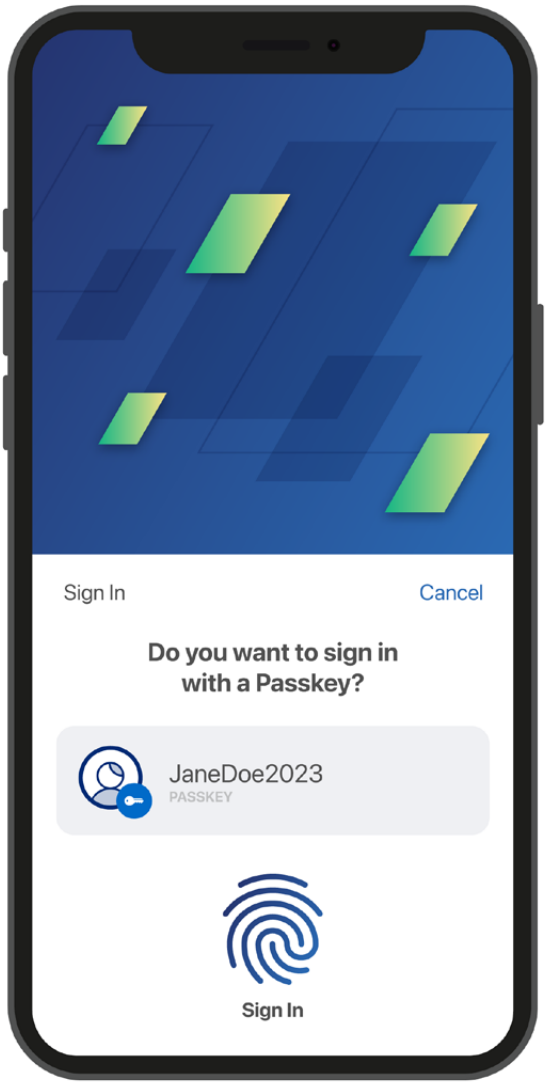
It's Time to Go Passwordless

Almost every business now relies on the internet, and digital identity is how people connect to these businesses. The average person has over 90 online accounts, each with its own unique password. However, it can be difficult to keep track of so many passwords, leading many people to reuse passwords across multiple sites. This is risky because if one password is compromised, attackers can potentially use it to access multiple accounts.

Authentication methods need to be easier and more secure for internet users. While there are good multi-factor authentication solutions available, many are complex and difficult to integrate. Passwordless technology is becoming more popular with organizations that want to provide a better online experience for their workers and customers.
The Fast Identity Online 2 (FIDO2) WebAuthn standard for passwordless authentication, approved in March 2019 by the World Wide Web Consortium (W3C), enables businesses to offer passwordless authentication. The WebAuthn passwordless standard is supported by major browsers and operating systems.[1]



WebAuthn uses public-key cryptography, where the user's private key never leaves the user's device. But, dependence on a specific device to authenticate does have its drawbacks – particularly if a user loses or replaces their device. Now, industry-leading vendors are helping expand the FIDO2 standard to support **passkeys**[2], a method that enables users to use one seat of passwordless credentials to authenticate to services across multiple devices, browsers, and platforms. Passkeys allow the user's private keys to be stored in a vault in the device vendor's cloud instead of on their physical device.

Phase in Passwordless

Passwordless authentication doesn't have to be an all-or-nothing project. You can roll it out in phases. Start with the people who need it the most: high-profile individuals who perform high-stakes transactions and are at the highest risk of phishing and other forms of attack. Tech-savvy users eager to enroll their WebAuthn-enabled devices are also good candidates for a passwordless pilot program.

You can roll out passwordless incrementally for your consumers as well — for example, by presenting every fifth user logging into your site(s) with an option to enroll a mobile device or hardware token for passwordless authentication.

 |

Orchestrate Your Way to Passwordless Authentication

ForgeRock's orchestration capabilities make it easy to go passwordless. You don't need to be a developer. Simply drag and drop pre-coded WebAuthn "nodes" into the orchestration user interface and wire them together. Test and optimize passwordless user experiences with different groups, and enable users to choose their preferred authentication devices. Passkeys is based on WebAuthn, and ForgeRock supports it out-of-box.

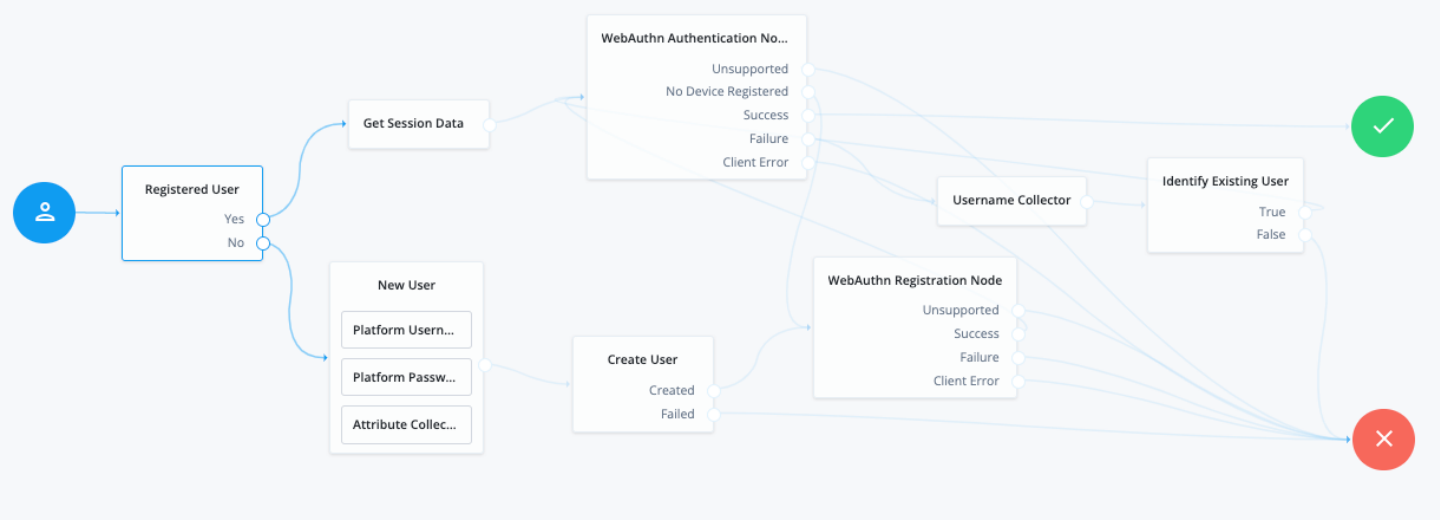


Figure 1: A passwordless user journey combining WebAuthn user registration and authentication

Going Passwordless enables you to:

- Support Zero Trust security decisions. Use device details, such as only allowing trusted devices to enable passwordless and usernameless authentication, or adding authentication barriers based on device trust, such as "read-only" if the user is on an untrusted device.
- Save on cost and complexity. Users can authenticate with any device or method that supports FIDO2 WebAuthn, including **passkeys**.
- Enable **usernameless** authentication for devices that support resident keys.[3]

Passwordless Authentication Benefits

- **Secure:** Login credentials are unique for every website, eliminating person-in-the-middle attacks.
- **Convenient:** Uses simple built-in methods, such as fingerprint readers or cameras, or leverages easy-to-use FIDO security keys. Consumers can select the device that best fits their needs.
- **Standards-based:** Secure, interoperable, and agile enough to meet new business demands.
- **Easy to implement:** Drag and drop no-code WebAuthn passwordless nodes into ForgeRock Intelligent Access trees.

Leverage Third-Party Technology for Flexibility and Choice

ForgeRock provides passwordless solutions that are flexible and customizable, allowing you to meet your changing needs. Solutions available through the ForgeRock Trust Network include biometric systems, decentralized passwordless authentication, and hardware authenticators.

Going Passwordless Is Simple. Get Started Today.

To learn more about ForgeRock Passwordless Authentication and how it can provide differentiated, secure, and cost-saving user experiences, download the white paper, " Go Passwordless. Authenticate Securely" today.

ForgeRock Passwordless Authentication Capabilities

- Cross-Platform FIDO or U2F Authenticators such as YubiKeys, Feitian, Titan, Duo, Google Titan, OneSpan DigiPass, RSA SecureID, Symantec VIP, CAC/PIV Smart Cards, Yubikey tokens, and any OATH compliant hardware tokens
- Platform Authenticators: (examples: Apple TouchID, Windows Hello)
- passkeys
- Device Attestation Formats: Packed, FIDO U2F, None
- Device Attestation Types: NONE, BASIC, SELF, CA (AttCA)
- MFA
- Passwordless
- Usernameless
- DisplayName and UserName
- Flexible Origins
- Trust Anchoring
- TrustStore for Supported Device Certs
- TrustStore CLI Tool
- FIDO Alliance Metadata Service
- Attestation data available to Authentication Nodes
- New Device Storage Node
- Enhanced Auditing
- API Protocols: SOAP, REST, Webhooks, GRPC, and LDAP

1 Yubico. "The WebAuthn Standard: Why It Should Matter to the Public Sector and How It Works"

2 Fido Alliance. "Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins."

3 Check with your device vendor before attempting to enable usernameless authentication with passkeys.

About ForgeRock

ForgeRock®, (NYSE: FORG) is a global leader in digital identity that delivers modern and comprehensive identity and access management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than 1300 global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit www.forgerock.com.

Follow Us

ForgeRock