Okta Adaptive Multi-Factor Authentication

okta

Security for all your apps

The increase and ease by which attackers can steal credentials through social engineering and phishing means all applications should be secured, not just "critical apps." Okta Adaptive Multi-Factor Authentication (MFA) provides the additional security to protect organizations from data breaches while offering administrators and end users the simplicity to stay productive. Leveraging device and user context through an adaptive, risk-based approach, Okta Adaptive MFA also integrates with the applications and infrastructure you're already using to make deployment that much easier.

Benefits and Features



Secure authentication for all environments

Okta Adaptive MFA protects identity and access to data wherever your users go and wherever your data lives. Built for rapid expansion with the cloud, Okta's MFA solution can also support your on-premises needs for VPN, RDP, and SSH. Hybrid environments and mobile users are also covered so access to apps and data is always secured.

Comprehensive second factors and assurance levels

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—levels of proof that a user is who they say they are—based on security needs. For example, SMS as a second factor may not be ideal for users in areas with poor cell phone reception. And one-time passwords may be acceptable for most users, but admins with access to internal databases may require crypto-based physical tokens for extra assurance. That's why Okta gives you complete flexibility with support for a full range of second factors spanning all assurance levels including:

SMS, Voice, and Email

One-time passwords, like Okta Verify and Verify Push, and third-party solutions, like Google Authenticator and Duo

Physical tokens including support for RSA, Symantec, and Yubikey tokens

Biometric factors including Windows Hello and Apple Touch ID

With Okta, you never have to choose between security and the usability end users want.

Adaptive and risk-based capabilities

User and risk levels are always 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 and device behavior, location, or other contexts. Adaptive MFA supports detection and authentication challenges for riskier situations like:

- Use of weak/breached passwords
- Proxy use
- Geographic location and zone changes
- Brute force and denial-of-service attacks
- Use of new/untrusted devices
- Indications of anomalous behavior

Fully integrates with your organization

Okta integrates with thousands of web apps through standards-based protocols and can centrally enforce MFA across all of them. And Okta's RADIUS Agent extends MFA to even more devices. For those who want even more flexibility, customer app integrations are also possible through Okta's API.

Beyond your business apps, Okta supports integrations with other security tools like SIEMs, CASBs, and network security devices so you can enhance your existing security investments with authentication data and full visibility.

About Okta.

Okta is the foundation for secure connections between people and technology. Our IT products uniquely use identity information to grant people access to applications on any device at any time, while still enforcing strong security protections. Our platform securely connects companies to their customers and partners. Today, thousands of organizations trust Okta to help them fulfill their missions as quickly as possible.