Okta Tutorial

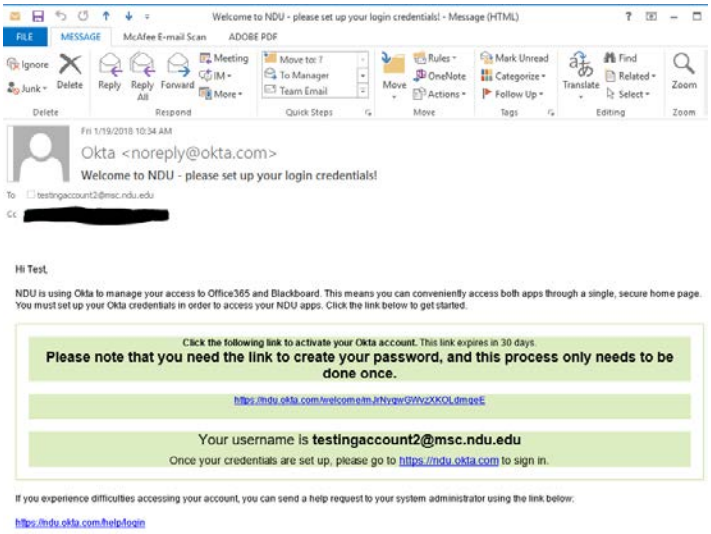
What is Okta?

Okta is a Single Sign-On solution to allow students and faculty to use one set of credentials to connect to multiple applications and services.

Okta Enrollment

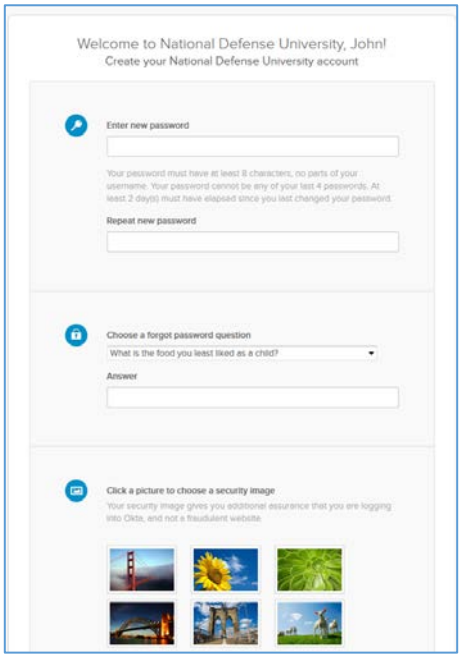
Step 1 – Activation email

You will get an email with an activation link and instructions on how to set up your Okta account.



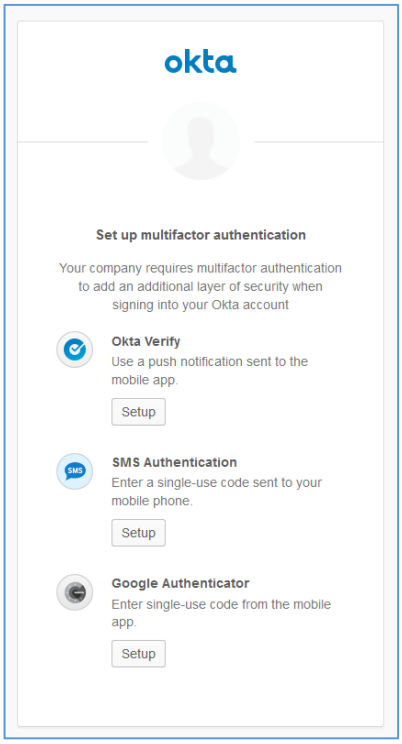
Step 2 – Account Setup

Please complete the new account activation form.



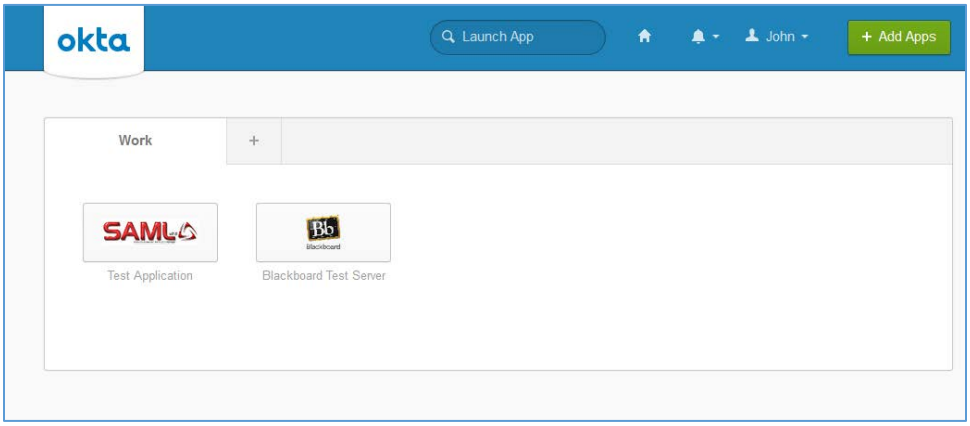
Step 3 – Set up Multifactor Authentication (MFA)

Please select one or more MFA methods you would like to use to access your account. If unsure, please use Okta Verify as the MFA method. Please refer to the MFA section below for additional details.



Step 4 – Log in to one of the applications

You will see a list of available applications. Please note that your main application screen may look different than the one illustrated below, because not everyone has access to all applications.



Single Sign-On

1. Go to the Okta Login Page (https://ndu.okta.com).
2. Enter your username and password (as established in Step 2 above).
3. Select an MFA method and authenticate.
4. Select an application from the list to log in.

Multifactor Authentication (MFA)

MFA is used as an additional security measure. After logging in with a username and a password, you must prove your identity with one of the additional authentication factors. Acceptable MFA methods include:

- **Okta Verify**, which requires a confirmation through an installed app on your smartphone.
- **Google Authenticator**, which generates a one-time code. Please note this option does not send data to any online services and does not require an Internet connection on the mobile device.
- **SMS verification** which sends a text message with a code.

The following table summarizes the pros and cons of the MFA methods

MFA Method	Pros	Cons
Okta Verify (Preferred method)	• The most convenient method – the user simply taps the "Approve" button on the phone when prompted.	• Okta Verify is a separate app that must be loaded on the user's phone or tablet • Okta Verify requires Internet Connectivity on the device
Google Authenticator	• Google Authenticator is used by a number of other online services • Users don't have to install an additional app if they already use Google Authenticator • This method does not require connectivity on the end user's smartphone	• Google Authenticator generates a time-sensitive code that must be then entered into the Okta login screen, which is not as convenient as Okta Verify
SMS Verification	• Works on phones that cannot run applications required for the other MFA methods • Does not require Internet Connectivity	• Not as secure as the other options • Slower and less convenient than other options

Okta Verify is the preferred MFA method that should work best for most of NDU users.