okta

Okta Adaptive Multi-factor Authentication

Balance security and user-friction for your customer apps

Identity attacks such as phishing, credential stuffing, brute-force-attacks, etc. to commit account takeover are increasingly common and more sophisticated. These attacks result in increased security risks, brand damage and outright fraud. Additionally, today's customer expects seamless access with minimal friction. Okta Adaptive MFA allows good-users in while keeping attackers out. Use our contextual access policies to detect login anomalies and enforce strong authentication for your customer applications, only when necessary.

Why choose Okta Adaptive MFA for customer applications?

Risk-based authentication to identify abnormal login patterns

Okta uses a machine learning model to categorize anomalies as high, medium or low. Use risk-based auth to pair a risk level with the appropriate factor.

Okta ThreatInsights mitigates the impact of large scale identity attacks

Okta's network effect captures billions of logins across all orgs. With ThreatInsight, admins can block access from suspicious IPs pre-authentication, thereby preventing account takeover and account lockout for your customers, and consumers.

Choose the factors that best fit your organization

Okta offers a wide range of multi-factor auth methods out of the box, and also lets you use any SAML or OIDC auth provider as a factor. Use our factors to meet any assurance or compliance requirement.

Provide users with secure, passwordless options from any device

Remove passwords from the login experience. Okta's passwordless authentication platform eliminates a range of Identity attacks, improves customer experience and reduces support costs.

Quick Integration, Easy day-to-day management

Use Okta's widgets, SDKs, and RestAPIs to integrate quickly and reduce your time-to-market. Once integrated, Okta's admin dashboard makes day-to-day user management a breeze.

Okta AMFA — Adaptive Authentication

How your users access their data - and the risk associated with those methods-is constantly changing. Your security should be able to keep up. Okta Adaptive MFA allows for dynamic policy changes and step-up authentication in response to changes in user behavior including location, travel patterns, network, etc. Adaptive MFA supports detection and authentication challenges for riskier situations like:

- Use of weak/breached passwords
- Proxy and Tor usage
- Geographic location and zone changes
- Brute force and denial-of-service attacks
- New devices detection
- New IP address detection
- Threat data
- App data

Okta's ThreatInsight aggregates high-risk authentication attempts seen from across Okta's customer base and allows all of Okta's customers to pre-emptively block or step-up traffic from these high-risk locations.

Risk-based Authentication uses machine learning models that ingest authentication data to Identify login anomalies. Customers can use this analysis to dynamically alter the authentication experience(e.g force MFA), block or even remove friction for good users. Additionally, use this feature to reduce the authentication rules written and managed by admins.

Multi-Factor Authentication (MFA)

Different situations require different strategies for authentication and identity assurance. Not all factors are appropriate in every circumstance, and organizations typically want a variety of assurance levels. That's why Okta offers flexible support for standards like FIDO2.0 and a wide range of second factors including:

- SMS, Voice, and Email
- One-time passwords like Okta Verify and Verify Push and third-party solutions like Google Authenticator
- Biometric factors including Windows Hello and Apple Touch ID, Face ID
- Physical tokens including support for Yubikey tokens, Symantec VIP and RSA SecureID.

Managing factors should be as easy as possible. Okta's self-service factor reset capability allows end-users to reset and enroll into factors without having to divert resources from the support team. Additionally, for businesses that need to meet compliance mandates, Okta MFA helps you deploy and manage MFA without much effort.

Passwordless Authentication Platform

The rational to eliminate passwords from the authentication experience is endlessly compelling. Emerging passwordless security standards elevated consumer experience expectations, and ballooning support costs make this mission-critical. Okta's platform offers a number of passwordless authentication options for consumers including email credential links*, factor sequencing, and WebAuthN. Use just one-click or one-touch to give access to your application. Passwordless authentication using WebAuthN can offer strong protection against most identity-driven attacks as well as man-in-the-middle and man-in-the-browser attacks. By offering a range of passwordless options for your users you can securely onboarding users or provide access without hardware support.

*Available in H2'19

Seamless User Experiences

The enhanced security required to stop account takeovers shouldn't add friction to your users' experience.

- Okta gives you the option to eliminate passwords from the authentication experience. Use email credential links, standards-driven passwordless authentication like WebAuthn or factor sequencing,
- Combine Okta's adaptive authentication with MFA to intelligently detect high-risk logins and enforce a second factor only when necessary
- Okta allows you to deploy MFA downstream in your applications when the user performs critical actions on your platform including transfer money, make changes to personal information, etc.

Quick Integration, Easy Management

Adding security to your application should be easy and customizable. With support for all major programming languages and frameworks, Okta's prebuilt widgets and SDKs make adding security into your applications quick and easy.

Should you need a more customized experience, integrate directly with Okta's Restful APIs. Our detailed API documentation, user forums, and support engineers provide product builders with all the support they need to add security layers to their application. Adding MFA is just the start. Okta makes managing users and application security simple. Okta's admin and user dashboard allows users, security teams, and support teams to quickly manage the factor experience, monitor suspicious activity, and enforce security measures as necessary. Okta's reporting dashboard provides security teams with all the details they need within the admin console. The Syslog API allows you to get a real-time feed of login events into your internal systems. Pre-built integration with all major SIEMS ensures your SOC team can construct a complete picture of the risks involved.

Visit the API product page or Product documentation to learn more about how Okta can provide a secure and frictionless experience for users, as well as a manageable 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 account takeovers.