

Okta End User FAQs

##

December 2020

Version 1.0

##

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Type of update | Completed by | Document Version |
| 12/18/2020 | New | Elaine Hsu | 1.0 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Document Purpose and Use](#_mkda3pvk9fpy) **4**

[General](#_72xmeegnsh8k) **4**

[General Okta Background FAQs](#_wfgs8afqt516) 4

[What is Okta?](#_k7pk81szpjy4) 4

[Does Okta work on my mobile device?](#_lyan7fwbwcdh) 4

[Who do I contact in case of issues with my Okta account?](#_o84vrqb09in6) 4

[Accessing the Okta Dashboard FAQs](#_2kvtyk8s31zd) 4

[How do I sign into Okta?](#_wt281i9wwlla) 4

[Navigating the Okta Dashboard FAQs](#_5zbsx37kqjyg) 5

[What is a plugin?](#_mp27qjul72ic) 5

[Do I have to use the Okta plugin?](#_mp27qjul72ic) 5

[How do I add Apps to my dashboard?](#_mp27qjul72ic) 5

[How do I customize my Okta Dashboard?](#_vj1ghsws4gj4) 5

[Why does my Okta session expire but some of the apps are still open?](#_u79sv3l1hkrn) 5

[Managing Passwords/Accounts FAQs](#_xejug451z0ll) 5

[How do I change my password?](#_5wteitbo8m6o) 5

[How do I unlock my account?](#_5wteitbo8m6o) 6

[What do I do if I forgot my password?](#_5wteitbo8m6o) 6

[Single Sign On (SSO)](#_p6t46m7kjn4p) **6**

[What is SSO?](#_4jxa1l4s3yxr) 6

[How does SSO work?](#_1pf8ga2g4z8m) 6

[How does Okta keep my username and password secure?](#_cc8nzy2y2i4z) 6

[Can I opt out of SSO?](#_vanarj9pahw0) 6

[What is my username and password for Okta?](#_96vqgidhdwhe) 7

[Multi-Factor Authentication (MFA)](#_nkum2ys6803j) **7**

[General MFA Background FAQs](#_k5sqjld6cpfc) 7

[What is MFA?](#_4o8xn4fwhhtw) 7

[What is a security ‘factor’?](#_cnm1adftpk6) 7

[Why is MFA required?](#_15wapufcxjf0) 7

[Why isn’t primary authentication enough, what’s wrong with passwords?](#_s79vgasle25z) 8

[What are the benefits of MFA?](#_cu56jy9rcdb4) 8

[Okta-Specific MFA Product FAQs](#_gyceai8rc5ss) 8

[How does Okta keep MFA factors secure?](#_cr8u45wbk3nk) 8

[Which MFA factors does Okta support?](#_u9joiq3ohqon) 8

[What is Okta Verify?](#_rm4twjcz4hs2) 9

[Do I need to set-up MFA again if I registered previously?](#_idz4vwq0eku3) 9

[Can I turn off MFA?](#_exrgtn7l7k1e) 9

[What are the different ways users can access Okta integrated applications?](#_a7y0mdo7rgnq) 9

[Can users register two devices for MFA?](#_kauakq3ahcn1) 9

[Okta-Specific MFA Product How-To/Troubleshooting FAQs](#_rq0rjc9s66w) 9

[How do I setup and register my MFA?](#_bzj5v6geaykd) 9

[How do I register a new device for MFA?](#_n0syllj3qqv4) 10

[How do I reset my MFA?](#_2lyxgjnmvtu) 10

[What can a user do if they are stuck on the “Enrolling your Device” screen on the phone they want to use for MFA?](#_qidmhrmddy) 10

[Why do I keep seeing MFA prompts after I’ve selected “Do not challenge me on this device again”?](#_q1wgm1momi94) 10

|  |
| --- |
| Document Purpose and Use |

The purpose of this document is to provide a list of frequently asked questions (FAQs) related to Okta. This list can be used by Okta’s customers as a reference or as a baseline when sending out training or communications to their end users regarding upcoming changes related to Okta. This document covers general Okta FAQs as well as common Okta products such as Single Sign-On and Multi-Factor Authentication FAQs.

Okta recommends that our customers tailor this list to your specific deployment of Okta, and post and/or send the information to all affected users.

|  |
| --- |
| General |

## **General Okta Background FAQs**

### **What is Okta?**

Okta is the foundation for secure connections between people and technology. Okta is a platform that securely connects employees, partners, and customers to the applications and tools they need in a single sign-on format.

### **Does Okta work on my mobile device?**

It does. Download the Okta Mobile app from your app store for full mobile access to Okta. Okta Mobile allows you to access your applications from your mobile device, so you get the security of Single Sign-On from your mobile device.

### **Who do I contact in case of issues with my Okta account?**

Contact your company's help desk or IT admin for assistance.

## **Accessing the Okta Dashboard FAQs**

### **How do I sign into Okta?**

Your sitename is the URL you visit to access your organization’s Okta sign-in page. It is usually structured as [company.okta.com]. Ask your IT admin if you’re not sure what your sitename is. You can watch this [short video](https://www.youtube.com/watch?v=QtPqvLxF1go&feature=youtu.be) on how to get started with Okta.

## **Navigating the Okta Dashboard FAQs**

### **What is a plugin?**

Plugins are browser applications that can be easily installed and are used as a part of a web browser. They’re sometimes called Browser Extensions (Chrome) or AddOns (Mozilla Firefox).

### **Do I have to use the Okta plugin?**

We recommend that you use the Okta plugin because it can help you get to your apps faster than through the web Dashboard, you can add your apps to Okta on the fly, and it also comes with security benefits.

Whether you have access to the plugin or not depends on the Okta settings that your administrator has selected. Ask your help desk if you aren’t sure.

### **How do I add apps to my dashboard?**

If your organization allows you to add your own apps, there will be an **+Add Apps** button on the left panel of your Okta Dashboard. Select that button, search for your app, and click the **Add** button.

### **How do I customize my Okta Dashboard?**

You can learn more customizations on your Okta dashboard [here](https://help.okta.com/en/prod/end-user/Content/Topics/end-user/dashboard-new-overview.htm?cshid=csh-user-dashboard-new-overview).

###  **Why does my Okta session expire but some of the apps are still open?**

When you’re logged out of your Okta session, Okta doesn’t automatically log you out of your applications. Your apps have their own session lifetime which they determine, or you can manually log out of them when you’re finished.

## **Managing Passwords/Accounts FAQs**

### **How do I change my password?**

To change your Okta password, log in to your Okta account. Click **Settings** on the left panel of your dashboard.

In the **Change Password** section, enter your current password and the new password you’ve chosen. Make sure your password meets the complexity guidelines set by your admin. Click **Change Password** and you’re good to go.

If you do not see the Change Password option, please contact your company's help desk or IT admin for assistance.

### **How do I unlock my account?**

If you’re locked out of your account (but still remember your password), click the **Need help signing in?** link at the bottom of the sign-in page. Then click **Unlock account** to unlock it. If that doesn’t work, call your help desk.

### **What do I do if I forgot my password?**

If you’ve forgotten your password, click the **Need help signing in?** link at the bottom of the sign-in page. Then click **Forgot password** to reset it. If that doesn’t work, call your help desk.

|  |
| --- |
| Single Sign-On (SSO) |

## **What is Single Sign-On (SSO)?**

SSO is one of the many products that Okta provides. SSO lets you use a single username and password to access all your apps. No more remembering all your different password and username combinations to get to the apps that you need to get your work done.

## **How does SSO work?**

With SSO, you sign in to your company’s Okta Dashboard. From there, you can launch any of your web apps without having to enter any other additional credentials. Okta manages all your application credentials and securely logs you into your apps. Sometimes, you might not even know what your username and password are for certain apps because your IT team will manage all of that for you in the background.

## **How does Okta keep my username and password secure?**

Okta provides rigorous security measures and controls to protect your information. This includes securing and verifying all communications with Okta, encrypting customer data, and ensuring that only the right people in your organization can control the Okta service. These controls are audited regularly.

## **Can I opt out of SSO?**

If your administrator has enabled SSO, you can’t choose to opt out. That would leave a huge hole in your organization’s security, and leave everyone’s data vulnerable to an attack.

## **What is my username and password for Okta?**

Your username and password are a pair of credentials that you use to log in to the Okta dashboard. If you don't know your username, contact your company's help desk. If you've forgotten your password, click the **Need help signing in?** link at the bottom of the sign-in page. Then click **Forgot password** to reset it. If you don’t see these options, contact your help desk.

|  |
| --- |
| Multi-Factor Authentication (MFA) |

## **General MFA Background FAQs**

### **What is Multi-Factor Authentication (MFA)?**

Multi-Factor Authentication is a security practice that requires more than one method of authentication, using independent categories of credentials to verify a user’s identity. For example, you may log in to a system using your password (“what you know”) and then verifying a separate six-digit number that is sent to your phone (“what you have”). By combining “what you know” and “what you have” verification, the hackers will have harder time breaking into our systems as they may not have both your password and your phone.

When you log in to an account or application, you’re asked for a password so you can prove you are who you say you are. You may then be asked for a second factor.

### **What is a security “factor”?**

The “factor” in MFA refers to a method of verifying your identity. The most basic type of factor is your password, which is often the primary, or initial authentication factor you’ll be prompted for. Your organization may choose to ask for more factors to complement your password. These additional factors could range from an app on your phone that generates a code for you to enter after you’ve typed in your password, to a USB key you have to insert into your computer, or even a fingerprint scan.

### **Why is MFA required?**

MFA is an effective way to provide enhanced security. Traditional usernames and passwords can be stolen, and they've become increasingly more vulnerable to malicious activity, and cyber attacks like phishing or brute force attacks. MFA creates multiple layers of security to help increase the confidence that the user requesting access is actually who they claim to be.

Reports show that applications and identities are the initial targets in 86% of breaches. It has become a necessity to protect our applications and identities through a second layer of security.

### **Why isn’t primary authentication enough, what’s wrong with passwords?**

* One set of login credentials (such as username and password) is not solving important access challenges.
* Passwords, in addition to being difficult to manage, are vulnerable to a variety of attacks like phishing, social engineering, etc.
* By boiling all applications down to one username and password, security strength is only as strong as that one set of credentials. If it's a bad password, your security situation hasn't improved.
* If hackers get a hold of a user’s login credentials, they can access all of the user’s resources. This is especially a threat if that user has access to privileged information or mission-critical data.

### **What are the benefits of MFA?**

* Lower the chances of end-user identities (and, subsequently, their IT resources) becoming compromised.
* Even if hackers have a user’s password, we can stop them by adding a personal, time-sensitive factor to the authentication process.
* Peace of mind for enterprise, knowing that users sensitive data is made safer by an additional security layer.
* MFA also adds a sense of mindfulness to authentication. By taking the time to add their second factor, users are reminded of the importance of tight identity security.

## **Okta-Specific MFA Product FAQs**

### **How does Okta keep MFA factors secure?**

Okta encrypts your user credentials using two different software locks called keys. It stores user data and the keys used to unlock that data in separate databases. For extra security, it then encrypts the keys in three different ways for even stronger protection. No one person at Okta can access the encrypted master key, and Okta maintains an audit trail to show how it manages the keys.

##

### **Which MFA factors does Okta support?**

Okta supports a number of factors: passwords, security questions, login codes sent via mobile apps or SMS, push notifications (Okta Verify with Push, Google Authenticator), email, voice, plug-in and wireless-enabled hardware keys, third-party factors (Duo, Symantec, RSA, and YubiKey OTP), and biometrics (Windows Hello, Apple TouchID). Please refer here for additional, detailed [Okta MFA Factors](https://support.okta.com/help/s/end-user-adoption-toolkit/mfa-factors-overview-for-end-users?language=en_US) information.

### **What is Okta Verify?**

Okta Verify is a mobile application from Okta that can be used to verify a user for MFA purposes. You receive a push notification on your mobile to confirm the second factor after the factor is set up. Please refer here for additional, detailed [Okta Verify FAQs](https://help.okta.com/en/prod/Content/Topics/Mobile/okta-verify-faq.htm).

### **Do I need to set up MFA again if I registered previously?**

No. Once done or configured, you need not set up a factor again.

##

### **Can I turn off MFA?**

If your administrator has enabled MFA, you can’t choose to opt out. That would leave a huge hole in the organization’s security, and leave everyone’s data vulnerable to an attack. However, your administrator might have enabled four or five different MFA options, and will only require two or three. That lets you choose the factor that best suits your working style. Are you constantly checking your phone? Then Okta Verify may be the right factor for you. Check with your help desk to see which MFA options are available to you.

### **What are the different ways users can access Okta-integrated applications?**

There are two ways users can log in:

* Users can go to <customer>.okta.com and log in first, and then they can choose the application they want to access.
* Users can directly go to the application they want to access using application URL, and then the application may or may not redirect the user to Okta login page depending on whether they have a valid session or not.

### **Can users register two devices for MFA?**

No, with push notification enabled, you cannot register two devices for a single account.

##

## **Okta-Specific MFA Product How-To/Troubleshooting FAQs**

### **How do I set up and register my MFA?**

1. User accesses Application / Okta Dashboard
2. User is redirected to Okta login page
3. User submits username and password
4. User is successfully logged in
5. User is prompted to enroll in MFA factors
6. User enrolls in 1 or more factors
7. User redirected to Application / Okta Dashboard

###

### **How do I register a new device for MFA?**

To register a new device you need to reset your MFA and then set it up again with the new device.

### **How do I reset my MFA?**

1. Go to your Okta Dashboard, where you’ll be redirected to the Okta login page
2. Submit your username and password
3. If prompted, add your second factor for authentication
4. Once you’re logged in, go to the **Settings** page, and click on **Edit Profile**
5. For security, you’ll be prompted to provide your password and/or second factor
6. Click **Remove** for factor to reset
7. Click on **Set up** for factor you wish to reset

### **What can I do if I am stuck on the “Enrolling Your Device” screen on the phone I want to use for MFA?**

If you get stuck in a loop when attempting to register via SMS/Email/QR code, or you are not getting any code to enter or any push notification, it means your device may not have enrolled correctly. In this case, you need to reset MFA from your account, uninstall Okta Verify on the device, install it again, and then set up the MFA again.

###

### **Why do I keep seeing MFA prompts after I’ve selected “Do not challenge me on this device again”?**

If you continue to see MFA prompts after selecting “Do not challenge me on this device again,” it could be for a few different reasons:

1) *Cookie management*: The “Do not challenge me again” choice is captured in a browser cookie. If you’ve recently cleared your cookies, or are using a new browser (like Chrome, Internet Explorer, Mozilla Firefox), it won’t remember the choice.

2) *Policy configuration*: Your Okta administrator sets how often they want MFA challenge prompts to appear. If they have set that window to every eight hours or 24 hours, you’ll see MFA prompts again after that window, even if you’ve selected the “Do not challenge me on this device again” checkbox.

3) *Exempted action*: Certain actions, like editing your account profile, will always trigger an MFA prompt as an additional layer of security.

##