Multi-Factor Authentication for first time users

**Multi-Factor Authentication will be required for all Duke University accounts on July 1st, 2016.**

What is Multi-Factor Authentication (MFA)??

Multi-factor authentication, also referred to as advanced or two-factor authentication, providing an additional layer of security when logging in or performing transactions online. When logging in, a user is required to enter a password and also authenticate using a second factor, typically a phone or hardware token.

Simplified – MFA requires a user to enter a secondary password when logging into specific Duke websites. This secondary password can be retrieved through your office/home phone, cell phone, mobile device, the smartphone Duo Mobile app, or by using a hardware token called a YubiKey. If you do not have access to any of these resources, a user can also retrieve temporary pass codes that can be used for a 72-hour period.

What does a MFA login look like?

When accessing a website that requires MFA to login, once a user types in their NetID, an additional field will appear under the password called Advanced Verification. This Advanced Verification section will offer the different ways in which you can retrieve your MFA information, either via a radio button selection or by inputting a passcode or YubiKey information in the text field.

To prevent a user from having to use MFA every time they log into a MFA protected Duke website, check the box next to “Remember this device for 12 hours” and this specific machine will now longer require MFA for the next 12 hours.

A user may select which Duke websites require MFA on the Multi-Factor Authentication website but the OIT Self Service page and the Duke@Work page are required.
Configuring Multi-Factor Authentication

**It is recommended that you configure MFA at your home/office so you have access to your home/office phone for initial configuration**

Home/Office phone Configuration

1) Log onto the OIT Self Service website by going to [http://oit.duke.edu/selfservice](http://oit.duke.edu/selfservice).

2) Once on the OIT Self Service page, click on the Multi-Factor Authentication link located on the right.

3) This will take you to a security challenge-response question page. These questions are used for password recovery or retrieving temporary MFA pass codes. Fill out the form and then press Continue.
4) On the Add phone or tablet page, enter the following:
   - In the first dropdown, select Home/office phone
   - Enter your 10 digit home or office phone number
   - Leave the Extension field blank
   - Give this phone a nickname (Home phone or Office phone)

![Add phone or tablet]

5) This takes you to a completion page that shows you the new MFA options you will see in the Advanced Verification section and what they will do. Click on the preferences page link to take you to the Multi-Factor Authentication website.

![Choose websites]
Smart Phone Configuration

1) If you’re not already there, log into the OIT Self Service website by going to http://oit.duke.edu/selfservice. Click on the Multi-Factor Authentication link on the right.

2) On the OIT Self Service website, click on the Add a smartphone or tablet link located on the right under the Manage Devices section.

3) On the Add phone or tablet page, enter the following:
   - In the first dropdown, select Smart phone
   - Select your phone operating system
   - Enter your 10 digit smart phone number
   - Give this phone a nickname (Cell phone)
4) This will direct you to a page asking you to download and install the Duo Mobile app. This is a free app that can be downloaded in the Google Play Store (Android devices) or the App Store (Apple devices).

5) On your smart phone, open the Duo Mobile app once installation is complete. Click on the **Add Account** button which will turn on the camera on the phone. If the app asks for permission to use the camera feature, select Yes.

6) Back on the Multi-Factor Authentication website, scroll to the bottom of the page where you will see a QR code. Hold your mobile phone in front of the screen so the camera will see and scan the QR code. No need to press any buttons, once the QR code is in focus it will recognize it.
7) You should now see Duke University listed in your Duo Mobile app.

8) Click **Continue** on the MFA smart phone setup page and you will be taken to a completion page that shows you the new MFA options you will see in the Advanced Verification section and what they will do. Click on the **multi-factor authentication home page** link to take you to the Multi-Factor Authentication website.
Generate Temporary Pass codes

If you are unable to use any of the MFA resources needed to login, you can generate temporary pass codes that will last for 72-hours and will allow you to login in.

1) When you go to a Duke website that requires MFA to login, type in your NetID so the Advanced Verification section will appear and then click on the **What are pass codes?** Link.

2) This will take you to an OIT FAQ page for Multi-Factor Authentication explaining what pass codes are. On the third bullet point for Temporal pass codes, click on the multi-factor authentication home page link in the last sentence.

3) This will take you to a login page that only requires your NetID and password.
4) Once logged in, this will take you to a page where you will need to answer a couple security questions you configured at the start of this guide. Answer the questions and press Submit.

5) You will now be giving 10 temporary pass codes that are good for a 72-hour period. Each pass code may only be used once.

6) Go back to the MFA protected Duke website, log in with your NetID and password and then enter one of the temporary pass codes in the text field under the Advanced Verification field to login.
YubiKey Configuration

A YubiKey is a hardware token that looks similar to a portable USB thumb drive. It is registered to the user’s NetID account and can be used on any computer. A user will plug the Yubikey into a USB slot and touch the gold circle to create a pass code to authenticate.

1) If you’re not already there, log into the OIT Self Service website by going to http://oit.duke.edu/selfservice. Click on the Multi-Factor Authentication link on the right.

2) Click on the Advanced Options link located under the Manage Devices section and then click on Register a hardware token (YubiKey).
3) This will take you to a 12 step guide on how to configure your YubiKey. Start by clicking on the link in Step 1 to direct you to a website to Download the YubiKey Personalization Tool.

4) On the Yubico website, scroll down to the 4th section titled Yubikey Personalization Tool and click on the Microsoft Windows Download link (for Windows machines) or the Mac OS X Download link (for Mac machines). Save and run the file to install the Yubikey Personalization Tool.

5) Plug your YubiKey into your computer. If you do not have a YubiKey, contact the TSC and they will provide you with one.
6) Open up the YubiKey Personalization Tool by going to the Start menu and typing in YubiKey in the search field. For Mac users, open your Spotlight search by clicking on the magnifying glass in the upper right and then typing YubiKey. Make sure the YubiKey Personalization Tool says **YubiKey is inserted** in the upper right and then click on the **Yubico OTP Mode** in the center of the window.

7) On the next screen, click on the **Quick** button.
8) This will take you to the configuration page for your YubiKey.

![YubiKey Configuration Page]

9) Under the Configuration Slot section, select the **Configuration Slot 1** radio button.

![Configuration Slot Selection]

10) Under the Yubico OTP Parameters section, click on the **Regenerate** button 2-3 times to make sure it gives you new values.

![Yubico OTP Parameters]

---

These instructions are for configuring your YubiKey for two-factor authentication. Make sure to follow the steps carefully to ensure your security.
11) Uncheck the Hide Values box.

12) Click the Write Configuration button.

13) On the pop-up window, click Yes to overwrite configuration slot 1 and then click Cancel when asked to save a configuration file.

14) Look back to the 12 step OIT guide to configuring your YubiKey and scroll down to the bottom. You will see Step 12 asks for 4 different text inputs.
15) You will find these inputs on the YubiKey Personalization Tool. Go ahead and input those values into the fields in Step 12. Leave the Optional field blank and press **Register YubiKey** when complete.

![YubiKey Personalization Tool](image)

12. Fill out the following information:

- **Serial number (located on the right; use the serial number associated with "Dec."):**
  
  2236055

- **Private Identity (the private identity has spaces; it is okay to either include them or leave them out.):**
  
  42 6c db 7e 00 b0

- **Secret Key (the secret key has spaces; it is okay to either include them or leave them out.):**
  
  2e 99 30 ff 5d ff 91 09 c5 d7 11 06 a2 43 5f

Optional: If you are an IT administrator authorized to use test and service accounts, you can associate

![Register YubiKey](image)

16) This will take you to a completion page where you can click on the **multi-factor authentication home page** link to take you back to the home page.

![Your changes have been made.](image)
17) To authenticate using the YubiKey, make sure it is first plugged into the computer. When you navigate to a MFA protected Duke website, enter your NetID and password and then place your cursor into the text box under the Advanced Verification section. When your cursor is in the text box, touch the gold circle on your YubiKey for about a second and encrypted text will auto-fill and log you into the site.
Quick Multi-Factor Authentication Homepage Overview

- The Website Preferences section on the left is where you can select which sites you would like MFA to be used for. Duke requires that you have MFA on the OIT Self Service page as well as the Duke@Work website.

- The Manage Devices section on the right is where you can manage which devices are set up for MFA as well as adding or removing devices.