okta

7 Things to Consider Before Making the Switch to MFA

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

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

7 Things to Consider Before Making the Switch to MFA

Passwords are hard. The (what feels like constantly) growing list of security requirements are intended to make passwords secure, but in many cases they've had the opposite effect. Complex passwords that meet all the requirements are often difficult to remember, so they're reused across many sites. Users scribble them on sticky notes. They weave in easily discoverable pet's names, birthdays, and phone numbers. It's no way to keep data secure. Thankfully, organizations are starting to not just understand, but also support the concept that while access should be hard for hackers, it needs to be easy for legitimate users. And the best way to make that happen is with multi-factor authentication, or MFA.

MFA is a great way to secure your users' apps and services from unauthorized access. Here are some points to consider as you plan your deployment.

1. User education

You're deploying multi-factor authentication to reduce security risks from password-only access, but some users may see this as an inconvenience. They may be worried that this process change will take up time they feel could be better spent elsewhere.

Nonetheless, make sure everyone from management to end users are aligned on why you're making the shift to MFA. It is important to achieve buy-in from form the entire organization to ensure everyone plays a role in keeping the company secure. Do this through education, so each user can appreciate the security benefits they contribute to by taking this additional step.

2. Consider your MFA policies

A good MFA practice deployment will balance security with usability to avoid becoming too onerous, so consider how you define your MFA policies to govern how and when an additional factor is required.

It may seem a bit counter-intuitive, but sometimes the key is to prompt for step-up authentication less often instead of more. A well-considered risk-based policy configuration should trigger step-up authentication challenges only when necessary.

For example, a policy could ensure that a second factor is required only when logging in to a service from outside the corporate network (based on a range of IP addresses) or outside of the country (based on a GeoIP location lookup). Or maybe you have a certain group of user accounts with broad access to sensitive data, and you need a stricter policy for them. MFA allows you to require a second factor when they attempt to access the sensitive resource, but not, say, when they access the company events calendar. The basic idea is that additional verification should be as transparent as possible to the user to foster a good user experience without compromising on security.

3. Provide for a variety of access needs

There are scenarios where a user has Internet access, but has little or no service from their cell phone carrier. This could be on a wifi-enabled airplane, at a rural home, or simply in the basement of a large concrete building. In these cases, where voice and SMS may not be feasible, Okta Verify with push or one-time password (OTP) are better choices, as their communication is encrypted over the phone's Internet connection.

Hardware devices that generate event-based or time-based one-time passwords (TOTP) don't require a communication channel at all. They are also more difficult to tamper with or copy. But along with the cost to deploy, a physical device becomes one more thing for employees to carry around, forget at home, or lose. Thus, they may not be the go-to choice for short-term contractors or in situations where there is substantial churn in workers.

When it comes to MFA factors, a lot of options exist to solve for a wide variety of scenarios. Choose what works best for each scenario in your organization, keeping in mind multiple policies and factors can be used when there isn't (and there hardly ever is!) a one-size-fits-all solution to accommodate all situations.

4. Think twice about using SMS for OTP

SMS is easy, and with the prevalence of cell phones and tablets, it's nearly everywhere, so it has become a common communications channel for OTP delivery. SMS has generally been assumed to be secure enough for this purpose, but that is due in part to the fact that the infrastructure is mostly both proprietary and opaque.

Research shows that SMS security is lacking, and not only when it comes to documented vulnerabilities. With SMS, you are trusting security to the telecom companies, and even if you trust that they have security best practices in place, there is always a risk of compromise through spoofing and social engineering. In many cases, it's not that technically challenging for an attacker to port your number to a device they control, and gain access to your SMS messages and OTPs.

While NIST recommends against using SMS for these reasons, ultimately you need to perform your own risk assessment based on your users, use cases, and the data being secured. After all, MFA with SMS is still better than no MFA at all.

5. Check compliance requirements carefully

Most IT compliance standards such as PCI DSS, SOX, and HIPAA mandate strong user authentication controls, making them likely motivators for an MFA deployment. It seems obvious, but if your goal is to meet such standards, make sure to have a detailed understanding of the requirements so you can tailor configuration and policies to them.

For example, PCI and HIPAA compliance both require strong authentication, which is at least two strong authentication methods out of these three: something you know, something you have, and something you are. And SOX focuses less on technology—but to pass an audit, you'll still need to prove that your organization's finance and accounting data is secure.

IT compliance requires implementing relevant standards, but it also requires an ability to prove that you've met them. Make documentation part of your configuration and implementation so you'll be able to quickly and confidently prove in an audit that they've been met. Your future self (and your org!) will thank you.

6. Have a plan for lost devices

The second authentication factor type in a typical MFA deployment is "something you have" (the first being "something you know" and third being "something you are"). In the case of SMS, voice, or an authentication app like Okta Verify or Google Authenticator, the user has their phone. In the case of a hardware token from YubiKey, RSA, or similar, the user has their token. But anything a user has, a user can lose.

A procedure for handling lost devices should already be part of your comprehensive IT helpdesk playbook. Extend it to include devices used for MFA, and ensure that reporting a lost device results in:

- Expiring any current sessions and requesting the user re-authenticate
- Disassociating the device from the user's account and access rights
- Remote wiping of corporate information on mobile devices, if necessary

It's also important to audit the user account's activity prior to the point in time when the device was lost to note any unusual activity. If there is anything suspicious, consider the possibility of a breach and escalate accordingly.

Once the immediate security concerns are handled, focus should shift to getting the employee back to work with a replacement device or login method. For example, an alternative process like calling the IT helpdesk to verify identity requirements can allow the employee to be productive while replacement factors are implemented.

7. Be prepared to review and revise

It's rare that complex deployments and policies are a perfect fit the first time. With a process change that can potentially affect all employees, it's always a good idea to track the effectiveness of an MFA solution as it is being deployed and used and be able to refine policies based on observations.

Get comfortable with the auditing functionality early in the process and it will be invaluable for troubleshooting and adjusting policy configuration. Once you've deployed MFA to users, use auditing tools to spot check adoption and use. A mechanism that allows user feedback to be reported can also be a good idea.

And while users may not always take the time to provide written feedback, an audit trail gives you some visibility into what they actually experienced. Did it take them three tries to enter their OTP? Did they give up? Problems like this could indicate a misconfiguration, a gap in user education, or simply a scenario that wasn't considered in the initial rollout plan.

Using audit tools and encouraging employee feedback assures all stakeholders that the system is working as intended and new security policies are being successfully adopted.

Bonus: Consider Adaptive MFA

These tips are a great start, and step-up MFA can even allow fine-grained control over how and when MFA is applied, but it requires careful consideration to configure. In some cases, even for well-defined policies and criteria, you may want to be able to make decisions on-the-fly based on changes to user or device context.

To take advantage of the ability to make dynamic changes, check out Okta's Adaptive MFA solution. Adaptive MFA works by noting access patterns and then adapting the policy around each user or group.

For example, an employee who routinely travels and checks email from overseas may only periodically require a second authentication factor, but an employee who never travels would immediately receive an MFA challenge should they do so. Risk-based policies, like prompting for a step-up authentication challenge when trying to access resources through an unauthorized proxy or automatically blocking access from known malicious IPs can also kick in when triggered by suspicious events.

Adaptive MFA is a powerful tool to automatically derive dynamic policies over time—ones that are tight enough to give you the security your organization requires, but flexible enough to treat your users as individuals.