ForgeRock

INTELLIGENT ACCESS SERIES

Go Passwordless

Authenticate Securely.

The Problems with Passwords

As an identity and access management professional, you know that passwords are a problem. Your users hate having to create accounts with them. Your security teams worry about email phishing attacks, credential theft, and data breaches.

The average user has more than 90 accounts. Remembering passwords is hard, which is why more than 50% of users have reused passwords across multiple websites.[1] Creating passwords that rely on personal information makes accounts vulnerable to dictionary attacks. Using a password management system is one way to deal with the password problem, but some of these services themselves are vulnerable.[2]

> In Verizon's "2021 Data Breach Investigations Report (DBIR)," 61% of breaches involved credentials.[3]

The ForgeRock Consumer Identity Breach Report 2020 found that unauthorized access was the number one attack method used by cybercriminals for 43% of breaches. Of the industries surveyed in the report, the healthcare sector suffered 34% of all breaches, followed by financial services at 12%.[4]

In 2018, Iowa's UnityPoint Health's business email system fell victim to a series of email phishing attacks targeting employee credentials. While the motive was likely to steal funds from the company, the attacks also resulted in leaking protected patient health information (PHI) and/or personal financial information.[5]

Breaches due to credential theft are not going away. Organizations can try to protect themselves and their employees and customers through security training, email security measures, and stronger authentication. But until username and password authentication is replaced with more secure methods, credential theft will continue to be a favored tactic for attackers.

This paper proposes that ForgeRock Passwordless Authentication, based on industry standards, can reduce or eliminate reliance on username and password-based authentication, and improve your organization's security posture.

But first, let's look at what alternatives are in use today.

Strong Authentication

Many applications and services now offer "strong authentication," using either two-factor authentication (2FA) or multi-factor authentication (MFA).

2FA requires a user to first authenticate with a username and password and then a second factor reliant on a one-time passcode (OTP). These are typically delivered via an authenticator app, a response to a push notification on a mobile app, or – least securely – over the SMS text messaging protocol. With 2FA, the second authentication factor must be presented at each authentication attempt.

MFA incorporates more contextual attributes – more types of authenticators and more context – such as user device, browser, IP, location, or time of day. Some MFA solutions may require the user to authenticate more or less, depending on the session context.

> Mixing two or more types of factors increases security, but combining two or more non-unique factors can do more harm than good.

The underlying principle of both of these methods is that strong authentication should require the user to authenticate with a combination of at least two unique factors. The username and password are "knowledge" factors (something they know). The mobile device, hardware token, or smart card are "possession" factors (something they have). And, biometrics, such as fingerprints or facial recognition identifiers, are examples of "inherence" factors (something they are).

Websites that require users to authenticate via a username and password and then ask the user to present other knowledge factors, such as "security questions" that the user may forget over time, render the second authentication factor useless. Answers to common security questions (example: mother's maiden name) are available through public records, social networking, or social engineering.

2FA and MFA are more secure than username and password authentication, but they too have their limitations. 2FA can become tiresome to users who have to authenticate two ways every time, especially if it involves switching to an authenticator app or SMS message to find and then enter the one-time passcode. MFA can be difficult to implement and often relies on configuring policy rules that do not provide the agility and fine-grained access that security teams need. A successful MFA or 2FA implementation also largely depends on the strength and flexibility of the organization's identity and access management solution.

A Standards-Based Approach to Authentication

Strong authentication is better served by a standards-based approach that can reduce or eliminate reliance on the username and password. Analyst firm Gartner recommends replacing passwords with biometric authentication and predicts that 60% of large and global enterprises and 90% of midsize enterprises will replace passwords with other methods for more than 50% of identity use cases by 2022.[6]

In 2019, the World Wide Web Consortium (W3C) ratified the Fast Identity Online 2 (FIDO2) Web Authentication (WebAuthn) standard, which enables usernameless and passwordless authentication.

Browser, operating system, and hardware vendors are signing onto the FIDO alliance and are rolling out support for FIDO2.[7]

The original FIDO standard, also known as Universal 2 Factor (U2F), uses a scalable public/private key model, where a new key pair is generated for each service, maintaining separation between key pairs to preserve privacy.[8] It allows "passwordless" authentication to online services using a hardware security key.

The newer FIDO2 standard is the "usernameless and passwordless" evolution of FIDO, and it relies on credentials stored locally on a user's device. FIDO2 consists of two specifications:

- A web-based API, called **Web Authentication (WebAuthn)**, enables "passwordless" authentication to web applications using public-key encryption and authenticators. WebAuthn supports credentials based on the original FIDO U2F standard and FIDO2 credentials.
- A FIDO2 **Client to Authenticator Protocol (CTAP2)**, enables the communication between client applications to FIDO2-enabled authenticators via FIDO2-enabled browsers and operating systems.

Types of authenticators

FIDO2 relies on public/private key pairs stored securely on local hardware and FIDO2-compliant browsers that interact with services to mint secure public/private key credentials for each service. The private keys in each key pair are stored locally and never leave the user's authenticator. The public keys are used by the authentication server to encrypt and sign communication to the users' endpoint devices.

The storage capability of the user's local authenticator determines whether we can enable "usernameless" as well as passwordless authentication.

Platform authenticators, based on the trusted platform module (TPM) or secure enclave installed on many laptops and phones, are usually unlocked by a biometric sensor, as in Microsoft Windows Hello or Apple TouchID.

Cross-platform, or "roaming," hardware authenticators present a user's access claims to another service or device. Examples of these are Google Titan security keys, YubiKeys, or Duo authenticators that use USB, near-field communication (NFC), and Bluetooth. When activated by inserting into a USB port, pressing a button, or by tapping, the authenticator sends a signed response that validates the user's login. Smartphones can also act as authenticators.

By relying on the secure credentials stored on the user's own trusted hardware, FIDO2 WebAuthN enables authentication without usernames and passwords, virtually eliminating the potential for data breaches related to credential theft.

ForgeRock Passwordless Authentication

ForgeRock Passwordless Authentication implements the FIDO2 WebAuthn standard in ForgeRock Intelligent Access. It enables you to design secure and seamless user journeys for authenticating without passwords, and in cases, without usernames as well.

ForgeRock Passwordless Authentication reduces your organization's attack surface by virtually eliminating credential theft arising from phishing attacks, password reuse, credential stuffing, keyloggers, and more.

Benefits of passwordless authentication

- **Secure:** Login credentials are unique for every website, and never leave the user's device. Unlike username and password, credentials are never transmitted on the wire, thus eliminating person-in-the-middle attacks.
- **Convenient:** It 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.
- **Private:** Keys are unique and can't be used to track users across sites. Biometric data never leaves the user's device.

"We are positioned to give all of our users a much better user experience through the elimination of usernames and passwords, as well as reduce calls to our service desk for forgotten passwords."

— Doug Neumann, IT Manager, U.S. National Nuclear Security Administration

How Passwordless Authentication Works

ForgeRock delivers passwordless authentication through ForgeRock Intelligent Access Trees and WebAuthn-specific registration and authentication nodes. To use passwordless authentication, the user must first register by authenticating with their username and password against the identity store, so that ForgeRock can identify the user and their device.

When a user first attempts to register their device, ForgeRock Intelligent Access detects whether the device supports the WebAuthn standard. If the device registration is successful, ForgeRock instructs the user's device to mint a unique public/private key pair for communicating with ForgeRock. When the user authenticates to their device using the built-in biometric sensor, the user's private key, which is stored securely in persistent memory and never leaves the device, becomes available to sign authentication challenges.

ForgeRock issues a challenge to the user's device and encrypts it with the user's public key. The private key on the user's device signs the challenge, which ForgeRock verifies with the user's public key. This process establishes the secure connection between the user's hardware device and ForgeRock, so they can then use passwordless authentication for subsequent logins.

Traditional username and password-based user journeys, paired with step-up authentication, should be maintained as an alternative method if the user cannot authenticate with ForgeRock using their registered trusted device (example: if their trusted device is unavailable, lost, or stolen).

Using passwordless authentication without biometrics

Some people can't use biometrics, or their organizations do not support it. You can enable passwordless authentication with any PIN-protected external authenticator (something you know and something you have), such as FIDO2-enabled smart cards, FIDO2, or Universal 2 Factor (U2F)-compliant hardware security keys, or smart watches. ForgeRock supports FIDO2 Web Authentication passwordless capabilities for numerous authenticators, attestation formats, and types. For more information, read the Solution Brief.

Configuring Passwordless Authentication

Passwordless authentication is a set of features in ForgeRock Intelligent Access designed to support the FIDO2/WebAuthn standard.Users can register trusted devices and use its built-in capability to store credentials locally. There are three pre-configured nodes in Intelligent Access trees. These nodes can be simply dragged and dropped into the Intelligent Access user interface to create user journeys. To learn more about Intelligent Access trees and nodes, read the white paper, "Introducing ForgeRock Intelligent Access."

Registering a device

Users must first authenticate with their username and password and then register their device before they can enjoy passwordless authentication. To enable this, build the user journey and add a WebAuthn Registration Node after the username/password collection and data store decision node. If the user successfully registers an authenticator of the correct type as determined by the node's properties, the tree evaluation continues along with the Success outcome. Passwordless authentication will fail if the client doesn't support WebAuthn – for example, if the browser they are using is unsupported, or if they registered with the wrong type of authenticator. A Client Error outcome can occur when the client registration times out.

Validating user identity

Any authenticator used for passwordless authentication should be validated against a user's identity to be considered secure. Organizations must validate users to their authenticators either in person or by using a trusted digital identity proofing process while registering authenticators. To learn more about identity assurance levels and digital identity proofing processes that you can build into ForgeRock Intelligent Access, download the white paper, Reduce Government Services Fraud – Incorporate Identity Proofing Into Citizen Registration and Authentication.[9] To learn more about incorporating credit-based identity verification, read the white paper, Reduce the Total Cost of Fraud.

Enabling authentication without a username

To make it possible for the user to authenticate without entering their username for future authentications, toggle on "Username to device" at the right of the Registration Node.

Authenticating without a username requires that the user's authenticators support storing resident keys.

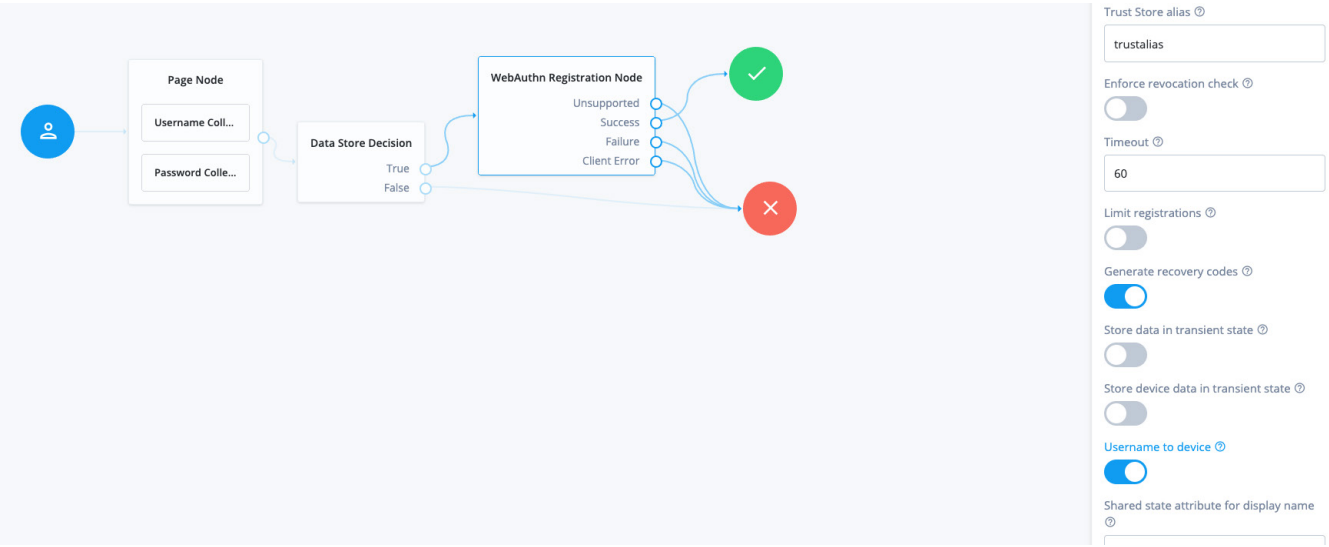

Figure 1: Passwordless registration with usernameless authentication enabled

After the user successfully registers and wants to sign in, the WebAuthn Authentication Node runs and shows the user a “usernameless” login journey.

Analyzing a device

If you want to perform additional analysis on a user’s device and delay registering a device until the outcome of the analysis is complete, you can add the WebAuthn Device Storage Node into your WebAuthn registration tree. This node is optional.

Here’s an example of how you can use it. Let’s say you want to enable usernameless and passwordless authentication, but only for employees who are using corporate-issued laptops made by a certain manufacturer and only for those laptops installed with a biometric TPM. You can add the WebAuthn Device Storage Node into the registration tree, along with a custom-scripted decision node designed to capture device-specific attestation data (example: serial number, and, for better security, a certificate chain to verify the device is genuine). This prevents even valid users from authenticating from unmanaged devices and strengthens your organization’s security posture.

To enable the WebAuthn Device Storage Node, toggle on “Store data in transient state” at the right of the screen. The transient state means that device data is only stored in temporary memory, thus allowing ForgeRock to use it for analysis.

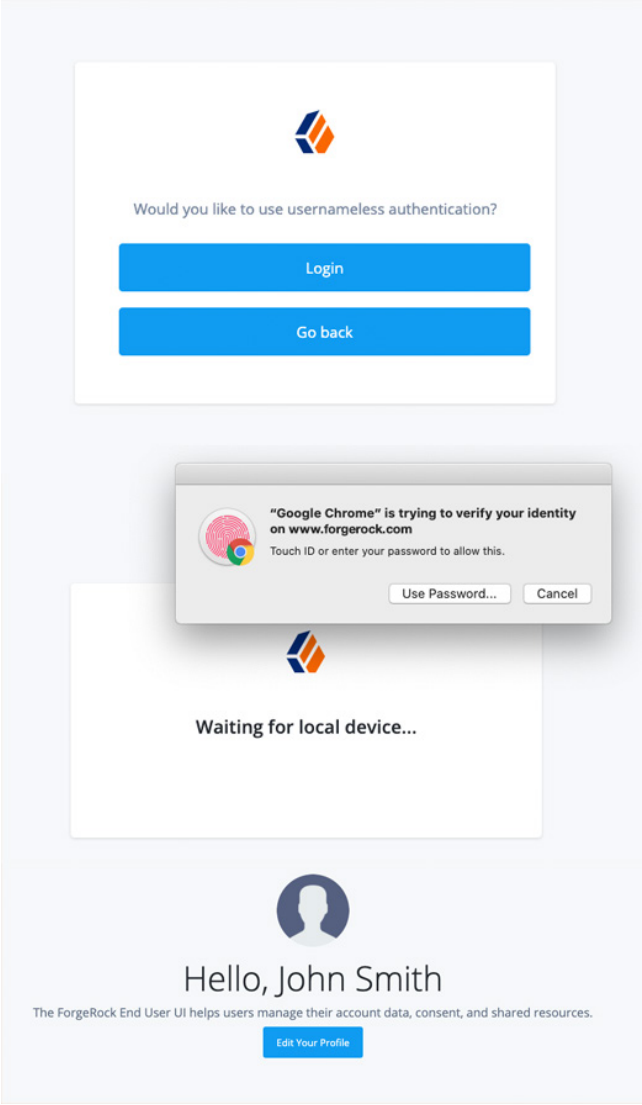

Figure 2: Authenticating without a username

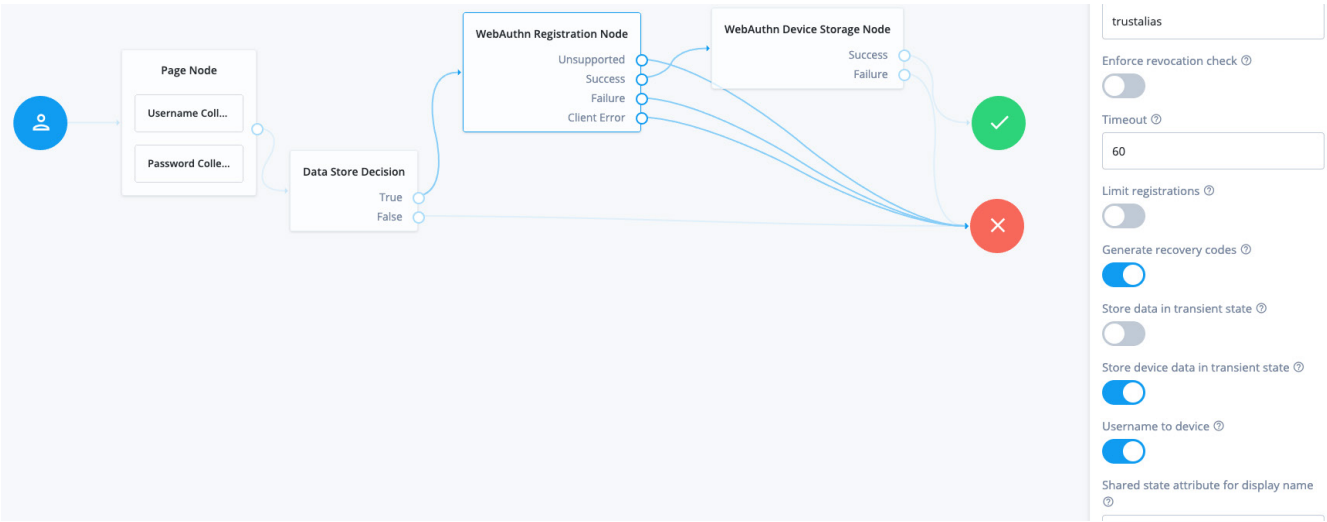

Figure 3: WebAuthn Device Storage Node in a registration journey

Passwordless authentication alternatives

Users should always have an alternative to passwordless authentication if their registered device is lost or stolen or if they are using a browser or device that doesn't yet support FIDO2 credentials and WebAuthn. You can design user journeys that collect username and password credentials and add MFA, incorporating the platform Trusted Platform Module (TPM), mobile push, or third-party authenticators.

When to use passwordless authentication

ForgeRock Passwordless Authentication is ideal for workforce users who authenticate to cloud or on-premises applications. ForgeRock Passwordless Authentication can be used for both initial login and step-up authentication, including transactional authorization. To learn more about step-up authentication and transactional authorization, read the white paper, "Introducing ForgeRock Intelligent Access."

As more browsers and consumer-facing applications begin to support FIDO2 and the WebAuthn standard, you will be able to design passwordless user journeys for customer use cases as well. The WebAuthn standard is being used today in social media, financial services, gaming, and cloud storage applications.

ForgeRock Passwordless Authentication can be used for both initial login and step-up authentication, including transactional authorization.

Conclusion

ForgeRock Intelligent Access makes it easy for you to quickly design secure authentication without usernames and passwords for workforce and consumer use cases. You can design these user journeys in minutes, and support multiple authenticators simultaneously, enabling significant cost savings over legacy strong authentication solutions. ForgeRock Passwordless Authentication offers better security, convenience, and privacy for your users.

[1]https://fidoalliance.org/what-is-fido/
[2]https://www.welivesecurity.com/2020/03/19/security-flaws-found-in-popular-password-managers/
[3]https://enterprise.verizon.com/resources/reports/dbir/
[4]https://www.forgerock.com/resources/2020-consumer-identity-breach-report
[5]https://www.unitypoint.org/filesimages/About/Security%20Substitute%20Notification.pdf
[6]https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security/
[7]https://www.theverge.com/2020/6/24/21301509/apple-safari-14-browser-face-touch-id-logins-webauthn-fido2
[8]https://www.yubico.com/blog/what-is-fido2/
[9]https://www.forgerock.com/resources/whitepaper/reduce-government-services-fraud