

Okta End-User Email Communication Templates

##

November 2021

Version 1.1

##

Contents

[Document Purpose and Use](#_3as4poj) **3**

[Single Sign-On (SSO) Email Templates](#_ihv636) **4**

[Email Template 1: Introducing Okta Single Sign-On (SSO)](#_32hioqz) 4

[Email Template 2: Okta Single Sign-On (SSO) Is Coming](#_1hmsyys) 5

[Email Template 3: Okta Single Sign-On (SSO) Is Here](#_2grqrue) 6

[Email Template 4: Reminder to Get Activated with Okta](#_1v1yuxt) 7

[Multi-Factor Authentication (MFA) Email Templates](#_4f1mdlm) **8**

[Email Template 1: Introducing Okta Multi-Factor Authentication (MFA)](#_2u6wntf) 8

[Email Template 2: MFA Is Coming—Setup and Security Preferences](#_3tbugp1) 10

[Email Template 3: Okta Multi-Factor Authentication (MFA) Is Here](#_nmf14n) 12

[App-Specific Email Template](#_37m2jsg) **13**

[Email Template 1: <specific app> Is Live with Okta!](#_1mrcu09) 13

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

The purpose of this document is to provide example email templates for Okta’s customers to use when communicating to their end users about upcoming changes related to Okta. This document covers the most common Okta product deployments, Single Sign-On and Multi-Factor Authentication, as well some app-specific Okta integrations.

Okta recommends a series of notifications for each change, allowing Okta’s customers’ end users ample time to adjust to, prepare for, and adopt the change.

Please note that all placeholder text in the email templates has been <bracketed and made red>. Please make edits to placeholder text accordingly before sending to end users, and tailor the content to your specific deployment of Okta.

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

## **Email Template 1: Introducing Okta Single Sign-On (SSO)**

**Purpose of Email:**

To introduce your users to Okta and the SSO process, providing for a brief explanation and definition of SSO, and to ready them for the upcoming changes when Okta is live in your environment.

**Recommended Timing of Delivery:**

As early in the project lifecycle as permits, but to prevent this information from becoming stale, Okta recommends 30-45 days in advance of the Go-Live event that enables Okta into your user environment.

**Subject:**

Introducing <customer name’s> new Single Sign-On provider, Okta—and what it means for you

**Body of Email:**

I am pleased to announce that we have partnered with Okta, a leading Identity and Access Management company, to provide <customer name> the ability to provide easier, faster and more secure ways to log in to the multiple applications we all use on a daily basis. This method is commonly called single sign-on (SSO). As the name suggests, it provides a method and process for all of you to sign in and have access to all of your applications you use in a very handy, easy-to-use dashboard.

**Benefits of using Okta SSO include:**

* Secure set of credentials that allow for access to multiple applications, saving you valuable time when repeatedly accessing.
* Provides additional security features and functionality like multi-factor authentication methods, secure mobile device verifications, and easy transparent biometric authentications.
* And much, much more!

Please be on the lookout for additional emails as we get closer to deploying this new Okta platform. We are carefully working with Okta and our internal IT and applications teams to ensure a smooth transition, and we will be alerting you to upcoming milestones and additional information as we get closer to our Go-Live date.

In the meantime, if you want to do a little more research on Okta and their SSO Platform, feel free to take a look at the link below:

<https://www.okta.com/products/single-sign-on/>

## **Email Template 2: Okta Single Sign-On (SSO) Is Coming**

**Purpose of Email:**

To inform your users that a change in the way they are logging into their applications is coming soon, and that Okta’s Single Sign-On process will be used and is going to be implemented in the next two weeks.

**Recommended Timing of Delivery:**

Timing is dependent on your specific user base, however Okta recommends that this “Coming Soon” email be sent two weeks before the Okta product is deployed into production.

**Subject:**

Review requested—Okta’s Single Sign-On is coming soon, and how it will affect you

**Body of Email:**

Per our previous email regarding Okta’s Single Sign-On partnership with <customer name>, we are entering our final stages of deployment in the next two weeks. To prepare for these changes, please review the following steps to understand how it will affect your login experience to your applications.

These changes will take effect on <enter date here>

* When you log in to your application using your browser or mobile device, you will be prompted to enroll into the Okta platform and will receive an email confirming that enrollment.
* Once enrollment is completed, you will have a single sign-on experience that provides an easy-to-use dashboard with all your applications you have access to.

Directly prior to our Okta Go-Live with this exciting SSO process, we will be sending out a detailed email on how to specifically enroll into the Okta platform. However, in the meantime, if you wish to understand this process in more detail, please feel free to review the following link. There you will find documentationdemonstrating Okta’s Single Sign-On platform.

https://help.okta.com/eu/en-us/Content/Topics/end-user/end-user-home.htm

##

## **Email Template 3: Okta Single Sign-On (SSO) Is Here**

**Purpose of Email:**

To inform your users that Okta has been deployed in your environment and to remind them of the actions that they need to undertake to enroll and successfully use the SSO method from Okta.

**Recommended Timing of Delivery:**

This email should be sent to coincide with the deployment of the Okta Single Sign-On platform to the users that are affected by this Go-Live event.

**Subject:**

ACTION REQUIRED: Okta Single Sign-On Is Here! Next Steps and Actions You Need to Take

**Body of Email:**

Great news! Per our previous communications, the Okta partnership with <customer name> has been successfully deployed with the implementation of Okta Single Sign-On (SSO) for your use going forward. This Go-Live event has occurred on <enter date here>.

As part of the deployment of the Okta SSO platform, there are some steps that you need to take to get access to all your assigned applications:

* Please watch your inbox for an email from <enter from email address> with a subject of <enter subject of mail here>. This is your Okta activation email and it will have detailed instructions on how to enroll in Okta’s Single Sign-On process. This email would have been sent on <enter date here>.
* Please ACTIVATE your account as soon as possible, as the activation email does expire.
* Once you have completed the activation process, please navigate to <enter Okta dashboard URL here>, where you will be prompted to log in to our Okta portal. You will then have access to all of your assigned applications.

You can find documentation of how to navigate Okta at the following link: https://help.okta.com/eu/en-us/Content/Topics/end-user/end-user-home.htm.

If you have any questions or need additional assistance with the enrollment process, please contact the <enter help desk contact info, by region if necessary>.

Additionally, you can review a list of FAQs at the following location:

<enter FAQ URL here>

##

##

## **Email Template 4: Reminder to Get Activated with Okta**

**Purpose of Email:**

To remind users that have not enrolled in Okta Single Sign-On to activate their account before their activation email expires.

**Recommended Timing of Delivery:**

Daily, until the user has successfully enrolled in the Okta Single Sign-On Process.

**Subject:**

URGENT ACTION REQUIRED: Enroll in the Okta Single Sign-On process

**Body of Email:**

We have not seen an Okta Single Sign-On enrollment that is linked to your account.

Your enrollment is an important step in the deployment process that ensures that the benefits of Okta are realized by each member of our organization that we have licensed this technology to.

Therefore, at your earliest convenience, please review the enrollment email sent on <enter date> which would have been sent from <enter from email address>, and ACTIVATE your account according to the instructions within the email.

You can find a video overview of how to navigate your new Okta dashboard [here](https://www.youtube.com/watch?v=QtPqvLxF1go&feature=youtu.be).

If you did not receive the email, or have additional questions, please contact <enter help desk contact info, by region if necessary>.

Additionally, you can review a list of FAQs at the following location:

<enter FAQ URL here>

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

## **Email Template 1: Introducing Okta Multi-Factor Authentication (MFA)**

**Purpose of Email:**

To introduce your users to Okta and the Multi-Factor Authentication process, providing for a brief explanation and definition of MFA and to ready them for the upcoming changes when Okta MFA is live in your environment.

**Recommended Timing of Delivery:**

Two or more weeks before implementation, depending on size of organization.

**Subject:**

Coming Soon—Multi-Factor Authentication for Okta Applications

**Body of Email:**

In order to protect <customer name> assets even better, <customer name> will be enforcing Multi-Factor Authentication (MFA) for <list affected user groups> when attempting to log in to Okta-managed applications like <list sample Okta integrated applications>. Please read the information below in preparation for this rollout.

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

* MFA is a method of authentication where the user is asked to provide two independent credentials in order to verify the user’s identity. For example, when a user authenticates with their password, and is also required to provide the six-digit code that is sent to their mobile device.

**Why is MFA required?**

* MFA is an effective way to enhance security. Traditional usernames and passwords can be stolen, and they've become increasingly more vulnerable to malicious activities.
* MFA creates an additional layer of security to help increase the level of 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, so it has become a necessity to protect them using a second layer of security.
* With more applications on external cloud infrastructures, MFA will help ensure our assets are better protected.

 **Who is impacted?**

* MFA is prompted for users who are trying to access Okta-integrated applications such as <list applications>.

**How convenient is it to use MFA?**

* With Okta, the current adaptive MFA policy is configured to be prompted only when <list cases where MFA is enforced - outside the network, certain applications, etc...>.

**When is this coming?**

* MFA rollout will be <insert details for MFA rollout - phased approach, one-time cutover of everything, etc...>. For more details on the rollout, please <insert a method for users to contact company support or deploying team for more information>.
* Rollout may be adjusted as needed.

**What do I need to do?**

* When MFA is rolled out for you, you will be prompted to register for MFA when you try to access Okta applications. Simply follow the prompts to self-register.
* For more details on registration, reset, or other FAQs, please refer to <insert link for MFA FAQ>

**Who should I contact if I have questions?**

* <insert a method for users to contact company support or deploying team for more information>

##

## **Email Template 2: MFA Is Coming—Setup and Security Preferences**

**Purpose of Email:**

To inform your users that a change in the way they are logging in is coming soon, and that Okta’s MFA process will be used and is going to be implemented in the next 1-2 weeks. Also, to notify users to enroll in MFA.

**Recommended Timing of Delivery:**

Timing is dependent on your specific user base, however Okta recommends that this “Coming Soon” email be sent 1-2 weeks before Okta MFA roll out.

**Subject:**

Okta/<insert applicable applications> Integration. Set Up Your MFA and Security Preferences Today

**Body of Email:**

As a reminder, <customer name> is integrating Okta with the following applications: <list applicable applications here>. This integration will be a secure solution, simplifying access to the important applications you use every day.

You are now able to set up your Okta Multi-Factor Authentication (MFA) preferences, as well as your self-service password reset (SSPR) security questions and recovery options, saving you time when the integration with Okta is live.

**What do you need to do?**

Please set up your MFA preferences and your self-service password reset security questions and password recovery options in the next <insert appropriate timeframe>. Click [here](https://mckessoncorp.sharepoint.com/sites/identity/SitePages/Okta%20Enrollment.aspx) <insert link> for enrollment instructions.

**Setting up your MFA preferences now will result in a smoother experience once the integration with Okta has taken place.**

**What happens next?**

In the coming weeks, we will send additional information as we prepare for the Okta integration into <insert applicable applications>.

**Questions or support?**

<Include methods for users to contact company support for more information. Example as below:

* For US users, please create a Support ticket through the self-service portal or by calling xxx-xxx-xxxx (US)
* For Canadian users, please contact Canada Support by [creating a ticket](https://newservicecatalog.mckesson.com/sc/catalog.product.aspx?product_id=create.an.it.service.desk.ticket) or by calling xxx-xxx-xxxx>

##

## **Email Template 3: Okta Multi-Factor Authentication (MFA) Is Here**

**Purpose of Email:**

To inform your users that Okta MFA has been deployed in your environment and to remind them of the actions that they need to undertake to enroll and successfully use MFA from Okta.

**Recommended Timing of Delivery:**

This email should be sent to coincide with the deployment of Okta MFA to the users that are affected by this Go-Live event.

**Subject:**

Okta Multi-Factor Authentication Is Live!

**Body of Email:**

As part of our ongoing commitment to the highest standards for data security and privacy protection, <customer name> will integrate the following applications: <list applicable applications> with Okta on <enter date>. Okta is a secure, multi-factor sign-on solution that will change how you access our <insert web portal/applications list>.

**What does this mean for you?**

On or after <enter date>, on your first login into the updated site, you will be led through a series of screens to set up your preferences for multi-factor authentication (MFA) and self-service password recovery (SSPR).

Specific instructions for logging into your account for the first time have been forwarded to your email address.

**What do you need to do?**

If you have already set up your MFA preferences, congratulations! You will be required to successfully pass the MFA option(s) that you selected during enrollment, moving forward, as a part of the new login process.

If you have not already done so, don’t worry. Setting up your MFA and SSPR preferences is easy. Click <insert location of instructions here> for instructions.

**Who should I contact if I have questions?**

<Include methods for users to contact company support for more information. Example as below:

* For US users, please create a Support ticket through the self-service portal or by calling xxx-xxx-xxxx (US)
* For Canadian users, please contact Canada Support by [creating a ticket](https://newservicecatalog.mckesson.com/sc/catalog.product.aspx?product_id=create.an.it.service.desk.ticket) or by calling xxx-xxx-xxxx>

|  |
| --- |
| App-Specific Email Template |

## **Email Template 1: <specific app> Is Live with Okta!**

**Purpose of Email:**

To notify users that <specific app> integration with Okta is live.

**Recommended Timing of Delivery:**

Day of <specific app> cutover to Okta completion.

**Subject:**

Single Sign-On for <specific app> Is Here!

**Body of Email:**

We are excited to let you know that the next time you log into <specific app>, you will have a new single sign-on (SSO) experience. The integration of Okta with <specific app> is now live.

By now, you should have set up your preferences for multi-factor authentication (MFA) and self-service password reset (SSPR). You will need to complete this simple process before you use <specific app>. Please keep reading to learn more about the benefits you can expect and how you can set up your preferences if you have not done so.

**Yes, I have set up my preferences**.

Congratulations! If you previously set up your MFA and SSPR preferences, you have two options for logging into <specific app>:

* As you do today either through <insert link> or by using the <specific app> URL; or
* Using Okta Single Sign-On. Once you have gone through the enrollment process for Okta, you will be directed to a new dashboard experience where you can access <specific app> and any other applications that integrate with Okta.

As a part of the new log-in process, you will be required to successfully pass the MFA options that you selected during enrollment.

**No, I have not set up my preferences.**

Don’t worry—setting up your MFA and SSPR preferences for Single Sign-on is easy. Please choose one of the following options to set up your preferences and to start experiencing the new Single Sign-On solution:

* As you do today either through <insert link> or directly through the <specific app> URL. Click [here](https://mckessoncorp.sharepoint.com/sites/identity/SitePages/Workday%20Login%20Instructions.aspx#logging-into-workday-from-mcknet-current-url) for instructions <insert link>.
* Use the Okta dashboard. If you choose this option, you will set up your preferences through the Okta dashboard, where you will also be able to access <specific app> and any other applications that integrate with Okta. Click [here](https://mckessoncorp.sharepoint.com/sites/identity/SitePages/Okta%20Enrollment.aspx) for instructions <insert link>.

**What other benefits can you expect?**

You will now be able to perform a variety of activities on your own such as:

* Resetting your password directly from the login page
* Changing your password once logged in
* Updating your security question and password recovery options
* Unlocking your account
* Updating your MFA preferences

Click [here](https://mckessoncorp.sharepoint.com/sites/identity/SitePages/Okta%20Single%20Sign-On%20Intructions.aspx) for instructions <insert link> on how to perform any of the activities above and more.

**Questions or support?**

<Include methods for users to contact company support for more information. Example as below:

* For US users, please create a Support ticket through the self-service portal or by calling xxx-xxx-xxxx (US)
* For Canadian users, please contact Canada Support by [creating a ticket](https://newservicecatalog.mckesson.com/sc/catalog.product.aspx?product_id=create.an.it.service.desk.ticket) or by calling xxx-xxx-xxxx>

##