Whitepaper

How to go passwordless with Okta

A brief guide to passwordless authentication options in Okta.

Introduction

86 percent of all web application data breaches involved the use of stolen credentials (i.e., compromised usernames and passwords), according to the 2023 Data Breach Investigations Report by Verizon. This is no surprise when users continue to reuse existing passwords even if they were compromised in previous breaches. Meanwhile, attackers are taking advantage of greater computing power at reduced costs to launch sophisticated techniques and tools to steal credentials. Reducing reliance on passwords as a major authentication factor is an important step toward reducing the risk of data breaches.

For consumers, everyday technologies such as Apple Touch ID, Face ID, and Windows Hello allow users to access their devices password-free. And for the workforce, technologies like fingerprint, card readers, and mobile authenticator apps help to provide a passwordless experience.

Leaving passwords behind is an important step toward better security, but how do we reach the point of deploying extensive passwordless authentication?

Implementing multi-factor authentication (MFA) is a great initial step for ultimately deploying passwordless. Secure factors such as FIDO2 WebAuthn and mobile authenticator apps that support biometric authentication will enable widespread adoption of passwordless authentication. These secure factors, coupled with contextual access, will help to eliminate the use of passwords.

And Okta is here to help. Okta Workforce Identity Cloud supports a variety of passwordless authenticators that can be configured alongside security policies that are further augmented by risk evaluations based on signals collected to understand the context of the access decision (e.g., user, location, device, network, and more).

In this introductory whitepaper, we will cover the various features within Okta that allow you to deliver passwordless authentication to the workforce.

How do I start thinking about deploying passwordless?

In the introduction, we mentioned that deploying MFA is an essential first step to going passwordless.

MFA is defined as providing two out of the three factor categories of knowledge, possession, and inherence as part of the authentication process. For example, a password plus an SMS one-time password (OTP) would be a combination of knowledge and possession, while a password with biometrics would be a combination of knowledge and inherence.

However, another category to consider would be implicit factors. These are factors that are not necessarily presented by end users but are considered before making an access decision. For example, if a login is coming from a new device and a new location, you will likely want to have a stronger factor type for authentication. However, if a login is coming from a known device and a known network, a single, low, or medium strength factor may be acceptable.

Ultimately, the goal is to start your passwordless journey by tying the appropriate factor to the level of risk. For example, if the device that initiated an access request has low or medium levels of assurance, a stronger factor can be required or access can be denied altogether.

What passwordless options are supported by Okta?

Okta offers a variety of passwordless authentication methods to address the requirements of your business and workforce. This section covers the features available today with Okta Identity Engine that help to achieve passwordless authentication.

Okta FastPass

FastPass enables secure passwordless and phishing-resistant authentication into the resources you need to get your work done — across devices, browsers, and applications. It does so by minimizing end-user friction, while enabling cryptographically secured access and adaptive policy checks that strengthen the Zero Trust security posture of your organization. It supports any SAML, OIDC, or WS-Fed app in Okta. It can be used on Windows, iOS, Android, and macOS devices, from any location or network. In addition, Okta supports an open ecosystem with third-party, best-of-breed, phishing-resistant authenticators, while providing controls through the Okta admin console.

How does FastPass work?
By establishing strong trust in user identities and in their devices, FastPass provides a Zero Trust authentication solution.

This starts with the user leveraging the Okta Verify app to register their device to Okta's Universal Directory. This establishes a trusted user and device pairing that verifies that the device is recognized by Okta and in possession of an authorized user. From there, users get instant access to all of their applications without being prompted for additional credentials.

Once the device is registered, IT admins can enforce app-level policies with device assurance in order to check sets of security-related device attributes as part of authentication policies before that device can be used to access Okta-protected resources. This helps organizations to establish minimum requirements for the devices that are used to access critical systems and applications, denying access if those requirements are not met. Okta also factors in risk signals from other third-party security solutions, to round out the context in which access is allowed or denied. With FastPass, organizations can provide their workforce with the tools they need to remain productive without sacrificing security.

FastPass works on managed and unmanaged devices. It has no requirements for directories or specific endpoint management tools.

Here's a detailed guide on how FastPass works.

FIDO2 (WebAuthn)

WebAuthn is a browser-based API that allows for web applications to simplify and secure user authentication by using registered devices (e.g., phones, laptops, etc.) as factors. This standards-based method ensures secure passwordless authentication, employing public key cryptography to safeguard users against sophisticated phishing attacks. In addition to FastPass, WebAuthn is one of the few factors that offer phishing resistance.

Here's a detailed guide on how WebAuthn works.

WebAuthn is compatible with a wide range of devices and security keys. These fall into two main categories:

1. Hardware-integrated factors (also known as on-platform authenticators) like Windows Hello on Windows 10+ (version 1903 and later), Touch ID on MacBook, Fingerprint on Android 7.0+, and Touch ID and Face ID on iOS.
2. Off-device, roaming authenticators such as YubiKey 5Ci, FEITIAN BioPass, HID Crescendo smart card, and more. These off-device authenticators provide additional options for secure authentication.

The use of WebAuthn is dependent on the combined support of the web app's authentication process, the browser, and the device.

Examples of browsers, hardware, and operating systems that support WebAuthn:

- Google Chrome on macOS using Touch ID
- Google Chrome on Windows 10 using Windows Hello
- Microsoft Edge on Windows 10 using Windows Hello
- Firefox on Windows 10 using Windows Hello
- Google Chrome on Android 7.0+ using devices with fingerprint support
- Desktop apps on Windows and macOS that use a WebAuthn-compatible browser for login using Windows Hello and Touch ID, respectively
- Native mobile apps that use a WebAuthn-compatible browser (e.g., Chrome) for login on Android 7.0+ using fingerprint support

WebAuthn is a secure way of implementing passwordless, phishing-resistant authentication across the organization, and Okta supports WebAuthn as part of our adaptive MFA solution.

Smart card (PIV/CAC)

In 2004, President George W. Bush issued the Homeland Security Presidential Directive 12 (HSPD 12) that mandated all federal employees and contractors in the United States be given a common identification card that could be used anywhere and everywhere. Acting upon this directive, the Information Technology Laboratory of the National Institute of Standards and Technology (NIST), working with private industry and other federal agencies, developed a standard for a common government-wide identification system.

This standard is the Federal Information Processing Standard (FIPS), specifying personal identity verification (PIV) requirements for Federal employees and contractors. It is based on the use of smart cards with a X.509-compliant certificate and key pair. More specifically, a physical card contains a digital file that can only be accessed by the owner. It can be used to verify that the PIV credential was issued by an authorized entity, has not expired, has not been revoked, and the holder of the credential is the same individual it was issued to. A Common Access Card (CAC) is also issued by the Department of Defense (DoD) for military personnel in compliance with the directive.

While PIV/CAC-based authentication may not be relevant for all industries, Okta’s implementation of PIV/CAC authentication offers another form of passwordless authentication. Admins can enable a smart card as an “Identity provider” in their Okta organization, which involves uploading a root certificate to Okta and configuring routing rules to define when login via PIV/CAC card is required. The end user will be redirected to an Okta authentication screen where they can use PIV/CAC as the login credential. They will choose the certificate stored on their PIV/CAC card, enter their PIN, and they’re in — no username or password required.

Okta also allows using PIV/CAC cards as a step-up MFA to authenticate to specific apps. Here's how it works:

1. Admins enable the smart card as an authenticator in the admin console.
2. Once admins add the smart card authenticator, they can configure an authenticator enrollment policy and authentication policy for each app they want to protect with smart cards.
3. When end users attempt to access a protected app, they will perform the smart card verification — again, no username or password required.

Desktop Single Sign-On

With Desktop Single Sign-on (DSSO), users are automatically authenticated by Okta after they sign in to their Active Directory network on their device (e.g., Windows, macOS). Following authentication, users can access applications through Okta without entering additional usernames or passwords. DSSO improves the user experience because users only need to sign in a single time and don't need separate credentials for each application they access through Okta. Two methodologies are available for DSSO implementation:

- Agentless (recommended)
- IWA web agent running on-premises

Here's how Desktop Single Sign-On works:

1. A user enters their AD credentials to log in to their desktops or laptops.
2. After logging in to their device, the user will not be prompted for any additional credentials (unless MFA is required) to access the Okta dashboard, a desktop client that supports modern authentication, or any Okta-protected application.

You may be wondering what the difference is between DSSO and Okta FastPass. The benefit of FastPass is that the device does not need to be Active Directory domain-joined or in-network for users to enjoy a passwordless experience to access their resources. Okta FastPass also works across Windows, macOS, iOS, and Android devices.

Email Magic Link

Email-based passwordless authentication has become very common for consumer use cases and is also gaining traction in workforce scenarios. This method is commonly used for authentication, enrollment, and password recovery. It involves sending a one-time secure link, often referred to as a “magic link,” to the user’s registered email address, allowing the user to reset their password and gain access to their account. It’s familiar to most users because they’ve used it dozens to hundreds of times.

Common apps like Slack and Medium have popularized this method of authentication. True passwordless authentication, however, takes the password reset flow a step further.

Here’s how the Email Magic Link feature works for this scenario:

1. A user registers for or logs in to an app by entering their email address.
2. The app will prompt them to click on a link sent to their inbox to finish the authentication process.
3. The user opens their inbox, clicks on the link, and is then redirected back to the app, completing the login.

App designers remove the password (and its associated resetting ceremonies). The best part? The user never needs to set, save, or type any passwords and has no hardware dependencies.

Summary

Feature
Okta FastPass Device-based, phishing-resistant, passwordless authentication for Windows, iOS, Android, and macOS
FIDO2 (WebAuthn) Phishing-proof, biometrics-based authentication using the FIDO2 standard
Smart Card (PIV/CAC) Authentication via an x509 certificate, mostly used by US federal agencies
Desktop Single Sign-On Passwordless login for AD domain-joined machines
Email Magic Link Email-based passwordless authentication best suited for workforce and consumer apps

How do I learn more?

This whitepaper is an overview of the various passwordless capabilities supported by Okta. If you would like to understand more about how multi-factor authentication can help with the journey to passwordless, visit our Okta Adaptive MFA web page.

About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology — anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.