#

#

# Okta is Coming

Coming soon to your computer is Okta (AHK tuh). Like Zscaler, Okta is an industry-leading software system, aimed at alleviating password issues and securing IT services. Okta will help us: strengthen our security posture; answer Federal mandates; and close some pretty prevalent audit findings.

As you are well aware, we are constantly being challenged for passwords and other information to authenticate to the many applications that we use to do our job. Each system requires a different password! Wouldn’t it be great if you could log into one system which could then broker your connections to the other systems that you use, without the need for entering your password? That’s exactly what Okta is designed to do. Provide a single sign-on capability for other systems.

**What is Single Sign-On?**

Single Sign-On, or SSO, is exactly what it sounds like: you sign in once, and you have easy access to other applications you need, without being prompted to sign in for each one. Applications like PMA already use SSO. Logging into your government-issued computer will also get you logged into PMA when needed. Okta will allow us to do the same for systems like O365, WebTA, E2, etc.

**But wait, don’t throw away your passwords yet!**

While Okta will broker your connections to other systems, there are a few things that you must keep in mind:

1. Okta won’t work with all systems, at least not without some pretty intricate customization. Keep reading for a list of systems that will be supported immediately with Okta.
2. Even though Okta will handle your authentication, it is not able to “interfere” with each system’s requirement to change your password regularly. So, you’ll still need to change your password regularly with WebTA (for example), but Okta will remember it for you when you do change it.

**Last but not least, SECURITY!**

The IT security game is all about risk management, and Okta helps us to mitigate some pretty significant risks. The biggest one of those is two-factor authentication (2FA). 2FA is the use of something you know AND something you have for authenticating to systems. It is meant to mitigate the risks of having just your password compromised. As you know, we implemented the PIV card for authentication to your laptop which is a type of 2FA, but what about accessing your email from a web browser? Okta will help us to secure systems like these with 2FA. Keep reading to find out how!

# What to expect

Okta will be rolled out in two simple phases.

* Phase one begins on August 3rd. With phase one, you will be able to enroll a device (e.g. a cell phone) as your second factor for the 2FA process (more on this below). Phase one will also enable the first wave of agency-wide systems to be used in SSO (see Figure 1). AFTER PHASE ONE, TWO FACTOR AUTHENTICATION WILL BE REQUIRED TO ACCESS EMAIL FROM WEB BROWSERS!
* Phase two will be for integrating other applications with SSO. That’s right, even though we’ll be integrating some pretty big applications in phase one, we’ll continue to add apps to Okta for single sign on!

**Okay, Now that we’ve told you what to expect, let’s drill down a little into phase one:**

In order to make some of this magic happen, we’re going to need your help. We’ll need you to enroll a device for your second factor. The “what you have” in the 2FA process, because remember: when phase one is implemented, you will need a second factor for accessing Office 365 from non-government computers. For most of you, this will be a cell phone (either government-issued or personal), and for your convenience, we’re giving you a choice of two ways to use it in the 2FA process.

1. **SMS** – With SMS authentication, you will enroll a cell phone number that can receive text messages. Whenever a second factor is needed, a code will be sent to your enrolled device, and you will then enter that code as a response to the Okta challenge. This method is very similar to what many banks are using now to protect online access to your account.
2. **Okta Verify App** – This is an app for iOS and Android. With this method, when a second factor is required, the app will ask you to validate the access to the requested system. It’s just that easy!

We’ll be sending out videos and conducting “lunch and learn” sessions to show you exactly how to enroll and use these methods.

# SSO-Enabled Apps

The following applications will be SSO-enabled in phase one:



Figure 1 SSO-Enabled Applications

# FAQs

* What is Okta?

Okta is the foundation for secure connections between people and technology. Okta securely connects employees, partners, and customers to the applications and tools they need.

### 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 simply log into your laptop. From there, you can launch any of the enabled apps without having to enter any other additional credentials. For supported applications, Okta manages all your application credentials and securely logs you in. 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?

### 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.

#

# Contact and support

We will be holding two “Lunch and Learn” sessions to show you how to enroll a device, and to answer your questions about Okta.

Session 1: Tuesday, July 28th at 12:30pm eastern

Session 2: Thursday, July 30th at 12:30pm eastern

Service Desk:

Phone: 866-336-9972

ServiceDesk@ntsb.gov