

Okta End User FAQs

##

November 2021

Version 1.1

##

Contents

[Document Purpose and Use](#_tyjcwt) **3**

[General](#_4d34og8) **3**

[General Okta Background FAQs](#_2s8eyo1) 3

[What is Okta?](#_17dp8vu) 3

[Does Okta work on my mobile device?](#_3rdcrjn) 3

[Who do I contact in case of issues with my Okta account?](#_26in1rg) 3

[Accessing the Okta Dashboard FAQs](#_lnxbz9) 3

[How do I sign into Okta?](#_35nkun2) 3

[Navigating the Okta Dashboard FAQs](#_1ksv4uv) 4

[What is the Okta plugin?](#_iy2cu88x9am9) 4

[Do I have to use the Okta plugin?](#_rn6beuxcaaue) 4

[How do I add apps to my dashboard?](#_44sinio) 4

[How do I customize my Okta Dashboard?](#_2jxsxqh) 4

[Why does my Okta session expire but some of the apps are still open?](#_z337ya) 4

[Managing Passwords/Accounts FAQs](#_3j2qqm3) 4

[How do I change my password?](#_xvdy16cq3mmm) 4

[How do I unlock my account (Okta Classic)?](#_xuxkpern5htl) 5

[How do I unlock my account (Okta Identity Engine)?](#_owv3ntk28hrl) 5

[What do I do if I forgot my password (Okta Classic)?](#_mm0pkq4nurrb) 5

[What do I do if I forgot my password (Okta Identity Engine)?](#_cphpv83mwrlp) 5

[Single Sign-On (SSO)](#_2xcytpi) **6**

[What is Single Sign-On (SSO)?](#_1ci93xb) 6

[How does SSO work?](#_3whwml4) 6

[How does Okta keep my username and password secure?](#_2bn6wsx) 6

[Can I opt out of SSO?](#_qsh70q) 6

[What is my username and password for Okta?](#_3as4poj) 6

[Multi-Factor Authentication (MFA)](#_1pxezwc) **7**

[General MFA Background FAQs](#_49x2ik5) 7

[What is Multi-Factor Authentication (MFA)?](#_2p2csry) 7

[What is a security “factor”?](#_147n2zr) 7

[Why is MFA required?](#_3o7alnk) 7

[Why isn’t primary authentication enough, what’s wrong with passwords?](#_23ckvvd) 7

[What are the benefits of MFA?](#_ihv636) 8

[Okta-Specific MFA Product FAQs](#_32hioqz) 8

[How does Okta keep your passwords secure?](#_1hmsyys) 8

[Which MFA factors does Okta support?](#_2grqrue) 8

[What is Okta Verify? (Okta Classic)](#_vx1227) 8

[What is Okta Verify? (Okta Identity Engine)](#_4a7x9teucxde) 8

[Do I need to set up MFA again if I registered previously?](#_3fwokq0) 9

[Can I turn off MFA?](#_4f1mdlm) 9

[What are the different ways users can access Okta-integrated applications?](#_2u6wntf) 9

[Can users register two devices for MFA (Okta Identity Engine)?](#_h0qrh622zzoc) 9

[Okta-Specific MFA Product How-To/Troubleshooting FAQs](#_28h4qwu) 10

[How do I set up and register my MFA?](#_nmf14n) 10

[How do I register a new device for MFA (Okta Identity Engine)?](#_1mrcu09) 10

[How do I reset my MFA (Okta Identity Engine)?](#_46r0co2) 10

[What can I do if I am stuck on the “Enrolling Your Device” screen on the phone I want to use for MFA?](#_2lwamvv) 11

[How do I download the Okta Verify app?](#_aam0ld7wcq6h) 11

[Okta Identity Engine Product How-To/Troubleshooting FAQs](#_1hgqkvpqxc9i) 11

[My sign-in experience has changed, how do I use the new sign-in experience?](#_6gup4gtnfyro) 11

[What does the “keep me signed in” checkbox do?](#_xp74gt7g92bo) 11

[What is the difference between Okta Verify for mobile devices and Okta Verify for desktop devices?](#_yyizy95uyi82) 11

[What is “Sign in with Okta FastPass”?](#_rd30qlxq81rp) 12

| 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. You can navigate to your sitename from your mobile device’s browser. Most apps can be launched directly from the mobile dashboard. Apps that rely on the Okta plugin, specifically apps where you have manually set a password, will require you to copy the password from the dashboard and manually paste it into the login form. Apps configured with an admin-defined password cannot be launched from mobile devices.

### **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.

## **Navigating the Okta Dashboard FAQs**

### **What is the Okta plugin?**

The Okta plugin 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, Safari) 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. The Okta plugin can autofill usernames and passwords for apps where the admin has configured a username or password for you. You can also add your own apps to Okta with the plugin. .

Whether you have access to the plugin or not depends on the Okta settings that your administrator has selected. Ask your IT admin 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 add sections, change between list and grid view, sort apps, and more. Learn more about 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 on your name in the top right corner of your dashboard which will open a dropdown menu. From the drop down menu, click **Settings.**

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, check if you have the **Edit Profile** button. Click on **Edit Profile**. This button may prompt you to re-authenticate with password and / or extra security methods. If this doesn’t work, please contact your company's help desk or IT admin for assistance.

### **How do I unlock my account (Okta Classic)?**

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. You may be prompted to authenticate with additional security methods. If you do not see this option, account unlock may not have been configured for your organization. Please call your help desk.

### **How do I unlock my account (Okta Identity Engine)?**

If you’re locked out of your account (but still remember your password), click the **Unlock Account?** link at the bottom of the sign-in page. You may be prompted to authenticate with additional security methods. If you do not see that option, account unlock may not have been configured for your organization. Please call your help desk.

### **What do I do if I forgot my password (Okta Classic)?**

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.

### **What do I do if I forgot my password (Okta Identity Engine)?**

If you’ve forgotten your password, and your organization has set up your sign in page so that you enter username and password directly on the sign-in page, then click **Forgot password?** link at the bottom of the page.

If your organization has set up your sign in page so you enter your username then click **Next**, you will see the **Forgot password?** link underneath the password entry field when you go to enter your password.

After clicking on the **Forgot password?** link, you will be prompted for authentication with additional security methods.

If you do not see the **Forgot password?** link or the security method is not working, please 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 sign in to one service, Okta, 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. Some apps you can navigate directly to the app and the app will sign you in from Okta.

## **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 a 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?**

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.

By giving access to all applications with just one username and password, security strength is only as strong as that one set of credentials. 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?**

MFA adds an extra layer of security to your account. If hackers get a hold of a user’s login credentials, they will still need to get access to the user’s phone, Okta Verify app, or security key before they can access your data or your company’s data.

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.

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

### **How does Okta keep your passwords 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 (Okta Verify, Google Authenticator), login codes sent via email or SMS, push notifications (Okta Verify with Push), 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 Classic)**

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. For more information about Okta Verify, see the documentation for [Okta Verify on iOS](https://help.okta.com/okta_help.htm?type=eu&id=csh-user-ov-manage-account-ios) and [Android](https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-mng-account-android.htm).

### **What is Okta Verify? (Okta Identity Engine)**

Okta Verify is a mobile and desktop application from Okta that protects your data, ensuring that you, and only you, can access your app accounts. Okta Verify can be installed on mobile and desktop devices.

On mobile devices (iOS and Android), depending on your organization’s configuration, you can use Okta Verify to verify your identity using a push notification sent to your device, a temporary six-digit code, or biometrics. If you see the option to “Sign in with Okta FastPass” on your sign-in screen, you can use Okta Verify to login without using a username or password.

On desktop devices, the Okta Verify app is used to assess the security of the device you’re using. Depending on your organization’s configuration, you may be able to use Okta Verify to sign-in to Okta without using a username or password.

For more information about Okta Verify, see the [end-user documentation](https://help.okta.com/okta_help.htm?type=eu&id=ext-ov-user-overview).

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

No. Once done or configured, you need not set up a security method again unless you reset that security method.

##

### **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 the 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 (Okta Identity Engine)?**

Users may register multiple Okta Verify devices and multiple security keys and biometrics for MFA, if these security methods are enabled for your organization.

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

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

If you are required to use MFA, you will be prompted for MFA enrollment the first time you login. When you go to access your Okta Dashboard or a specific application protected by Okta, after you submit your username and password, Okta will prompt you to enroll in 1 or more security methods. If you are required to enroll, you will be unable to skip this step. Depending on the security method your admin has configured to allow you to use, you may be required to download the Okta Verify app, enter your phone number to receive an SMS or Voice Call, or use a security key.

After you have successfully enrolled in required security methods, you may see the option to enroll in optional security methods. This is so you have a back-up security method to login if you don’t have your primary option. Okta recommends enrolling in at one optional factor if set up. You may skip this step and continue on to your Okta Dashboard or application.

###

### **How do I register a new device for MFA (Okta Identity Engine)?**

You can download Okta Verify to your device and add a new account.

* [Documentation for Android](https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-new-install-signin-android.htm)
* [Documentation for iOS](https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-new-install-signin-ios.htm)
* [Documentation for Mac OS](https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-setup-macOS.htm)
* [Documentation for Windows](https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-setup-windows.htm)

From the Okta dashboard, you can also do the following:

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, click on your name in the top right corner, and click on **Settings** from the dropdown menu.
5. For security, you may need to click on **Edit profile**, and be prompted to provide your password and/or second factor
6. From the settings page, Click **Remove** for the factor you want to reset.
7. Click on **Set up** for the factor you wish to reset

### **How do I reset my MFA (Okta Identity Engine)?**

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, click on your name in the top right corning and click on the the **Settings** page from the dropdown menu
5. Click **Remove** for the factor you wish to reset
6. For security, you may be prompted to provide your password and/or second factor
7. Click on **Set up** for the 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.

### **How do I download the Okta Verify app?**

For more information about downloading, installing, and using Okta Verify apps for different devices, please see the [Okta Verify documentation for end users](https://help.okta.com/okta_help.htm?type=eu&id=ext-ov-user-overview).

##

## **Okta Identity Engine Product How-To/Troubleshooting FAQs**

### **My sign-in experience has changed, how do I use the new sign-in experience?**

For more information about the changes, visit the Okta documentation [here](https://help.okta.com/okta_help.htm?type=eu&id=ext-sign-in-flows).

### **What does the “keep me signed in” checkbox do?**

If you select the **Keep me signed in** checkbox before you proceed with username and your credentials, you may reduce the number of username and security method prompts you see the next time you sign in. Your organization may let you skip extra verification, or you may not be required to re-authenticate at all. **Please do not check this box on shared or personal computers.**

If you don’t see any changes to the sign in experience the next time you sign in, it could be that you’re using a browser that does not support persistent browser cookies. For example, the embedded browser that opens on your phone when you click on a link from your email mobile application may not store persistent browser cookies. Otherwise, your admin may not have configured Okta to have a different sign-in experience when **Keep me signed in** is checked.

### **What is the difference between Okta Verify for mobile devices and Okta Verify for desktop devices?**

The Okta Verify app for mobile devices (iOS and Android) is an application that can be used to verify your identity and assess device security. Okta can send you a push notification that you approve using Okta Verify. Okta Verify can generate a six-digit code that you enter into your Okta login screen to access your required app. Alternatively, if configured by your admin, the Okta Verify app can be used for **Sign in with Okta FastPass** and allow you to sign in without entering a username or password. Your admin may have configured your Okta Verify app to require device biometrics as well.

The Okta Verify app for Mac and Windows can be used to verify your identity and assess device security. If configured by your admin, the Okta Verify app on desktop can be used with the **Sign in with Okta FastPass** option on the sign in screen with you having to enter username or password. The Okta Verify app can also be used to assess device security and ensure that your device meets your admin’s security requirements.

For more information about Okta Verify apps, please see the [Okta Verify documentation for end users](https://help.okta.com/okta_help.htm?type=eu&id=ext-ov-user-overview).

### **What is “Sign in with Okta FastPass”?**

The **Sign in with Okta FastPass** button allows you to sign in without entering your username. Your admin may have set it up so you can sign in with device biometrics or without any additional action at all! Sign in with Okta FastPass requires you to have the Okta Verify app downloaded and set up on your device. If you have not yet enrolled in Okta Verify on that device, clicking on the **Sign in with Okta Fastpass** button will prompt you to enroll in Okta Verify.

For more information about Okta Verify apps, please see the [Okta Verify documentation for end users](https://help.okta.com/okta_help.htm?type=eu&id=ext-ov-user-overview).