okta

Okta Passwordless Authentication

Goodbye passwords and identity-driven attacks.
Hello, seamless experiences.

Identity attacks such as phishing, credential stuffing, brute-force-attacks, etc. are increasingly common and sophisticated methods for committing account takeovers. These attacks result in increased security risks, brand damage and outright fraud. Additionally, today's customer expects seamless access with minimal friction. Okta passwordless authentication keeps attackers at bay without locking out good users by tackling the crux of the problem - poor or compromised credentials.

Redefine the authentication journey with passwordless authentication

Security

Reduce or even eliminate a majority of password-based attacks.

User experience

Cut authentication time and deliver a seamless experience of up to 50%

TCO

Drive efficiency and create happy Support and IT organizations by reducing credential management costs

Passwordless options for every use-case

Email Magic Links

Simply click on a link embedded in a verified email to validate the request, and continue the login process. Ideal for passwordless authentication into applications that require infrequent authentication. Use email magic links to bootstrap users into higher assurance passwordless authentication methods such as WebAuthn or factor sequencing. Email magic links are easy-to-use, cost-effective and your time-to-market.

Factor sequencing

Factor sequencing allows you to authenticate using one or more high assurance factors. Dynamically alter the authentication experience by using factors like Okta Verify with Risk-based Authentication to remove the need for a second factor.

WebAuthn

WebAuthn is a standards-driven approach to passwordless authentication. Use authenticators like Yubikeys or TouchID to authenticate into your applications. Best of all, there is no back-and-forth credential sharing needed. Use WebAuthn to stop all password-based identity attacks and deliver a cost-effective, seamless authentication experience.

Passwordless with device trust

Okta's device trust integrates with leading endpoint management systems to deliver a passwordless login experience on desktop and mobile. When you utilize a Unified Endpoint Management (UEM) vendor that can integrate it's own identity capabilities into Okta, you are able to both enforce device security and deliver a seamless login experience for users. Explore device trust

Desktop single sign-on

Use passwordless authentication to login to Okta on machines joined on your Active Directory domain (Windows and macOS). Okta offers agent-based (using Okta IWA) or agentless (using cloud based Kerberos) approaches.

Login to machines with your Active Directory credentials → open an Okta managed app on browser or modern auth desktop apps → login with no username or password prompt. Explore desktop single sign-on - IWA and Agentless

PIV/Smart-card

Use PIV/Smart-cards (or any x509 supported cards) to authenticate in Okta or any apps integrated with Okta without passwords. PIV/Smart-card based authentication is ideal for customers in regulated industries (healthcare, banking) or governmental organizations. Explore PIV/Smart-cards

Visit the Product page or Product documentation to learn more about how Okta can provide a secure and frictionless experience for users, as well as a easy experience for product builders and administrators. Reach out to our product experts to learn more, and see how Okta can keep your service safe from identity-driven attacks and account takeovers.