Passwordless Authentication with Passkeys

Passkeys enable users to sign in to apps and websites with biometrics (facial recognition or fingerprint), PIN, or pattern, delivering a more secure and seamless passwordless authentication experience.

GUIDE INTEGRATIONS

What are Passkeys?

Passkeys are a phishing-resistant alternative to traditional authentication factors (such as username/password) that offer an easier and more secure login experience to users. Passkeys are modeled from FIDO® W3C Web Authentication (WebAuthn) and Client to Authenticator Protocol (CTAP) specifications.

Passkeys reduce the friction experienced with single-device authentication methods by allowing credentials to sync across devices. Cross-device authentication eliminates the need for users to reenroll on each of their devices. It also supports a more reliable recovery method as the stored credentials can survive the loss of an originating device.

Are Passkeys Secure?

Passkeys represent a fundamental improvement in security over traditional password-based authentication. Passkeys leverage advanced cryptographic techniques and modern authentication frameworks, providing several key advantages:

--> Phishing Resistance: Passkeys use public-key cryptography, where a unique key pair is generated for each service. The private key never leaves the user's device and is never exposed to the service provider, making it resistant to phishing attacks.

--> No Password Reuse: Since passkeys are unique for each service, there’s no risk of password reuse across different sites, a common issue with traditional passwords.

--> No Central Password Storage: Service providers do not store passwords, only public keys. This means that even if a service provider’s database is breached, attackers cannot obtain user credentials.

--> Local Authentication: Authentication is performed locally on the user's device, significantly reducing the risk of credential interception during transmission.

--> Multi-Factor Authentication (MFA): Passkeys can serve as a form of multi-factor authentication by combining something the user has (the private key) with something the user is (biometrics) or something the user knows (a PIN).

Passkey Benefits

User Experience

Elevated user experience by logging users in with face ID or fingerprint.

Security

Public-private key pairs eliminate any credential phishing attempts.

MFA

Passkeys are both possession (device) and inherence (biometrics).

What Devices Support Passkeys?

Passkeys are supported by >90% of devices, with a wide range supported across different operating systems and platforms.

Supported operating systems include iOS (16+), macOS (13+), Android (9+), Windows (10/11), and Linux.

Supported browsers & apps include Safari, Chrome, Brave, Edge, Firefox, iOS apps, Mac apps, Samsung Internet, and Android apps.