

Adaptive Multi-Factor Authentication

The right balance of intelligent, secure access and user experience

Workforce users require secure access to the apps and tools they depend on, anytime and from any device, regardless of location. However, one thing is clear: traditional MFA is not enough. Not only are users frustrated with repeated authentication prompts, but MFA alone lacks the visibility and reach to protect the enterprise.

Okta's Adaptive Multi-Factor Authentication (Adaptive MFA) provides a contextual access approach to enforcing security. This approach considers how your users access their resources—and the risks associated—are constantly changing, allowing for dynamic policy enforcement and step-up authentication only when there are changes in user behavior, device posture, location, and other contextual insights.

Why choose Adaptive MFA?

Dynamic, contextual access control

Multi-factor authentication isn't great when all you can enforce is a basic "yes" or "no." Okta supports step-up authentication when it makes sense based on context and other login characteristics, including signals from integrated endpoint security tools.

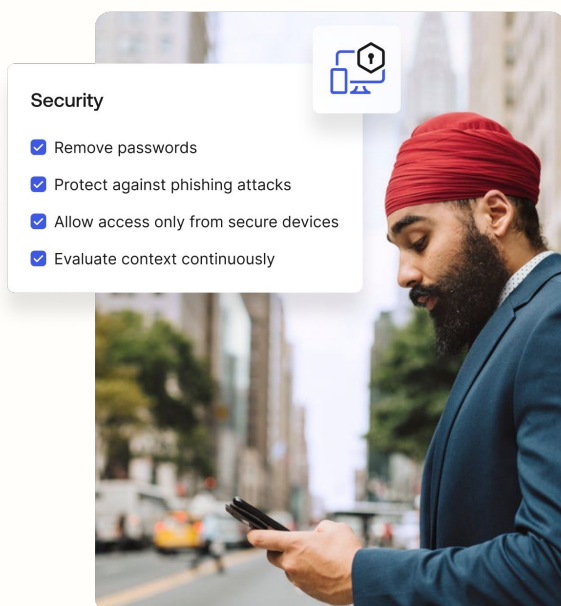
Adaptive MFA enforces additional authentication challenges for riskier situations such as:

- Location & network zone changes, including proxy use
- Brute force & denial-of-service attacks
- Changes to device posture & management state
- Indications of other anomalous behaviors (e.g., impossible travel)

Passwordless, phishing-resistant authentication

Adaptive MFA helps protect your organization against phishing attacks with support for a range of phishing-resistant policies and factors, such as Okta FastPass, FIDO2 (WebAuthn) authenticators, and PIV/CAC smart cards. These authenticators provide high levels of security assurance while eliminating passwords as a sufficient means for app access. By leveraging more secure authenticators such as those supporting biometric authentication, you can also reduce user login friction.

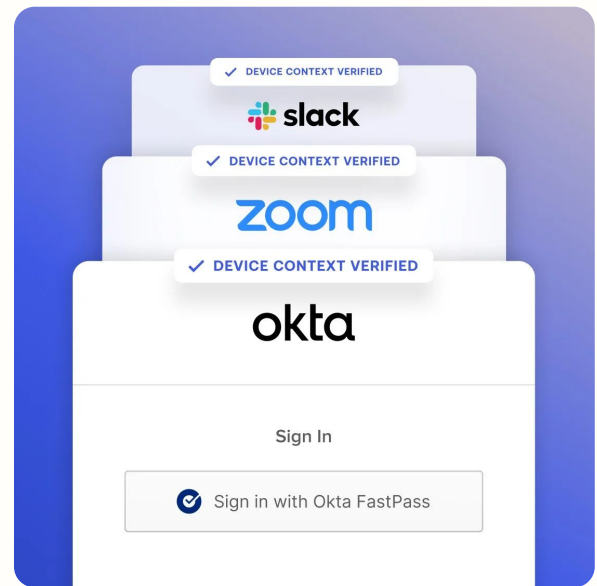
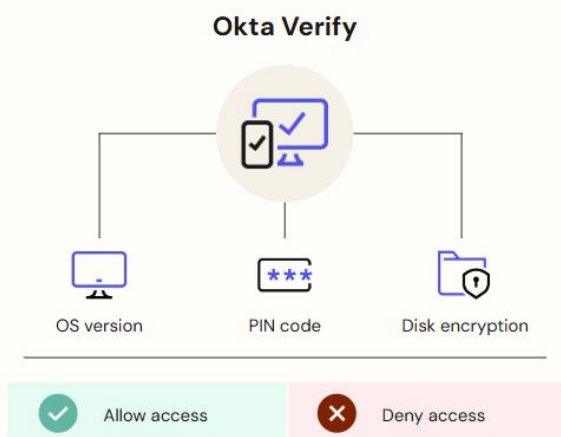
With Okta's self-service factor support, users can enroll and recover factors and authenticators without burdening the support team.



Device Assurance for Zero Trust security

With Adaptive MFA, you can leverage Okta Verify and FastPass not only for authentication, but for device assurance. Admins can configure Device Assurance policies or sets of security-related device attributes to be evaluated during authentication. For example, a Device Assurance policy can be used to ensure a specific operating system version or security patch is installed before that device can be used to access Okta-protected resources. If a user is not in compliance with a required device attribute or setting, the Okta Sign-in Widget provides them with self-service remediation instructions that can be customized to your organization's needs.

Device Assurance is an extensible device compliance solution that empowers you to tailor compliance checks that meet your unique security needs for managed and unmanaged devices. Admins can create custom checks to reinforce MDM policies and drive compliance for devices before allowing access to downstream resources.



Key features include:



Assess devices against predefined policies—collecting device signals in real time when starting a new session, opening a new app, or for continuous risk assessment with Identity Threat Protection—so that only secure, compliant devices have access



Enhance the security of unmanaged devices by driving more extensive evaluation and proactive nudges to improve device posture even in the absence of MDM enrollment



Enable end users to self-remediate with custom, detailed guidance on why access was denied and how to swiftly bring their devices into compliance to unblock access without burdening IT admins

Learn more about Adaptive MFA at okta.com/products/adaptive-multi-factor-authentication

About Okta

Okta, Inc. is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success. Learn why the world's leading brands trust Okta at okta.com.