

8 Steps for Effectively Deploying MFA



Table of Contents

The value of MFA	3
1. Educate your users	4
2. Consider your MFA policies	5
3. Plan and provide for a variety of access needs	7
4. Think twice about using SMS for OTP	10
5. Check compliance requirements carefully	11
6. Plan for lost devices	12
7. Plan to deploy MFA to remote workers	14
8. Phase your deployment: Be prepared to review and revise	16

The value of MFA

[Multi-factor authentication \(MFA\)](#) has never been more important. With the growing number of data breaches and cybersecurity threats—and the steep financial and reputational costs that come with them—organizations need to prioritize MFA deployment for their workforce and customers alike. Not doing so could spell disaster; an invitation for bad actors to compromise accounts and breach your systems.

Adopting modern MFA means implementing a secure, simple, and context-aware solution that ensures that only the right people have access to the right resources. It adds a layer of security, giving your security team, your employees, and your customers peace of mind. Unfortunately, while the benefits are clear, implementing MFA can be a complex project.

In our [Multi-factor Authentication Deployment Guide](#), we've outlined eight steps that you can take to better enable your MFA deployment:

- ✓ Educate your users
- ✓ Consider your MFA policies
- ✓ Plan and provide for a variety of access needs
- ✓ Think twice about using SMS for OTP
- ✓ Check compliance requirements carefully
- ✓ Plan for lost devices
- ✓ Plan to deploy MFA to remote workers
- ✓ Phase your deployment: be prepared to review and revise

In this eBook, we'll take a deeper dive into each of these elements, giving you tactical advice and best practices for how to implement each step as you get ready to roll out Okta MFA.

1. Educate your users

As you get ready to deploy MFA across your organization, you may receive pushback from users that view this security feature as an inconvenience. To get ahead of this feedback, it's important to be proactive and transparent about the changes you have planned—especially any potential impacts to user experience. We recommend doing a combination of the following:

a. Use email communication

This will likely be the most effective method for keeping users informed and educating them around MFA. At Okta, we've developed a set of [end-user training materials](#) specific to MFA, which are available for sharing with your colleagues.

b. Allow employees to reach out to IT via a messaging app

Modern workforce messaging apps allow you to create company-wide groups so that employees can exchange ideas and ask for help. On Slack, for example, you can create a channel and dedicate it to a specific topic. Consider creating a group that allows your employees to ask IT team members for help during and after your MFA rollout.

Having buy-in across the organization is vital to the success of a new feature. Ensure that your employees understand how they can help better secure your organization by enabling MFA on their account. Ultimately, they can play a key role in keeping your company safe.

2. Consider your MFA policies

Before you roll out MFA, you'll have the opportunity to set policies that make sense for your workforce. For instance, instead of having users constantly interrupted and prompted for a second factor, you can define MFA policies that account for the risk associated with each login event.

The types of policies you deploy will vary depending on your industry or the sensitivity of the data your users have access to. In some cases—like at a financial institution—it may be necessary to prompt users for MFA every couple of hours. In others, users may only need to authenticate via MFA when accessing critical applications.

To help guide your policy decisions, we've developed some general guidelines:

Prompt users for MFA every eight to 12 hours

To ensure [high assurance](#) sessions, consider setting the session time in Okta to between eight to 12 hours and prompt users for MFA when the session expires. While this may seem rigorous, it's important that your MFA solution is able to continually validate that users are who they say they are when logging in.

Setting up session-based MFA policies in Okta

In the admin console, go to **Security > Authentication > Sign-On**. When editing individual rules, you'll see an option for **Session Lifetime**.

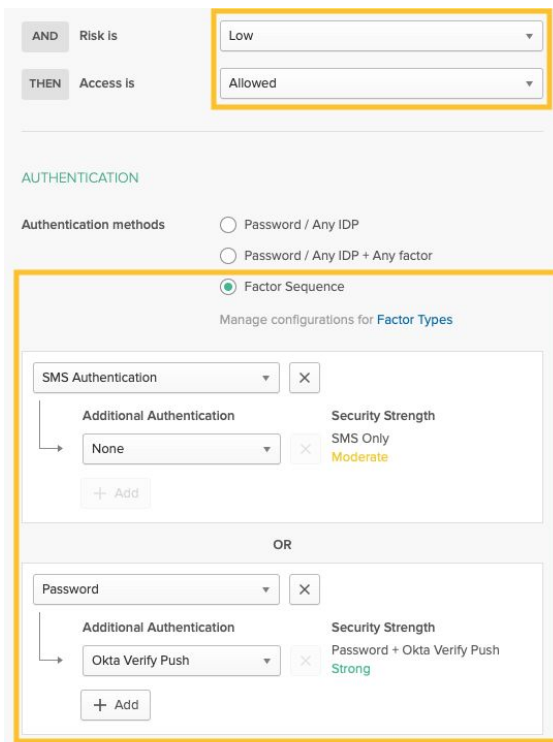
The screenshot displays the 'AUTHENTICATION' configuration page in the Okta admin console. Under 'Authentication methods', the 'Factor Sequence' option is selected. Below this, there is a configuration for 'FIDO2 (WebAuthn)' with 'Additional Authentication' set to 'None' and 'Security Strength' set to 'FIDO2 Only Strong'. A '+ Add' button is visible below the configuration. At the bottom of the page, the 'SESSION LIFETIME' section is highlighted with a yellow border, showing 'Session expires after' set to '8' hours.

Combine Risk-Based Authentication with your factor choice

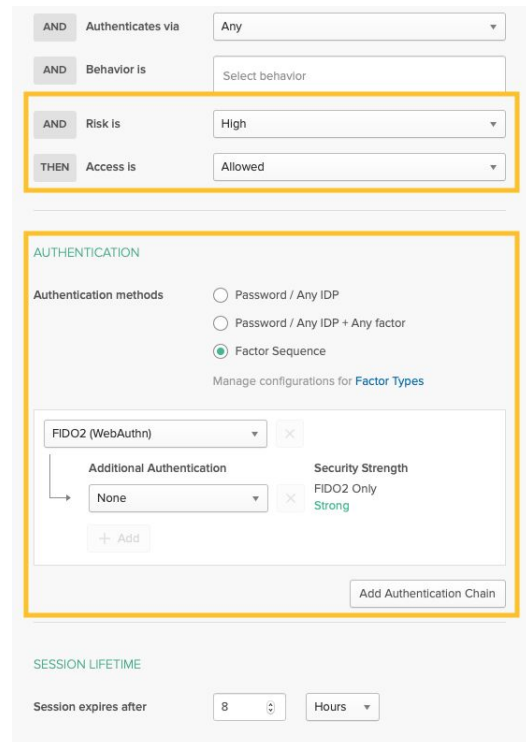
While you should consider enforcing MFA on every login, in some cases you may be comfortable with less secure factors for low-risk logins. This can be done with [Risk-Based Authentication](#). In these low-risk instances, you could require a password and SMS OTP. Meanwhile, in medium-risk logins, requiring a stronger factor like Okta Verify Push or WebAuthn is preferred. These stronger factors will also help you set a great foundation to eventually go passwordless.

Combine Risk-Based Authentication with a specific factor type in Okta

In the Okta admin console, go to Security > Authentication > Sign-On.



If the risk is low: use SMS OTP OR Password + Okta Verify Push.



If risk is high, only allow WebAuthn.

Bonus deployment tip for Risk-Based Authentication

If you'd like to test Risk-based Authentication and track entries in Syslog using a phased approach, but do not want to impact the end user experience when modifying policies, try the following:

- Choose the “high”, “medium”, or “low” options in the drop down, but do not modify any other policy settings
- You can do this for each rule within your sign-on policies, or add new rules with the risk level settings that mock the existing end user experience

You can choose to do this for a subset of users initially to track the “high”, “medium”, “low” Syslog entries, without modifying end user experience based on the risk level. When ready, you can modify the policy rules to also change the access response based on risk level.

3. Plan and provide for a variety of access needs

It's important that you plan your MFA deployment to support a range of factor needs. Different user groups may require different factor options. We suggest the following breakdown:

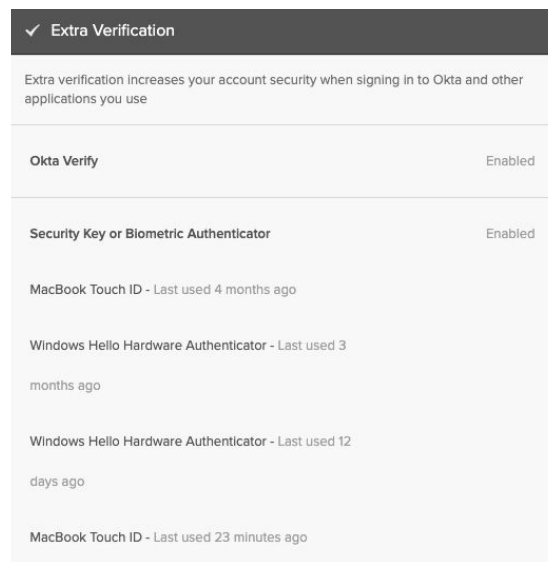
Group	Factors
Most full time employees	<ul style="list-style-type: none">Daily login using their password and Okta Verify Push or WebAuthnWhen they do not have internet access on their mobile phone, use WebAuthn on their laptop
Executives with access to sensitive data	<ul style="list-style-type: none">WebAuthn
Partners accessing resources in your Okta tenant	<ul style="list-style-type: none">Okta Verify OTP
Call center employees that cannot bring their phones	<ul style="list-style-type: none">WebAuthn using on-device authenticators like Mac Touch ID or Windows Hello (e.g., in scenarios where users are assigned to a single machine)
Temporary interns or contractors	<ul style="list-style-type: none">Daily login using their password and Okta Verify PushSMS OTP as a backup

Thankfully, there are a variety of factor options available in Okta, and using MFA you can enable specific factor types for different groups. Here are some MFA deployment tips:

WebAuthn allows you to enroll multiple devices

When you have WebAuthn enabled in Okta, users can enroll up to five devices on their account. If the user misplaces a device, they can use another WebAuthn device as a backup. For example, here's what an individual's account at Okta might look like ("Security Key or Biometric Authenticator" is the WebAuthn factor type):

You'll also notice we don't allow SMS OTP as a factor.



Enable Okta Verify OTP for partners

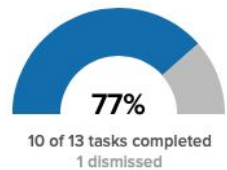
Okta Verify OTP is a free factor available to all customers and increases the fidelity of partner logins.

Utilize Okta HealthInsight to help you identify where weak factors are enabled







If you are already a long-time user of Okta's MFA products, you may already have a number of factor enrollment policies that are hard to keep track of. Okta HealthInsight is available to all of our customers and helps easily identify which policies allow for weak factor types. You can find Okta HealthInsight in your admin console under **Security > HealthInsight**.

HealthInsight

These are recommendations based on a live audit of the security settings of your organization. [Read more](#)



Incomplete Complete Dismissed

Issue	Security Impact	Actions	Dismiss
 Weaker Factors are set in 2 policies	High	Go to Multifactor	
<p>Okta recommends reviewing the enrollment policy and disabling Security Question, SMS, Email and Voice factors. Strong factors like Okta Verify, WebAuthn, or Google Authenticator have better resistance to phishing and man-in-the-middle attacks. Learn how to enable strong factors instead</p> <ul style="list-style-type: none">MFA enrollment has SMS/Email/Voice enabled as a factor.Default Policy has SMS/Email/Voice enabled as a factor.			
 SAML authentication supported but disabled for 3 apps	High	Go to SAML Report	
 Password Policies for 3 policies are weak.	Moderate	Go to Auth Policies	

Bonus deployment tip to secure accounts

Enable Okta ThreatInsight. This tool detects suspicious IPs accessing your org and proactively blocks those IPs before the authentication process, helping to prevent both account lockouts and account takeovers. To learn more, read our [Okta ThreatInsight whitepaper](#).

Ensure users have a backup factor available

When your users are able to easily reset their factors and use an alternate factor in case their primary becomes unavailable, your IT helpdesk will thank you. Your users will also appreciate that they can get quickly up and running on their own.

Choose factors for your user groups in Okta

Change your factor enrollment policies in the Okta admin console, under **Security > Multi-factor > Factor Enrollment**.

Factor Types | Factor Enrollment

Add Multifactor Policy

1 MFA enrollment

2 MFA enrollment policy for ev...

3 Default Policy

MFA enrollment Active Edit Delete

Description: Enroll users to MFA

Assigned to groups: **Everyone** ← Define your groups here

Eligible Factors

Factor	Status
<input checked="" type="checkbox"/> Okta Verify	Required
<input checked="" type="checkbox"/> Okta Verify with Push	
<input type="checkbox"/> SMS Authentication	Optional
<input type="checkbox"/> Email Authentication	Disabled
<input type="checkbox"/> Voice Call Authentication	Optional
<input type="checkbox"/> Duo Security	Disabled
<input type="checkbox"/> Security Question	Disabled
<input type="checkbox"/> FIDO2 (WebAuthn)	Required

SETTINGS FOR REQUIRED FACTORS

Enrollment grace period: None

Add Rule

Priority	Rule Name	Status	Actions
1	Prompt for MFA enrollment	Active	Info Edit Delete

Bonus deployment tip for managing MFA and sign on policies

Edit Rule

Rule Name: Prompt for MFA enrollment

Exclude Users: Teju Shyamsundar (teju.shyamsundar@okta.com)

IF User's IP is: Anywhere

AND User is accessing: Okta, Applications

THEN Enroll in multi-factor: the first time a user signs in

Update Rule | Cancel

Factor enrollment rule

Edit Rule

Rule Name: MFA for Super Admins

Exclude Users: Teju Shyamsundar (teju.shyamsundar@okta.com)

IF User's IP is: Anywhere

AND Authenticates via: Any

AND Behavior is: Select behavior

THEN Access is: Allowed

AUTHENTICATION

Authentication methods: Password / Any IDP, Password / Any IDP + Any factor, Factor Sequence

Additional Authentication: Password | Security Strength

Update Rule | Cancel

Sign-on rule

4. Think twice about using SMS for OTP

SMS is familiar to your users and easy to rollout as a factor. With the prevalence of cell phones and tablets, it's easily accessible and has become a common communications channel for OTP delivery. Up until recently, SMS has generally been assumed to be "secure enough" for this purpose. Now, SMS has proven to be an insecure method for securing access to accounts. Common issues include SIM swapping or hacking, lost devices, and social engineering attacks like phishing.

Instead of using SMS for your OTP purposes, we suggest that you replace it with more secure factor types like Okta Verify Push or WebAuthn. Here are a couple of tips for removing SMS OTP.

Utilize the MFA usage report

You can utilize the MFA usage report to understand which users continue to log into Okta using SMS OTP. This report will include the enrollment date as well as the last used date for every user. The report can be downloaded as a CSV to further analyze MFA usage. It's available under **Reports > Multi-factor Authentication**.

Enable WebAuthn in your org

You can start by enabling WebAuthn as an optional factor type, and communicate this to your users via email so that they know it's available. Hardware support for WebAuthn includes the following:

Off-device/roaming authenticators

These are WebAuthn-supported factors that are not built into the hardware (computer/phone).

- [Yubikey 5Ci](#)
- [Feitian BioPass](#)
- [HID Crescendo smart card](#)

On-device authenticators/platform authenticators

These are WebAuthn-supported factors that are built into the hardware (computer/phone).

- Windows Hello on Windows 10 1903 and later
- Touch ID on MacBook
- Fingerprint on Android 7.0+

Support for WebAuthn is dependent on the web app updating their authentication process to support the WebAuthn API, browser support, OS support, and hardware support. This may seem overwhelming, but thankfully, many operating systems, devices, and browsers already support WebAuthn. While consumer apps are still in the process of adopting this standard, if you're using an enterprise-grade authentication provider like Okta to secure access for the workforce, it's likely you'll be able to use WebAuthn with that provider.

5. Check compliance requirements carefully

IT compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX), and the Health Information Portability and Accountability Act (HIPAA) mandate strong user authentication controls. These standards are usually strong motivators for an MFA deployment.

If you do have compliance requirements to meet, ensure you have a detailed understanding of what they entail so that you can correctly tailor configuration policies to them. We suggest taking the following steps:

Make documentation a required part of your implementation process

PCI and HIPAA require strong authentication, with at least two authentication methods out of these three categories:

- Something you know
- Something you have
- Something you are

By requiring Okta MFA, you can meet these requirements. While SOX is less focused on the technology itself, you will still need to prove your organization's financial data is secure in order to pass their audit. Ensure that you have documented your configuration for others to reference in the future in case of any changes in requirements.

Learn about how Okta can help you meet compliance requirements

At Okta, we've done a lot of work to ensure that our platform meets various requirements from different regulations, and in some cases our customers can inherit compliance with certain elements.

Okta's [HIPAA Compliant](#) cell is specifically designed to meet HIPAA requirements for service providers. From end-to-end encryption of data to dedicated hardware, Okta enables organizations to manage employee, vendor, and patient identities with a single, secure solution.

Okta can also help you comply with [PCI DSS 3.2](#), an information security standard for organizations that store, process, or transmit credit card data. Among other controls, this standard requires strong MFA to authenticate access to servers and software handling credit card data, strong encryption, and the ability to ensure that only authorized employees have access to credit card data.

Okta's [Universal Directory](#), [Lifecycle Management](#), and [Adaptive MFA](#) solutions enable customers to easily implement these controls within the cloud and the on-prem components of their Cardholder Data Environments, simplifying compliance to the PCI standard and reducing compliance costs. With the release of Okta's PCI-DSS Attestation of Compliance (AOC), customers are no longer required to demonstrate to auditors how Okta is out of scope to their PCI environment. They can directly leverage the strong protections for identity that Okta offers within their own compliance programs.

You can enable [FIPS-mode encryption for Okta Verify](#). This means that passcodes and push notifications generated by Okta Verify on the following device versions are FIPS 140-2, Level 1 compliant:

- All versions of Okta Verify on Apple iOS 7 and higher
- Okta Verify versions 4.4.0 and higher on Android 6 and higher

For more information on all Okta's service certifications, see [Okta Trust](#).

6. Plan for lost devices

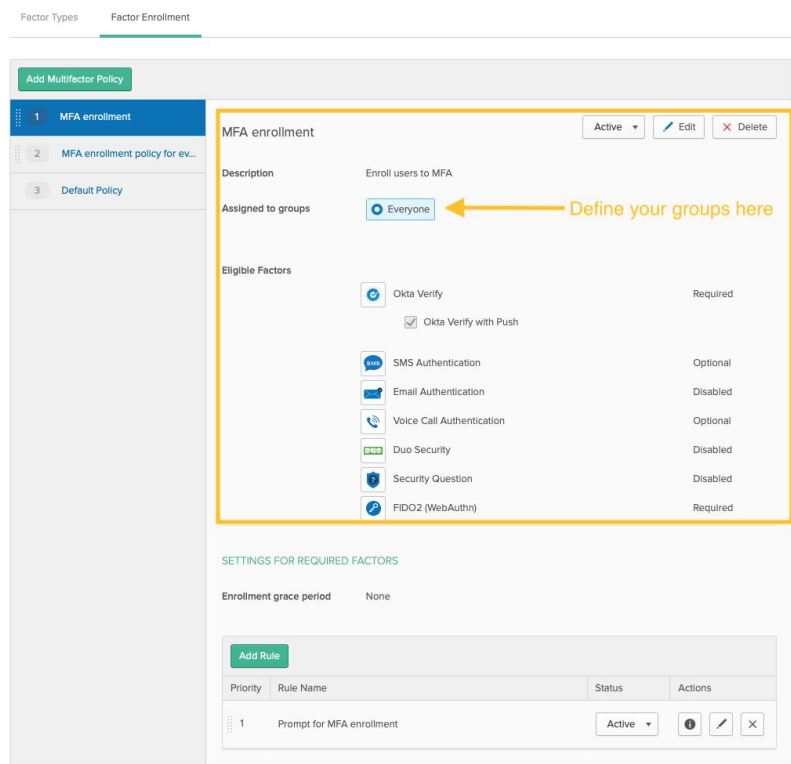
Anything a user has, they can lose. As such, you should always have a plan for lost and/or stolen devices and security keys. Ideally, in such a case, users should be able to access their account with a backup factor and disassociate a lost device or key from their account. This will minimize the probability of account compromise. With this in mind, there are a couple of ways that you can plan for any instance where your user loses their authentication hardware.

Ensure users have a backup factor available

If your users are able to easily reset their factors and use an alternate factor type in case their primary one becomes unavailable, your IT helpdesk will thank you. Your users will also appreciate that they can solve a potential account compromise on their own.

Choose different factor types in Okta

You can select the factors available to different user groups using Okta's factor enrollment policies in the admin console, under **Security > Multi-factor > Factor Enrollment**.

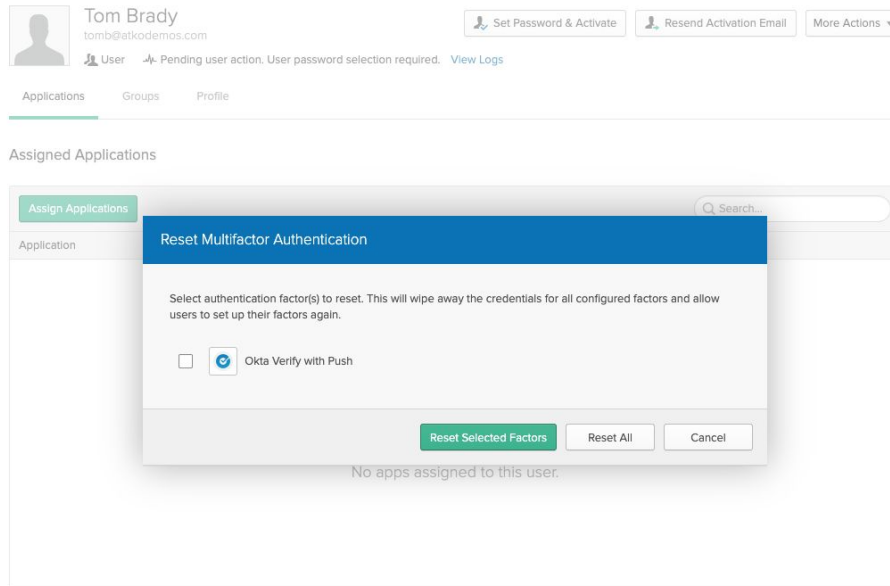


Communicate the features of WebAuthn

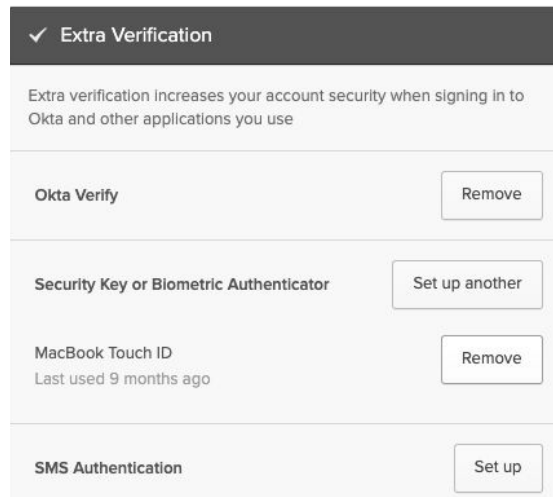
If you are using WebAuthn, your users can enrol multiple devices—and they should be aware of this feature. Okta allows you to register up to 5 WebAuthn factors to an account.

Disassociate lost/stolen factors from an account

This process can be either admin-initiated or user-initiated, but in a scenario where a user can no longer recover a factor, it's important to disassociate that factor type from their account. That way, if the device ends up in the hands of an attacker, they won't be able to access the user's account.



Admin-initiated factor reset via a user's Universal Directory profile



User-initiated factor reset via the end user Settings page

Bonus deployment tip for factor reset

These reset actions are also available via our [Factors API](#). Some organizations create lightweight apps that call these APIs so that users do not need to login to the Okta dashboard to reset their factor.

7. Plan to deploy MFA to remote workers

Optimizing IT processes to support remote employees is now more critical than ever. Traditionally, employees go through a full in-person onboarding process where they set up their device and account (including MFA) with the help of IT. However, as more employees work from home, it's important to have a streamlined process for getting users onboarded from afar. Here are some of the things you can do to get this right:

Utilize the secondary email attribute in Okta during the pre-hire process

You may have noticed a field called "secondary email address" in Universal Directory. It's a good idea to create users before their official start date. This can be done manually, via directory integrations or HR-as-a-Master integrations, and ensures that anyone on your IT/onboarding team can communicate with the user before Day 1.

Use productivity tools (including MFA) to help with remote onboarding

Having to remotely onboard employees has pushed us to be more creative around this process. While you could just ship your new employees a laptop and send them an email with setup steps, you may also want to consider a more interactive onboarding experience. One example is Zoom, an app that saw [110% growth](#) between February and March 2020, which can be used to guide users through the process of setting up their device, account, and MFA.

Deploy intelligent access policies using Adaptive MFA

It's no secret that attackers have been taking advantage of the chaos around the COVID-19 pandemic to launch a flood of phishing and identity attacks. Barracuda researchers have observed a [667% increase](#) in spear-phishing attacks since the end of February 2020 and the FBI has even [issued a warning](#) about an increase in fraud schemes due to the pandemic.

This means we all need to stay ahead of threats. Creating policies using Okta's Adaptive MFA is a great way to do that.

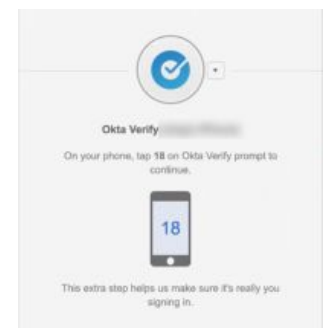
- Enable [Okta ThreatInsight](#) on your org to proactively prevent account lockout and account takeover from suspicious IP addresses.
- If there are specific locations/regions you know that no employees should be accessing apps from, use Okta's country-based dynamic zones to deny access from those locations.

The screenshot shows the 'Edit Dynamic Zone' configuration page. The 'Zone Name' field contains 'Risky Countries'. Below it is a checkbox for 'Blacklist access from IPs matching conditions listed in this zone' with a warning message: 'WARNING: Selecting this option will prevent matching IPs from accessing Okta.' The 'IP Type' dropdown is set to 'Any'. The 'Locations' section features a search bar and a list of countries: Romania, Philippines, Pitcairn, Poland, Portugal, Puerto Rico, Qatar, Reunion, and Romania. To the right of the list are two 'State/Region (Optional)' dropdown menus. At the bottom right, there are 'Save' and 'Cancel' buttons.

- Create policies for behavior detection—especially new device logins. Set your authentication policy to always prompt for MFA on new device logins.

Bonus deployment tip to enforce adaptive policies

Did you know you can combine Risk-Based Authentication with Okta Verify to protect against phishing attacks? When Okta detects a high-risk login, end users are presented a **Review** button in Okta Verify allowing them to review details about the authentication attempt. End users can then tap either **Yes, It's Me** to access their Okta account after satisfying a simple verification challenge or **No, It's Not Me** to deny the authentication attempt.



You can learn more about this feature [here](#). You can also enable the feature on your org via the self service feature manager, **Settings > Features**. Look for **Phishing Resistant Okta Verify Push**.

8. Phase your deployment: Be prepared to review and revise

This is true for any technology in your environment: you should be prepared to modify policy configurations and adapt to new business requirements as they emerge. Get comfortable with our auditing functionality (via Syslog) early in the process—it will be invaluable for troubleshooting and adjusting policy configuration. Once you’ve deployed MFA to your users, use auditing tools to spot check adoption and use. Deploying a mechanism that allows users to provide feedback can also be useful—while users may not always take the time to provide written feedback, an audit trail gives you some visibility into what they experienced.

Here’s one feature that we’ve developed to help users have more insight into their account activity.

UserInsight

[Userinsight](#) alerts users via email when suspicious activities like an MFA factor enrollment or password change is detected on their account. From there, the user has the opportunity to report the activity to their IT admins if they don’t recognize it.

🔒 General

Security Notification Emails Edit

New sign on notification email	Enabled
MFA enrolled notification email	Enabled
MFA reset notification email	Enabled
Report suspicious activity via email	Enabled

This feature allows users to report activities they do not recognize from email notifications. [Learn more](#)

okta

Hi User,

You enrolled in multi-factor authentication for your account [example@user.com](#).

Details
SMS Authentication
Thu, May 9, 2019
San Francisco, California, US

Don't recognize this activity?
Your account may have been compromised, we recommend reporting the suspicious activity to your organization.

[Report Suspicious Activity](#)

The security of your account is very important to us and we want to ensure that you are updated when important actions are taken.

Today’s digital environment and growing levels of security risks make it indispensable for companies to deploy adaptive multi-factor authentication. This context-aware tool makes it easier for you to secure your people—the new perimeter—and engage your users in actively protecting your resources and data. With these eight steps, you’ll be well on your way to a successful MFA deployment that secures your users, without compromising their productivity.

If you have read this far, you’re ready to start deploying MFA!

For more information on how to get started with deploying Okta Adaptive MFA, [watch our demo](#).