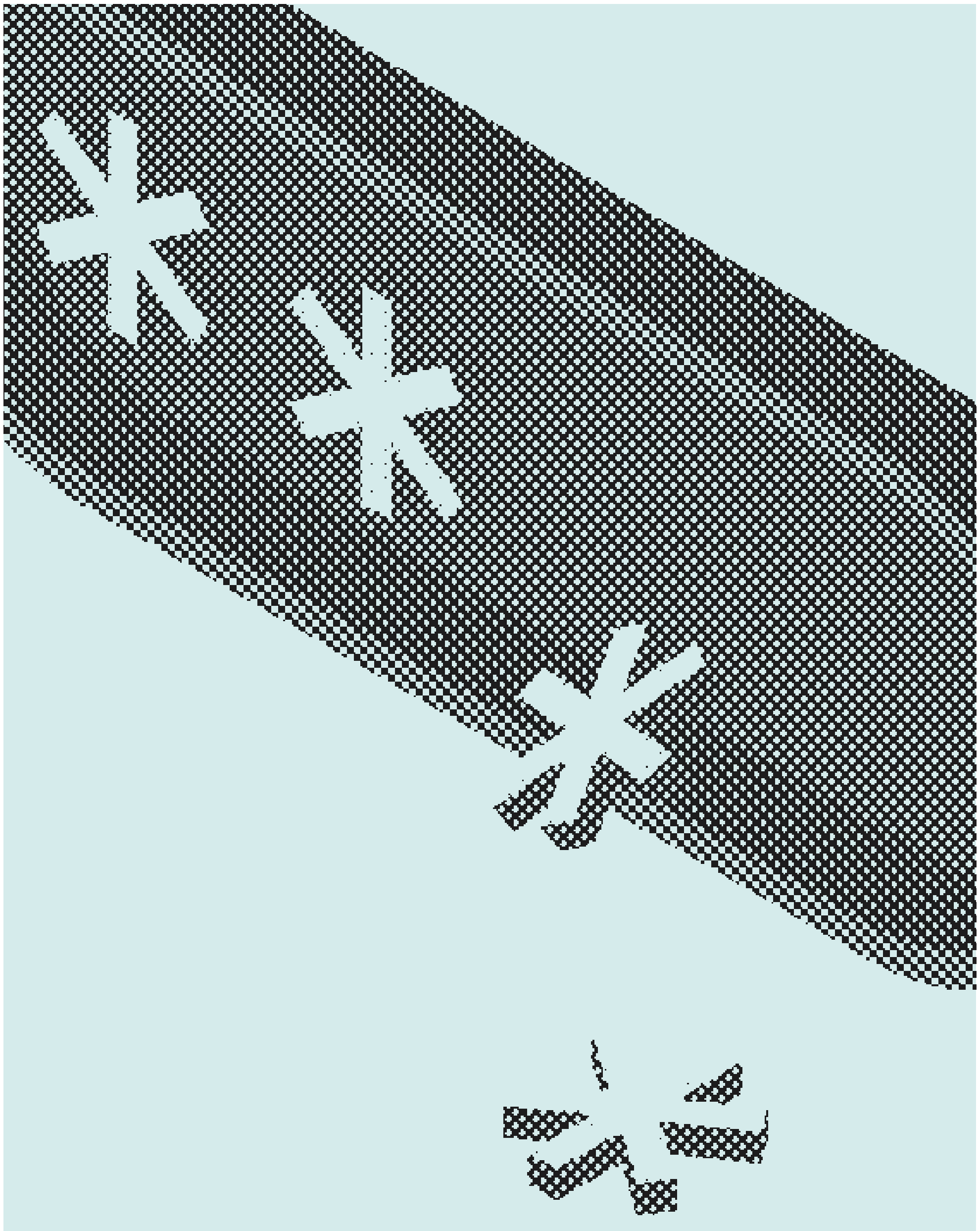
Whitepaper

March 2022

How to go Passwordless with Okta

A brief guide to passwordless authentication options in Okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



Introduction

Passwordless authentication is no longer a dream of the distant future. For consumers, everyday technologies such as Apple Touch ID and Face ID and Windows Hello allow users to access their devices password free. And for the workforce, technologies like fingerprint and card readers and mobile authenticator apps help to provide a passwordless experience.

Leaving passwords behind is an important step towards better security and identity access management (IAM), and it's equally important to strengthen authentication by taking into account the context of every login request.

The question is, how do we get to the point of deploying passwordless authentication? Implementing multi-factor authentication (MFA) is a great foundation for ultimately deploying passwordless. Secure factors such as FIDO2.0/WebAuthn and mobile authenticator apps that support biometric authentication will put you on a path to eventually deploy passwordless authentication company wide. These secure factors, coupled with login context, will allow you to forego the requirement for a password in the authentication process.

This is where Okta can help. Okta's integrated Single Sign-On and Adaptive Multi-Factor Authentication solutions allow organizations to include risk evaluation derived from context (user, location, device, network and more) in the access decision—including passwordless authentication.

For example, you can choose to only allow passwordless logins for low risk logins. And, for a high risk login, you can require one or more strong authentication factors. In this introductory whitepaper, we will cover the various features within Okta which allow you to deliver passwordless authentication to the workforce, customers, and consumers (B2E, B2B and B2C).

How Do I Start Thinking About Deploying Passwordless?

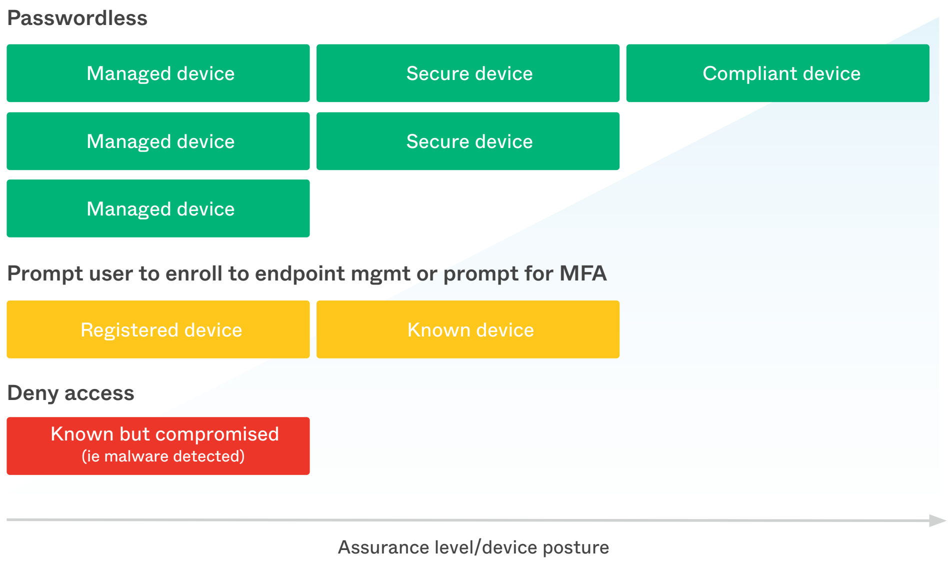
In the introduction we mentioned that deploying multi-factor authentication is the foundation to going passwordless.

Multi-factor authentication is defined as two out of the three categories of knowledge, possession, and inherence factors. For example, a password plus SMS OTP would be a combination of knowledge and possession; a password with biometric would be a combination of knowledge and inherence.

However, there's also a fourth category that isn't always mentioned—implicit factors. These are factors which are not necessarily presented to end users, but rather considered before making an access decision. For example, if a login is coming from both 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 varying levels of risk.

For example, in the following image, we see that there could be varying levels of device assurance that could be tied to passwordless authentication, where medium and low levels of assurance could require a strong factor, or be denied login altogether.



What Passwordless Authentication Options Are Available in Okta?

Okta offers a variety of passwordless authentication methods to address the requirements of your business, across both workforce and customer identity. This section covers the features available in Okta today which help to achieve passwordless authentication, as well a few features on the roadmap. This section also identifies which use case (workforce identity vs. customer identity) each feature is most applicable to.

Okta FastPass

Okta FastPass enables passwordless authentication into any resource you need to get your work done (cloud apps, on-prem apps, VPNs), on any device. For any Okta-connected resource that supports SAML, WS-Fed or OIDC, the login experience can be enhanced with Okta FastPass. Here's how it works.

1. User registers their device to Universal Directory using Okta Verify.
   To support this registration experience, we are enhancing the existing Okta Verify app on iOS and Android and delivering a new Okta Verify app on Windows and MacOS.
2. Admins set policies for when Okta FastPass should be delivered.
   Admins can specify Okta FastPass usage only on managed devices, on any device registered to Okta, only from specific networks, etc.
3. When a user logs in to an Okta resource, they will not be prompted for username or password. Okta Verify will check the policies set by administrators, and allow the user to log in assuming the login meets the correct context.
   This passwordless experience works on browsers (both service-provider-initiated flows and login directly to the Okta dashboard), native mobile apps, and desktop thick clients.

Okta FastPass is available now, and you can learn more about it on the **Okta FastPass web page**.

Use case: Workforce Identity

Factor Sequencing

Factor Sequencing allows administrators to require a chain of factors based on login risk and context. Okta Adaptive MFA allows organizations to achieve secure passwordless authentication by combining the appropriate factor with the appropriate level of risk.

When threat levels are low, the login experience can be streamlined and users can be offered a simpler path to the resources they need access to. However, when the risk level associated with a login is high, additional authentication factors will be required. Here's how Factor Sequencing works.

1. Administrators create a policy (via org-level Sign On rules) defining a factor chain, optionally combined with adaptive policies.
   This includes foregoing the requirement for a password (if desired)

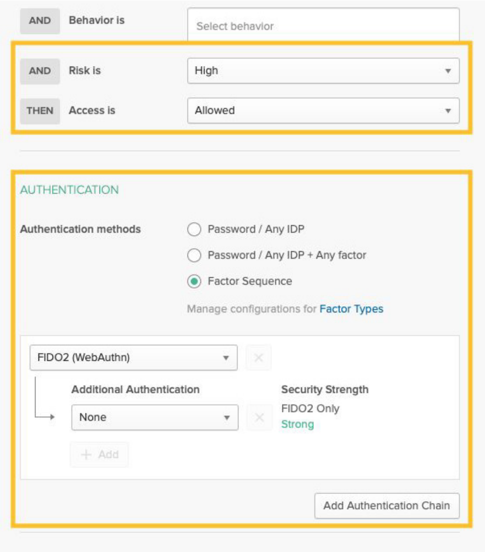
2. End users will see factors presented to them on login, based on the context and factor chain defined by administrators.
   If the administrator has removed the option for password from the login process, end users can now use what was their secondary factor as their primary.

Factor Sequencing is a good example of how a clear MFA strategy helps you to achieve passwordless authentication.
Here are a few examples of policies you could create with Factor Sequencing:

1. Require biometrics-based login (WebAuthn) for high risk

2. Allow Okta Verify with Push or WebAuthn for any login, with no password

3. Present a non-password factor to the user before the password (e.g., Okta Verify Push, then password)
   This can help to protect against password spray attempts



AND Behavior is: Select behavior
AND Risk is: High
THEN Access is: Allowed

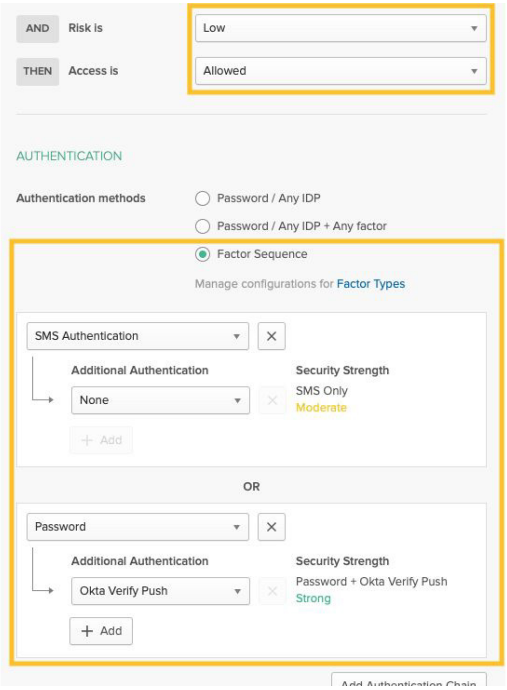
AUTHENTICATION

Authentication methods
○ Password / Any IDP
○ Password / Any IDP + Any factor
● Factor Sequence

Manage configurations for Factor Types

FIDO2 (WebAuthn)
Additional Authentication: None
Security Strength: FIDO2 Only, Strong

4. If risk is high, only allow WebAuthn.



AND Risk is: Low

THEN Access is: Allowed

AUTHENTICATION

Authentication methods:
○ Password / Any IDP
○ Password / Any IDP + Any factor
● Factor Sequence

Manage configurations for Factor Types

SMS Authentication — Additional Authentication: None — Security Strength: SMS Only, Moderate

OR

Password — Additional Authentication: Okta Verify Push — Security Strength: Password + Okta Verify Push, Strong

5. If the risk is low, use SMS OTP or password plus Okta Verify Push.

Use case: Workforce Identity & Customer Identity

WebAuthn

WebAuthn is a browser-based API that allows for web applications to simplify and secure user authentication by using registered devices (phones, laptops, etc) as factors. It uses public key cryptography to protect users from advanced phishing attacks. Today, WebAuthn is the only factor which is phishing-proof.

Here’s how WebAuthn works.

Off-device and roaming authenticators
These are WebAuthn-supported factors that are not built into the hardware (computer or phone).

- YubiKey 5Ci
- FEITIAN BioPass
- HID Crescendo smart card

On-device authenticators and platform authenticators

These are WebAuthn-supported factors that are built into the computer or phone hardware.

- Windows Hello on Windows 10 1903 and later
- Touch ID on MacBook
- Fingerprint on Android 7.0+
- TouchID and FaceID on iOS

Support for WebAuthn is dependent on a web app's authentication process supporting the WebAuthn API, browser support, OS support, and hardware support. This may seem overwhelming, but thankfully, many operating systems, devices and browsers already support WebAuthn. And, Okta supports WebAuthn via our Adaptive Multi-Factor Authentication products.

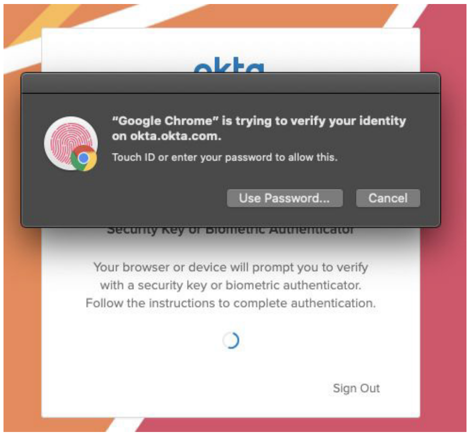
Benefits of WebAuthn over SMS OTP and mobile authenticator apps:

- A standards-based approach to secure passwordless authentication
- Phishing-proof factor type via a public and private key pair for each WebAuthn factor that a user enrolls with
- Best experience for end users—biometrics usage means swift, seamless logins
- The same biometric you use to log in or unlock the device can be used to access apps
- Multiple options for devices and security keys

Examples of browsers, hardware, and operating systems which 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 across the organization.

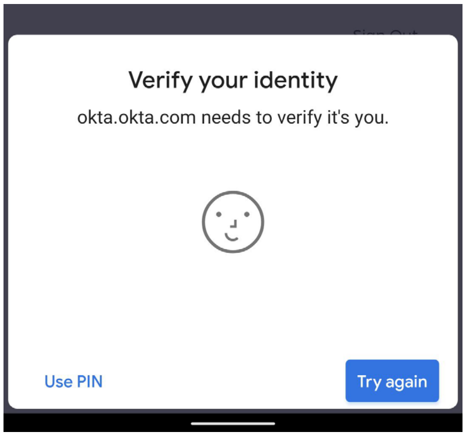

“Google Chrome” is trying to verify your identity on okta.okta.com.

Touch ID or enter your password to allow this.

Security Key or Biometric Authenticator

Your browser or device will prompt you to verify with a security key or biometric authenticator. Follow the instructions to complete authentication.

TouchID on MacOS


Verify your identity

okta.okta.com needs to verify it's you.

Face Unlock on Android

Use case: Workforce Identity & Customer Identity

PIV smart card

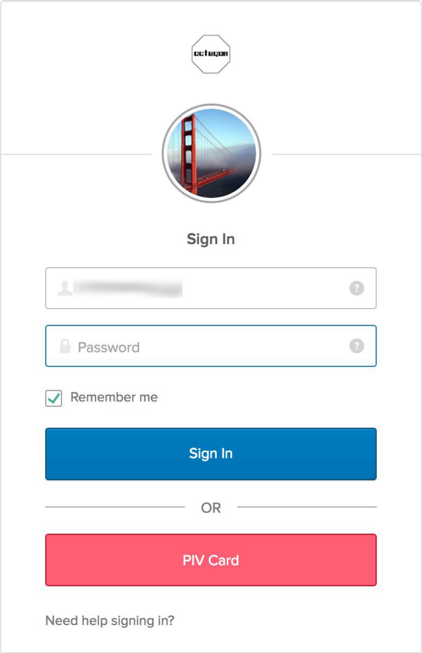
In 2004, President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD 12) that mandated all federal employees and contractors in the United States be given a common identification card that could be used anywhere and everywhere. Acting upon this directive, the Information Technology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

The standard, Federal Information Processing Standard (FIPS) for a personal identity verification (PIV) system, 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.

While PIV-based authentication may not be relevant for all industries, Okta’s implementation of PIV authentication offers another form of passwordless authentication. Here’s how it works.

1. Admins enable Smart Card as an “Identity Provider” on their Okta org.
   This involves uploading your root certificate to Okta and configuring Routing Rules to define when login via PIV or smart card is required.

2. Once the smart card has been configured, end users will see the PIV Card option (screenshot below) when logging into Okta.



Sign In

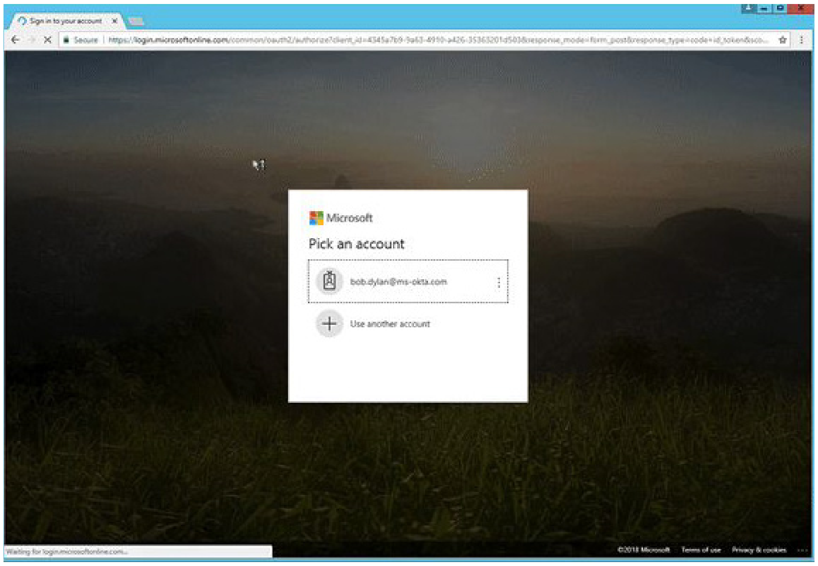
[redacted]

Password

☑ Remember me

Need help signing in?

3. The end user will be redirected to an Okta authentication screen where they can use PIV as the login credential. They choose the certificate stored on their PIV card, enter their PIN, and they're in—no username or password required.



https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&response_mode=form_post&response_type=code+id_token&sco...

Pick an account

bob.dylan@ms-okta.com

Waiting for login.microsoftonline.com...

Use case: Workforce Identity

Desktop Single Sign-On

With Desktop Single Sign-on (DSSO), users are automatically authenticated by Okta when they sign in to your Active Directory network on their device (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 in Okta works.

1. User enters their AD credentials on their desktop login page.
2. When accessing Okta via the browser, or a desktop thick client that supports modern authentication, the user will not be prompted for any additional credentials (unless MFA is required).

You may be wondering what the difference is between Desktop Single Sign-On and the Okta FastPass feature mentioned above. The benefit of Okta FastPass is that the device does not need to be Active Directory domain joined or on network for the passwordless experience, and Okta FastPass works across Windows, MacOS, iOS and Android.

Use case: Workforce Identity

Device Trust integrations (via SAML)

Device Trust is a feature in Okta which allows administrators to set access policies on managed vs. unmanaged devices. Most often, this means allowing access to Okta from managed devices, while prompting for MFA (at a minimum) or denying access from unmanaged devices. The term “managed” specifically refers to devices that are managed by an endpoint management solution, such as Jamf, VMware Workspace ONE, Microsoft Intune, etc.

Some solutions, such as VMware Workspace ONE, have built-in passwordless capabilities (frequently referred to as mobile single sign-on). Okta can integrate with these solutions to provide a frictionless access experience for end users. Here’s how Device Trust SAML integrations work.

1. Administrators utilize Okta’s IdP Discovery feature to route logins to the endpoint management solution.
   This requires that the endpoint management solution offers its own lightweight identity solution (e.g., VMware Workspace ONE, MobileIron Access).
2. The endpoint management tool will check if the device is managed.
   Based on whether the device is managed, Admins can configure policies to deny access, prompt for enrollment, allow access, or prompt for MFA.
3. On managed devices, users will not be prompted for any additional credentials—they are logged into the application seamlessly.

You can learn more about **Device Trust integrations on our blog**.

Use case: Workforce Identity

Email Magic Link

COMING SOON

Email-based passwordless authentication has become very common for consumer use cases. This method is, at its core, a password reset flow; a secret link is sent to the user that allows them to bypass their password and set a new one. It's familiar to most users because they've used it dozens or hundreds of times.

Apps like Slack and Medium have popularized this method of authentication. True passwordless authentication takes the password reset flow a step further. Here's how the Email Magic Link feature works.

1. User registers for or logs in to an app by just 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 and 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) and simply send a secret, time-limited or user-lifecycle limited, single-use link to the user's email address. Clicking that link authenticates the user and sets a cookie with a long lifetime to keep them logged in. The user never needs to set, save, or type any passwords at all, which is a very appealing feature, particularly on mobile devices. This method of passwordless authentication requires no hardware dependencies and is very attractive to consumer applications.

Use case: Customer Identity

Feature	Use case
Okta FastPass Device-based passwordless authentication for Windows, iOS, Android and MacOS, with no dependency on on-prem directories or a specific endpoint management tool	Workforce Identity
Factor Sequencing Defining a chain of factors, combined with user, device, and location context	Workforce Identity & Customer Identity
WebAuthn Phishing-proof, biometrics-based authentication using the FIDO2.0 standard	Workforce Identity & Customer Identity
PIV smart card Authentication via an x509 certificate, mostly used by US federal agencies	Workforce Identity
Desktop Single Sign-On Passwordless login for AD domain-joined machines	Workforce Identity
Device Trust Integrations tilize endpoint management solutions' mobile single sign-on features to deliver passwordless	Workforce Identity
Email Magic Link (coming soon) Email-based passwordless authentication best suited for consumer apps	Customer Identity

How Do I Learn More?

This whitepaper is an overview of the various passwordless capabilities in Okta. If you would like to learn more about deployment considerations for passwordless and the benefits and challenges associated with these features, see **Move Beyond Passwords.** If you would like to understand more abou how multi-factor authentication can help with the journey to passwordless, visit our **Okta Adaptive MFA web page.**

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 8,400 organizations, including JetBlue, Nordstrom, Slack, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to **okta.com**.