.

Implementing passkeys enables organizations to:

- **Streamline IT Operations**
  Reduce costly password reset requests, support tickets and lockout incidents.
- **Boost Security**
  Eliminate password reuse and decrease the risk of phishing attacks.
- **Improve the User Experience**
  Power faster and more consistent log-ins across devices.
- **Align With Industry Regulations**
  Comply with mandates and requirements for phishing-resistant MFA like NIST, NIS2 and CISA.

Calculate Your Savings With Passkeys

When it comes to phishing, the question isn't if, but when you'll be attacked. Passkeys mitigate this risk and spare you the substantial expense of repair and recovery.

Calculate your savings

HID

How HID Helps You Succeed

5

HID

How HID Helps You Succeed

HID provides the industry's most complete passkey toolkit — from phishing-resistant credentials and management at scale to native identity integrations and global support. Whether you're starting with a pilot or expanding globally, we'll help you reduce complexity and accelerate success.

HID provides everything you need to power secure, efficient passkey adoption, including:

- **FIDO Authenticators**
  Maximize productivity and minimize downtime with passkey-enabled smart cards and security keys that enable users to access both physical and digital resources.
- **Synced Passkey Support**
  Give users the flexibility to access their accounts with both synchronized and device-bound passkeys.
- **Support for Platform Authenticators**
  Power a faster and more personalized authentication experience with credentials that support Windows Hello and Face ID — and enable users to log in with biometric data.
- **Expert Deployment Support**
  Accelerate time-to-value with the help of our expert Professional Services team, which reduces complexity through practice-driven design and deployment workshops — and drives long-term success with ongoing support and optimization.
- **Enterprise Passkey Management**
  Rolling out passkeys isn't just about issuing secure devices — it's about managing them with the same precision as the rest of your identity stack. With a single point of registration and management, and more — HID's Enterprise Passkey Management solution gives security teams **full visibility and lifecycle control** across the entire enterprise passkey footprint, hardware and software alike.

Member of
Microsoft Intelligent Security Association

Microsoft Security

Conclusion

Authenticate With Confidence

The move to passkeys is no longer theoretical — in fact, **87% of businesses** we surveyed with the FIDO Alliance either have deployed or are deploying passkeys. Yet as the consequences of phishing attacks continue to rise, the organizations that succeed aren't the ones that leap the furthest. They're the ones who move intentionally.

HID can help you build an effective, phased passkey roadmap that improves security, boosts productivity and simplifies compliance — without disrupting your workflow.

Start where you are.
Scale where it makes sense.
Standardize when you're ready.

Find Your Path to Passkeys:

- Try a free sample
- Calculate your ROI
- Learn more about FIDO Authentication with FIDO Alliance

HID

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171-1108

For more global phone numbers click here

2025-08-05-iams-the-passkey-playbook-eb-en

Part of ASSA ABLOY