Duke Clinical Research Institute

Multi-Factor Authentication

Quick Reference Card

Enrolling and Using MFA

Overview

The Multi-Factor Authentication (MFA) feature is a crucial security measure that protects your account and DCRI assets. This quick reference card (QRC) details how to enroll in the service, set up notification options, and use this two-step authentication feature.

How MFA Works

A website/web app that has MFA enabled prompts you to enter your NetID/password, and then prompts you to authenticate using a *second* factor (such as answering a phone call, pressing the Approve button on a smartphone/tablet, or entering a code). With MFA enabled, even if a hacker gains access to your password, they are unable to login to your account without the second factor.

MFA is *automatically* applied to every user using a remote access application (Cisco AnyConnect or Citrix Receiver). Employees and Contractors also have the option of placing MFA on specific websites and web apps of their own choosing (at a minimum, Duke@Work).

To use MFA, you must enroll on Duke's Office of Information Technology (OIT) website. During this process, you select up to four "second factors" (see the callout box below) that best suit your work situation. You select *one* of these notification options each time you use MFA.

Notification Options ("Second Factors")

A typical option is having the system place a phone call to your choice of phone (work phone, basic cell phone, smartphone, or other—you can list up to four phones). A recorded voice advises you to press any number on the phone's keypad, and then hang up. Depending on the style of MFA fields, you might need to also click **Enter**.

Another option is to have the system push a notification to the **Duo Mobile** app on your smartphone or tablet. In this case, you would tap the **Approve** button on the app. Or, you can have the app generate a passcode you enter into the appropriate MFA field. Duo Mobile is a free app you can download from your choice of app store.

You also have the option of entering a code from a list sent to you by **SMS**. These codes do not expire until they are used.

Finally, you have the option of purchasing **YubiKey** hardware. After you plug the hardware into your computer's USB port and touch the gold disk, you enter the code it creates into the appropriate MFA field.

Tips:

- You are free to add or delete the devices (phones, tablets, and YubiKeys) for these notification options at any time.
- The OIT website provides additional information at: https://idms-mfa.oit.duke.edu/mfa/help

Enrolling in the Service

1. In your choice of browser, go to oit.duke.edu/mfa.

   The Multi-factor authentication page appears.

2. Read about the feature, and then click the **Enroll in MFA Now** button.

   The Duke sign-in page appears.

3. Enter your NetID and password, and then click **Enter**.

   The Multi-Factor Authentication page appears.

4. If you are a DCRI employee or contractor, make selections in the **Website Preferences** section. Otherwise, proceed to Step *5*.

   Note: You have the option of placing MFA on *all* NetID-protected websites. Otherwise, you can specify particular sites. *Always* select Duke@Work. When done, be sure to click the **Submit** button.

5. In the **Manage Devices** section, specify up to four devices (total, across all options).

   Tips:

   - Clicking a plus sign either expands a category with more information or (when adding a device) opens a new page.
   - Clicking a minus sign collapses the category.
   - To add a smartphone or tablet, download and install the **Duo Mobile** app on the device before you enroll it. This free app is available at most app stores.
   - The sequential order in which you list devices can have importance on sites that have single Passcode fields for MFA (see the "Style 2: Single Passcode Field" section). For this reason, consider writing down what you enter in this area for future reference.
   - Use **Advanced options** to register YubiKey hardware.

- To view a list of the devices you already have registered, go to the **View Devices** section at the bottom of the page's left column.
- You can skip the other sections on the page.

6 Since updates to the **Manage Devices** section are saved as you make changes, you can simply click the **Sign Out** link in the upper right corner of the page to exit.

Important! Changes you make to the **Website Preferences** section are not saved until you click **Submit**.

The Duke Log Out page appears.

7 Since you have finished making changes, you can click the **Log Out** button.

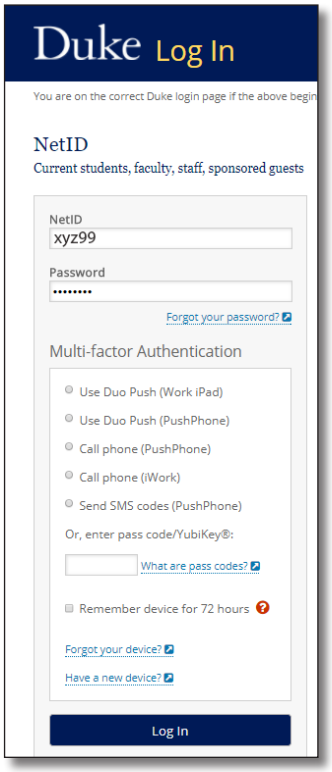
Note: If your email address is known to the system, you receive email notifications after you make changes to your MFA settings.

Using MFA

When you access a site or application that has MFA enabled, you view one of two different styles of MFA fields.

► Style 1: Multiple Fields

Most sites, such as the Duke LMS or Duke@Work, begin as the standard Duke log in page. Then, once you enter your Password, a new set of fields appear under the Password field, based on the notification options you set at the OIT website.



First, select the the authentication method you want to use this time. Then, complete the authentication process. As examples, depending on the method you select, you might need to answer a telephone call (then press any number on the keypad and hang up), approve a notification in the Duo Mobile app, or simply enter a code.

Tip: If you select **Remember this device for 72 hours**, then—after authentication—you bypass MFA authentication for the next 72 hours, *provided* you log in with the *same* computer, IP address, and browser. (For safety, you are still prompted to enter your NetID and password.)

Then, click **Log In** or **Enter** (the button varies from site to site).

► Style 2: Single Passcode Field

A few sites offer only a single field for MFA. If you have a YubiKey code, Duo Mobile code (by tapping the app's key icon), or an unused SMS (Short Message Service) code, enter it into this field. Otherwise, you are expected to enter one of the following *words*:

- Enter **phone** to have the system call the top phone you listed in the OIT website. You can enter **phone2** or **phone3** to have the system call the second or third phone on your list.
- Enter **push** to have the system push notification to the Duo Mobile app on the top smartphone or tablet you listed in the OIT website. You can enter **push2** or **push3** to send to the second or third device on your list.
- Enter **sms** to have the system send you a batch of passcodes. Enter one of them to authenticate this session.

As needed, complete the authentication process. For example, answer a telephone call (then press any number on the keypad and hang up) or approve a notification in the Duo Mobile app.

Then, click **Enter** or **Log On** (the button varies from site to site).

Getting Help

If you have questions or comments about the content of this QRC, please email IT Training [**dcriittrain@dm.duke.edu**]. If you experience any technical problems working with Multi-Factor Authentication that you are unable to resolve, email the DCRI Service Desk [**dcriservicedesk@dm.duke.edu**] or, for time-sensitive issues, call them Monday through Friday (6 a.m. to midnight, Eastern time, except holidays) at 919.668.8916.