CCSNH
Okta Multi-Factor Authentication (MFA)
FAQs

***Please Note: It is highly recommended that everyone sets up multiple MFA sources to avoid issues if a phone is lost or forgotten. An office phone is suggested for use as an alternative method if you are using a cell phone.**

- **What is Multi-Factor Authentication?**

Multi-factor Authentication "MFA" is a second authentication credential in addition to the traditional password you currently use. It is similar to the way your bank requires you to ask for a code before allowing you to access your account. The bank sends a text message to your phone as a secondary security check.

- **Why do we need MFA?**

Data breaches are occurring at an alarming rate. The information stolen can include usernames and passwords. Passwords alone are not sufficient to protect critical data. MFA reduces the risk to a great extent.

- **What systems will require MFA?**

Office 365 applications (Outlook, Teams, One-Drive, etc.), Canvas, Student Information System, Banner, Zoom, myCCSNH, Adobe Sign, Adobe Creative Cloud.

- **How long will sessions stay active after authenticating with MFA?**

12 hours. Please see ***When will I need to use MFA*** for more information on this.

- **What is a session?**

A session consists of the data or files that are persistent throughout the use of a web browser. When you open a browser and login, that session begins. For as long as that browser stays open, the session is still alive. You can open various tabs on that browser and won't need to authenticate again. If the browser is shut down, the session will end. Sessions are individual to the browser type (Firefox, Chrome, Edge, Safari). If you have a session open in Firefox and open another Chrome browser, you will be forced to authenticate again as that is a different session.

- **If I use the Outlook application, will I still need to perform MFA every day?**

No, the Outlook application keeps a token that allows you to maintain a connection for up to 90 days. Only browser sessions timeout after 12 hours. Please see ***When will I need to use MFA*** for more information on this.

- **When will I need to use MFA?**

You will need to use MFA every 90 days when logging into Office 365 applications on your desktop, laptop or mobile devices. You will need to use MFA after 12 hours in each browser that you use to access one of the following applications: Office 365 (Outlook, Teams, One-Drive, etc.), Canvas, Student Information System, Banner, Zoom, myCCSNH, Adobe Sign, Adobe Creative Cloud. If you close a browser session, use a private browser session or clear your cache, you will need to use MFA again.

- **If I use the Canvas application, will I still need to perform MFA every day?**

Yes, the Canvas app is just an interface for the web browser session.

- **Will I need a mobile phone?**

Using the Okta Verify mobile application on a smartphone is the recommended factor as it is the most secure. If you do not own, or choose not to use your cell phone, you may select the Voice Call Authentication factor as an option instead. This allows the use of a home phone, land line, office phone, or alternative phone number. Please note that the Okta Verify app is NOT available for Windows or Mac OS.

- **Can I use my personal email as an MFA method?**

No, unfortunately, this feature is not supported and is not allowed.

- **What happens if I don't have a cell phone or don't want to use my personal device?**

Using the Okta Verify mobile application on a smartphone is the recommended factor as it is the most secure. If you do not own, or choose not to use your cell phone, you may select the Voice Call Authentication factor as an option instead. This allows the use of a home phone, land line, office phone, or alternative phone number.

- **What if I never receive a verification code or push notification?**

If you are using voice call authentication, you must press the "Call" button within the Okta prompt to receive the code. If you are using SMS text authentication, you must press the "Send Code" button within the Okta prompt in order to receive the code. In addition, network related reasons can cause a delay in notification of the verification code or push notification. If you haven't received a code after a minute or two, try sending it again or choosing another factor. If you still have not received anything after that, please contact your local IT help desk.

- **How can I simplify the two-factor authentication login process?**

By utilizing the Okta Verify app from the Apple or Android store on your mobile device and selecting the 12 hour "Remember this device" option upon the first login of your session.

- **If I use the Okta Verify app on my personal cell phone, will CCSNH have access to or be able to view what I do on my personal device?**

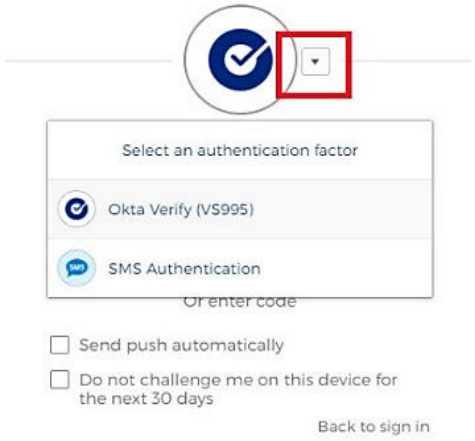
No, the Okta application is only used for the push notification or an authentication code. There aren't any management profiles applied at all on the device.

- **How will I get a code if I'm out of cell phone range?**

The Okta Verify app acts as a code generator as well. Open the app and check for the Authentication Code that is always changing.

- **How do I change my MFA method?**

Log into your account. Before you send a code, select the drop-down box to the right of the Okta logo (see screenshot below). Choose your preferred method for MFA.



- **What do I do if my account gets locked?**

For security purposes, your account will automatically lock after ten incorrect login attempts. You will need to wait 15 minutes for your account to unlock and then try again. If your account does not unlock after 15 minutes, please contact your local IT help desk.

If you have any questions, please contact your local IT department. Contact information for each location can be found at the bottom of the CCSNH Online Resources page: http://resources.ccsnh.edu.