

Okta FastPass

Passwordless authentication with strong phishing resistance

Okta FastPass is a cryptographic multi-factor authenticator that enables secure passwordless authentication into anything you need to get your work done, on any device, from any location. Utilize Okta FastPass to minimize end-user friction with phishing-resistant factors and adaptive policy checks to securely access corporate resources.

Why use Okta FastPass?

A growing hybrid workforce and changing user preferences to access corporate resources from any device have made it increasingly difficult for enterprises to maintain security while minimizing friction. With Okta FastPass, you benefit from:



Passwordless Login Experience

Passwordless authentication to any SAML, OIDC, or WS-Fed app in Okta. Can be coupled with your choice of device management tool.



Enforcement of phishing resistant authentication flows

Protect from real-time credential phishing across different platforms.



Ensure the security of the devices in use

Integrate with any device management tool to enforce phishing resistant flows. Additionally, amplify the security of your unmanaged devices with Device Assurance using Okta Verify.



Combine with device-level biometrics

End-to-end (from login to app access) passwordless on devices which support biometrics (login to device with biometrics, no additional prompts when accessing Okta-managed apps).



Consistent user experience across all platforms and devices

Reduce user friction to improve productivity



Reduce IT spend

Eliminate passwords from the authentication flow to reduce IT helpdesk costs related to factor enrollment and reset

Supported use cases

Many organizations use a combination of different tools for device management, but the good news is that Okta FastPass can work alongside a wide range of use cases. Okta FastPass can be combined with the following deployments to check if a device is managed before delivering passwordless auth:



Windows devices that are Azure Active Directory joined/Hybrid AAD joined + EMM/MDM managed (VMware Workspace ONE, Microsoft Intune, System Center Configuration Manager, MobileIron, etc.)



AD joined Windows devices



MacOS devices managed by Jamf Pro or any other enterprise mobility management tool



Mobile devices (iOS, Android) managed by an EMM/MDM (Intune, VMware Workspace ONE, MobileIron, etc.)

...and many more!

Learn more at www.okta.com/passwordless-authentication.

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 16,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, and Teach for America, trust Okta to help protect the identities of their workforces and customers. For more information, go to [okta.com](https://www.okta.com).