okta

What Is Multi-Factor or Two-Factor Authentication?

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

What Is Multi-Factor or Two-Factor Authentication?

Introduction

Passwords aren't good enough.

Securing your enterprise can seem like a daunting task. In the past, companies were comfortable with the standard username- and password-based authentication to all apps and services, with no additional methods of authentication or authorization. Access to corporate resources was protected by firewalls and VPNs.

Here's the thing, not only are passwords not good enough, they're actually pretty terrible. As we saw in this year's Businesses at Work report they're hard to remember, and in an effort to enforce "secure" passwords, admins default to implementing daunting password complexity rules—we can all relate to the 16 character, special symbols, lower case/upper case password requirements mandated by IT. Even with these password controls, companies consistently see passwords like "$ecuremy@ccount!123" or "Th!sisMyP@ssword01!" used across all corporate apps and devices assigned to end users. Even worse, end users tend to use these same passwords for consumer applications as well.

Using passwords as the single and only form of authentication enables bad actors to easily spoof a user's identity. You've probably heard of the term "phishing"—a cyber attack most commonly launched via email, where bad actors send what looks to be a legitimate email that informs the user to log in to accounts such as banking or corporate accounts. At first glance, these emails look scary, as they may claim that your account will be "cancelled" or "deleted" if no action is taken, or sometimes even falsely state that your password has already been compromised, and therefore you need to log back in and change it again to keep your account secure. Unknowingly, many of us fall for this trick, and before you know it, you've clicked on an email, entered your password into a malicious form and exposed your password to hackers. Now that the hackers have your password, they're able to log in to applications instantly if there is no requirement for a second factor of authentication.

It's critical that access to your corporate resources should be difficult for hackers, but seamless and secure for your end users. This is where multi-factor authentication helps.

Two-Factor Authentication

You've probably noticed that consumer applications like Gmail, Facebook, Twitter and others introduced the concept of two-factor authentication (or 2FA). Sometimes this is referred to as two-step verification.

With 2FA enabled, end users are required to provide two forms of identity verification before accessing the application. In most cases, this includes a password and a form of authentication on a user's mobile device—SMS is the most common. After both the factors are verified and confirmed against that specific user account, the user has access to the application. We see this in enterprise scenarios as well, where an

end user is sent an SMS code valid for a specific number of minutes to be entered into the application they are accessing.

Two-factor authentication provides an additional layer of security in protecting your access to applications. There's no arguing that 2FA is more secure than a single factor like a password. With 2FA enabled, an attacker would need to identify both your password and determine how to spoof your second factor in order to impersonate your identity and gain access to applications.

So, what's the difference between 2FA and MFA?

Multi-Factor Authentication

You may be wondering how you can authenticate to an application via your mobile device if you've lost your phone, or if you're traveling and do not have internet access. Your second factor does not necessarily need to be your mobile device—in both consumer and enterprise scenarios, we see a variety of second factors such as Yubikey, U2F, or biometric factors like Windows Hello and TouchID. This is where the concept of multi-factor authentication (or MFA) comes into play.

Multi-factor authentication is most often presented as a combination of what you know, what you have, and what you are. 2FA is just a subset of multi-factor authentication—with multi-factor authentication enabled, users need to provide their password and a second factor as defined by the administrator. Multi-factor authentication grants you access to your corporate applications based on multiple data points and factors derived from an end user's login attempt.

While it seems like MFA is the easy answer to enforce security across the enterprise, many companies continue to put off their multi-factor authentication deployment to avoid disrupting end users. However, when combining multi-factor authentication with a solution that provides a flexible policy and contextual access engine, you can ensure that end-user productivity is not compromised.

Adaptive Multi-Factor Authentication

An adaptive authentication solution provides you with multi-factor authentication in addition to the flexibility to determine when an MFA policy needs to be enforced. This means that admins have full control over when and where MFA is required, and who needs to provide MFA. Even better, admins can choose which types of factors are best fit for various personas in your organization. For example, executives have access to especially sensitive data, and therefore, a stronger authentication method like Yubikey or biometric authentication may be a better fit. On the other hand, contractors and interns may not have access to sensitive information, and may not stay at the company long-term, and therefore authentication methods like SMS or an authenticator app could make more sense, as those are intuitive and easy to use.

Okta's Adaptive Multi-Factor Authentication integrates with your company's applications and resources—each time a user logs into an app managed by Okta, we are able to analyze that login request, and determine how to grant (or deny) access.

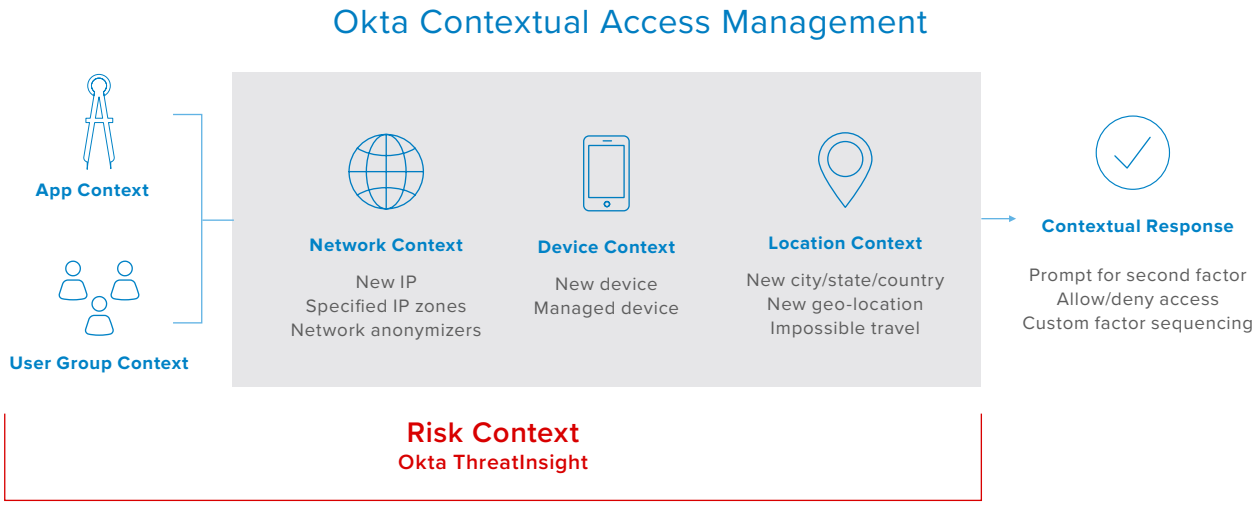
For example, if you have an employee that usually logs into Okta from the same laptop and the same

network location on a daily basis, but one day logs in from a brand new device and location, Okta can take various actions based on that login. First, Okta's behavioral detection engine can identify the new device, location and IP addresses accessing the Okta service, and prompt for step up (or MFA) on that new login. Additionally, when an end user logs in from a new device, they are sent an email with identifying information, such as browser, OS, login date/time and network location. This helps end users themselves manage secure access to their account—if they get an email identifying a login that they did not initiate, they can then notify their Okta administrator.

Ultimately, it's important to evaluate risk context for each login to make an access decision. At Oktane18, we announced Okta ThreatInsight. Okta ThreatInsight is the first step to delivering a solution that acts as an input to assign risk scores to individual user logins to Okta. Customers get the benefit of a network effect since we analyze suspicious activity across all customers.

With Okta's Adaptive MFA, there's a wide spectrum of possibilities—MFA based on changes in login pattern (behavior detection), proxy detection, geolocation, and more. Additionally, you can create policies such that only managed or known devices can be authenticated into these apps, whether they are on-premise or in the cloud.

As companies make a shift towards the cloud, it's essential to consider how you can modernize your approach to security. Security breaches and attacks continue to become more commonplace, and therefore strong authentication is essential. Okta makes it simple to secure your environment by addressing common points of vulnerability, and we see Adaptive MFA as the first step to a full security solution. Interested in learning more? Check out our AMFA product page, or sign up for a free trial.



About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at: www.okta.com


okta