RESOURCE CENTER

# Passkey vs password: What's the difference?

Get the full interactive view at https://bitwarden.com/ja-jp/resources/passkey-vs-password-whats-the-difference/

bitwarden

## Overview

Most professionals manage various accounts, from banking to social media, shopping, and everything in between. Modern password managers have made maintaining strong, unique credentials for every account both secure and convenient. As technology evolves, so do authentication methods. Enter: passkeys.

Enterprises may manage thousands of credentials used by global teams on a daily basis. When businesses need high-confidence authentication while maintaining efficient, secure collaboration, understanding both options helps inform the best choice for their specific needs.

Both passwords and passkeys have their strengths when users leverage strong and unique credentials for every account. While passkeys offer certain advantages through their cryptographic architecture, passwords managed through reliable password managers remain a trusted and secure authentication method. Passkeys have some bonus inherent security features, such as resistance to phishing and brute-force attacks.

This comparison explores both authentication approaches, examining their features, implementation considerations, and implications for enterprise security, helping decision-makers understand the available options.

## What are passkeys?

Passkeys use public key cryptography, asymmetric encryption, and biometric verification to provide a more secure authentication method than traditional passwords. Unlike passwords (which need to be remembered), passkeys are cryptographic key pairs where the private key remains securely stored on the user's device and the public key is stored on the service's server. Authentication happens when the device proves possession of the private key. No shared secret is transmitted across the internet during login.

From a user's perspective, logging in with a passkey typically means using the device's built-in authentication method, such as a fingerprint, face scan, or PIN. This creates both a simpler user experience and stronger security.

**Read more:**
Living the passwordless life with Bitwarden biometrics

## The essential difference: Passwords vs passkeys

Both passwords and passkeys serve as authentication methods, each with distinct characteristics.

- Passwords, when properly managed with a password manager, provide secure authentication based on something you know. Password managers eliminate the need to remember complex passwords while ensuring users have strong, unique credentials for each account.
- Passkeys are phishing-resistant and offer built-in multifactor authentication. They use cryptographic key pairs where only the user's device holds the private key. Authentication occurs by proving possession of this key, often using a fingerprint or facial recognition.

A password and passkey manager transforms both security and the user experience, eliminating the need to remember complex passwords while significantly reducing vulnerability to common attacks.

## Direct comparison: Passwords vs passkeys

| Feature | Traditional passwords with a password manager | Passkeys |
|---|---|---|

| | | |
|---|---|---|
| **Authentication basis** | Something you know (memorized secret) | Something you have (device) + Something you are (biometrics) |
| **Security model** | Encrypted password storage | Public/private key cryptography |
| **Vulnerability to phishing** | Dependent on each user's vigilance and adherence to best practices | Very low |
| **Vulnerability to data breaches** | Dependent on each user's vigilance and adherence to best practices | Very low |
| **Need for memorization** | No, as long as the user has a password manager | No |
| **Typical user verification** | Type characters or autofill | Fingerprint, face scan, or device PIN |
| **Cross-device usage** | Requires sync or re-entry | Requires initial setup per device |
| **MFA requirement** | A separate step is needed for authentication | Two-factor authentication is built in by design |
| **Password fatigue** | Low, when using a password manager | None |
| **IT support burden** | Moderate, when managed centrally | Low |

## Current adoption status

Passkeys aren't just theoretical—they're already here. Over 95% of iOS and Android devices are passkey-ready, and more than 90% of all iOS and Android devices have passkey functionality enabled. Passkeys have been used over 1 billion times across 400 million accounts. Major platforms, including Google, Apple, Microsoft, and the FIDO Alliance, have standardized passkey implementation. Many popular services, including Google, PayPal, eBay, and Best Buy, now support passkey authentication.

Given the widespread use of mobile devices as a primary means of web interaction, passkeys are already viable for mass adoption. It is important to use a supported browser to ensure compatibility with passkeys.

## The day-to-day user experience with passkeys

Whether a team uses a password manager or passkeys, both methods offer a streamlined user experience and enhanced security. For those using passwords without a password manager, switching to passkeys brings several noticeable daily changes.

| User experience | Traditional passwords without a password manager | With passkeys |
|---|---|---|
| **Password generation** | Users struggle to remember dozens of complex passwords, creating a poor user experience | Users simply use their fingerprint, face, or device PIN to authenticate |
| **Login process** | Users type or copy/paste a long string of characters, often making errors | Users receive a prompt to authenticate with biometrics—just one touch or glance |
| **Anxiety** | Users worry about creating strong enough passwords or forgetting their credentials | The system handles security without requiring users to create or remember anything |
| **Authentication** | Average login time is 12-15 seconds when typing manually | Login typically takes 2-3 seconds using biometrics |
| **Password resets** | The average user resets 3-4 passwords monthly due to forgetting them | Since nothing needs to be remembered, password resets become virtually extinct |
| **Cross-device experience** | Users must either sync passwords across devices or remember them for each device | After initial device setup, authentication flows smoothly between authorized devices |
| **Account recovery changes** | Users typically receive a reset link via email or SMS | Recovery typically uses alternate devices, backup codes, or account recovery services |
| **Phishing resistance** | Users must vigilantly check website URLs to avoid entering credentials on fake sites | Phishing protection is built in as passkeys are linked to specific domains |

## Implementation considerations

When evaluating a password and passkey manager, organizations need to consider a variety of factors.

**Scalability**

**With passkeys**

Check out this

passkeys FAQ.

Organizations should deploy a centralized identity management system that supports FIDO2 standards. Gradually roll out this system to high-value applications, while establishing clear key management protocols and recovery procedures for lost devices. Scaling can be limited by the need for specialized hardware in some implementations, incompatibility with legacy systems that don't support the FIDO2 standard, and challenges with account recovery when users lose access to their authenticated devices.

**With a password manager**

Organizations should use a comprehensive deployment strategy that includes centralized administration tools, single sign-on integration, and automated user provisioning, along with consistent training programs, to ensure proper adoption across departments. Scaling limitations include managing the administrative overhead for large user bases, addressing integration challenges with diverse tech stacks, and navigating the user adoption hurdle as employees must adapt to new workflows and security practices.

**Multifactor authentication**

By design, passkeys have MFA built in by requiring both a private key and optional biometric verification for access, which reduces phishing risks. Implementing passkey authentication at scale requires adherence to key management best practices for secure distribution, storage, and revocation of private keys.

Organizations can integrate a password manager with additional verification methods, such as time-based one-time passwords (TOTP), hardware security keys, or biometric authentication.

**Backward compatibility**

Systems need to support both password and passkey authentication methods for users at different stages of adoption.

**Vendor considerations**

Organizations should evaluate potential vendor lock-in concerns and ensure that the chosen password and passkey solutions follow open standards to maintain flexibility.

**User education**

The biggest hurdle for most new users is understanding how password managers and passkeys work. Planning for proper training and gradual rollout is essential.

**Regulatory compliance**

All passkey-based authentication systems must comply with relevant regulations, such as GDPR, HIPAA/HITECH Act, and PCI-DSS standards.

Password managers must meet specific requirements including end-to-end encryption of stored credentials, comprehensive access controls with role-based permissions, detailed audit logging capabilities for all credential access events, secure sharing protocols that maintain the principle of least privilege, and certification for relevant standards such as SOC 2, ISO 27001, GDPR, HIPAA, and CCPA depending on industry and jurisdiction.

## Enterprise security and compliance

**Which is safer to use: passwords or passkeys?**

The short answer: As long as a robust password manager is in place, both passwords and passkeys can meet enterprise security

requirements.

Security and regulatory compliance concern technology leaders for several reasons:

- **Reputation risk:** Security breaches and compliance failures damage consumer trust and affect the bottom line.
- **Regulatory penalties**: Non-compliance can result in fines, penalties, and legal action.
- **Liability concerns**: Companies may be held liable for security breaches resulting from non-compliance.
- **Complex data protection laws:** Regulations like GDPR, CCPA, and HIPAA/HITECH require robust security measures.
- **Compliance fatigue**: Managing compliance across different jurisdictions is a challenge for many organizations.
- **Supply chain risks:** Companies must ensure that suppliers and partners also maintain compliance.
- **Global presence challenges**: Companies operating globally face unique security and compliance challenges due to varying regional regulations.

#### Passkey security features

Passkeys utilize modern cryptography to meet the high security standards expected by enterprises, regulatory bodies, and end users alike.

Passkeys utilize encrypted data to enhance security, ensuring that access is safeguarded through public key cryptography and unique keys. By adopting passkeys, organizations can achieve compliance without complicating user workflows while significantly reducing the likelihood of account compromise.

**Advanced cryptography** includes keyless encryption, public-key infrastructure, quantum-resistant cryptography, high-strength key exchange protocols, secure authentication methods, and secure key storage and management.

**Protection against common attacks**: Passkeys provide built-in protection from phishing, password cracking, and compromise attempts.

**Compliance with standards:** This includes the FIDO standards like FIDO2– a widely adopted standard for secure authentication and biometric verification, the USSDAI – an international standard for secure storage devices, and ISO 29115 – a global standard for software security testing and validation.

#### Password manager security features

**End-to-end encryption** ensures that passwords are encrypted on the device before being transmitted and remain encrypted until the user accesses them on an authorized device, preventing anyone, including the password manager provider, from seeing the unencrypted data.

**Multi-factor authentication support** adds an extra layer of security by requiring something you know (password) plus something you have (like a mobile device) or something you are (biometric data) before granting access to the password vault.

**Centralized administration** allows IT teams to manage password policies, user access, and security controls across an entire organization from a single dashboard.

**Compliance with industry standards** demonstrates that a password manager adheres to established security frameworks like SOC 2, ISO 27001, or GDPR, ensuring it follows recognized best practices for protecting sensitive data.

**Audit trails and reporting** provide detailed logs of who accessed what passwords and when, enabling security teams to monitor for suspicious activities and maintain accountability.

## Cost and maintenance comparison

### The financial impact of unmanaged credentials

For a medium-sized enterprise with 5,000 employees, password-related costs can exceed $1 million annually.

- **IT support**: The average cost per password reset is $70, with help desk staff spending 30-50% of their time on password-related issues. Weak passwords further exacerbate these costs by making accounts more vulnerable to compromise, necessitating additional support and security measures.
- **Lost productivity**: Employees lose 20-30 minutes per password reset incident. Large organizations spend an average of $5.2 million per year on password resets. Password-related inquiries comprise 20-50% of all help desk calls.
- **Security paradox**: Increased security measures often lead to decreased actual security, as complex password requirements result in predictable patterns that are easier for attackers to guess. A recent Bitwarden survey showed that 38% of users change their password completely when prompted to make an update; the other 62% only change it by a few characters or a single character, or reuse an existing password.

### Potential savings with passkeys

Where possible, transitioning from passwords to passkeys can lead to significant cost savings and security improvements:

- **Reduced operational costs** include up to 90% savings on SMS-related expenses for authentication, drastically reduced need for password resets and related IT support, and simplified account recovery processes.
- **Enhanced security benefits** include protection against phishing attacks, eliminating vulnerabilities from password reuse, and a reduced risk of large-scale data breaches, since passkeys are not stored in centralized databases. However, the need for strong passwords persists on platforms that do not yet support passkeys. Using strong passwords with a password manager can help maintain security.
- **An improved user experience** means that authentication via biometric sensors or PINs eliminates the need to remember complex passwords, which provides seamless authentication across devices without requiring re-enrollment and reduced account abandonment rates.
- **Long-term benefits** include single-step multifactor authentication without the complexity of passwords and OTP, as well as consistent security across all enterprise applications and services.

## Integration with existing systems

The ability to integrate with existing tech stacks plays a crucial role in the seamless transition for large-scale businesses. Platforms like Bitwarden Password Manager facilitate the integration of passkeys, which enhances security and simplifies user access to accounts.

Explore identity provider integrations with Bitwarden such as Okta and Azure AD.

### Passkey integration capabilities

Passkeys leverage existing identity provider infrastructure while potentially reducing administrative burdens related to password resets and credential management. Identity providers like Okta, Google Workspace, and Azure AD can issue passkeys for single sign-on experiences across multiple applications, often incorporating biometric verification as part of the authentication flow.

The technology supports unique capabilities such as shared device access through one-time QR code scanning without storing sensitive credentials, though it requires compatible browsers and platforms. As an emerging technology with growing support, passkeys offer the potential for a simplified long-term authentication architecture while maintaining strong security guarantees.

### Password manager integration capabilities

Password managers integrate with identity systems using protocols like SAML, OAuth 2.0, and OIDC to facilitate single sign-on experiences, while browser extensions and mobile applications provide auto-fill capabilities across websites and applications. They also support the enforcement of password policies and complexity requirements while providing comprehensive audit trails for compliance purposes. Password managers implement robust encryption and can integrate with multi-factor authentication systems to create defense-in-depth security architectures suitable for enterprise environments.

## Implementation planning

When planning to roll out a password and passkey manager, organizations should:

- **Assess current infrastructure** to evaluate existing authentication systems and identify integration requirements.
- **Phase the rollout** by considering implementing passkeys for specific applications or user groups first.
- **Verify service compatibility** by checking which applications and services in the ecosystem support passkeys.
- **Plan a transition strategy** to prepare for a period where both passwords and passkeys are supported.
- **Determine an onboarding and education plan** to improve adoption.

**Read more:**

How to foster user adoption for your new company password manager

### User experience and adoption

Ultimately, success depends on user adoption. When addressing potential hesitation from customers, clients, or employees, emphasize the ease and convenience of making passkeys and using a password manager. Users can log in without needing to remember complex passwords or reset credentials, thus enhancing the overall user experience and boosting security.

### Benefits to communicate

1. **Simplified login experience**: Eliminate the need to remember complex passwords or constantly reset forgotten ones.
2. **Enhanced productivity**: No more time lost to password resets or login difficulties.
3. **Reduced frustration**: Employees no longer need to remember passwords.
4. **Improved security**: Passkeys are phishing-resistant and enhance safety in the event of a data breach, and password managers signal to users they may be on a suspicious website by not autofilling credentials on lookalike sites.

### Implementation guidance by organization size

**For small businesses**

- Begin with password management rollout and utilize built-in passkey support from major identity providers. Ensure that your web browsers are compatible with passkey technology and have team members install the password manager extension to facilitate seamless integration and enhance security.

- Prioritize customer-facing and high-value applications for initial implementation.
- Leverage managed passkey solutions to minimize technical overhead.

**For mid-size organizations**

- Develop a phased implementation plan starting with high-value applications.
- Establish clear key management protocols and responsibility assignments.
- Invest in user training and support resources.

**For enterprise organizations**

- Create a comprehensive passkey governance structure.
- Implement a robust key management infrastructure with appropriate redundancy and recovery strategies. Develop detailed migration timelines that involve appropriate stakeholders. Phased implementations and rollouts are a safe bet.
- Establish metrics to measure implementation success and security improvements.

## The path forward

A password and passkey manager is a secure authentication solution. Password managers have proven their value in enterprise environments, providing robust security and convenience. Passkeys add another layer of options for organizations seeking to enhance their authentication strategies. They offer significant benefits for securing online accounts by reducing vulnerabilities and allowing quick access. The benefits of higher security, ease of use, and better reliability will more than justify the investment.

Whether you choose to maintain a password manager infrastructure, implement passkeys, or adopt a hybrid approach, both methods offer paths to secure, efficient authentication. Begin planning your passkey implementation today to future-proof your authentication strategy and position your organization at the forefront of secure, modern access.

To learn more, explore the Bitwarden approach to authentication management and see how a trusted provider supports both password management and passkey deployment, helping organizations make informed decisions about their authentication strategy.

Get started managing passkeys in Bitwarden with a free account or a 7-day free enterprise trial.