Multi-factor Authentication Guide

Contents

Multi-factor Authentication Set Up

In order to prevent unauthorized access, Multi-Factor Authentication is required when accessing certain web apps from off-campus. You can choose to receive a phone call, or SMS text message with a verification code in the event you are unable to install the authenticator application; however, the authenticator application is the recommended method for validating your identity.

Note: Registering a device gives your device access to your organization's services and doesn't allow your organization access to your device. Read more about MS Authentication at https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-faq

Prerequisites:

Download the **Microsoft Authenticator Application** to your mobile device. This can be downloaded to any Android or iOS device.

1. Go to the **App Store** on your device and search for the **Microsoft Authenticator**.

2. Once you find the Microsoft Authenticator application, tap **Get** or **Install**.

The app will start to install automatically. Once this download has completed, **do not attempt** to setup the Authenticator without first reading the rest of the instructions.

Recommended Method: Set Up Multi-factor Authentication

1. Complete the prerequisites section.
2. You need to have your mobile device available for this, **but do not use** your mobile device to **initiate the setup**.
3. From a workstation go to https://aka.ms/mfasetup (Open a web browser window and type in the address then press **Enter**.

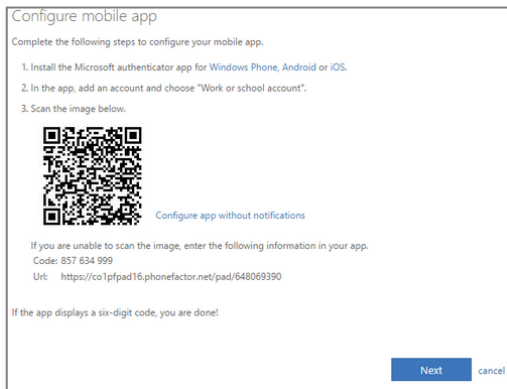4. You will be notified that you must provide additional information, click **Next**.

5. On the following page, click the radio button to **Receive notification for Verification** and click **Set Up**.

6. A **QR code** prompt will appear. Read the next step do NOT click Next.

7. Open your mobile phone **(If you haven't installed the Authenticator application refer to the prerequisites)**. In the **Microsoft Authenticator** application choose **Work or School account**. This will automatically open the camera on your cell phone. Simply hold your phone up to the screen so your camera captures the **QR code.** Once successful, a 6-digit code appears on your cell phone, you may now click **Next** on the computer screen (see above image).
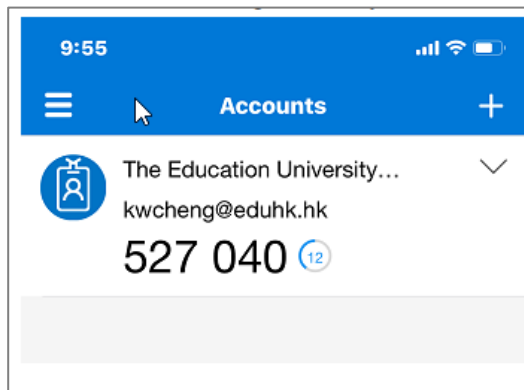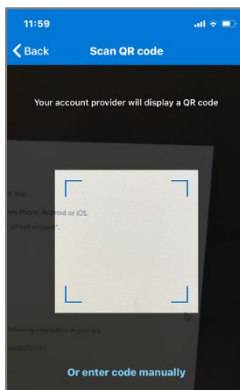

You might see a timer counting down next to your active verification code. This timer is so that you never sign in using the same code twice. Unlike a password, we don't want you to remember this number. The idea is that only someone with access to your phone knows your code.
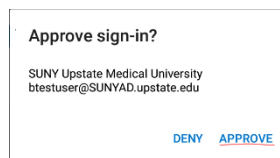
8. It may take up to **3 minutes** to verify the application for the first time. Once you see **Mobile app has been configured for notifications** click **Done**.

9. The system will send a notification to your mobile device. Tap **Approve** from your mobile device.

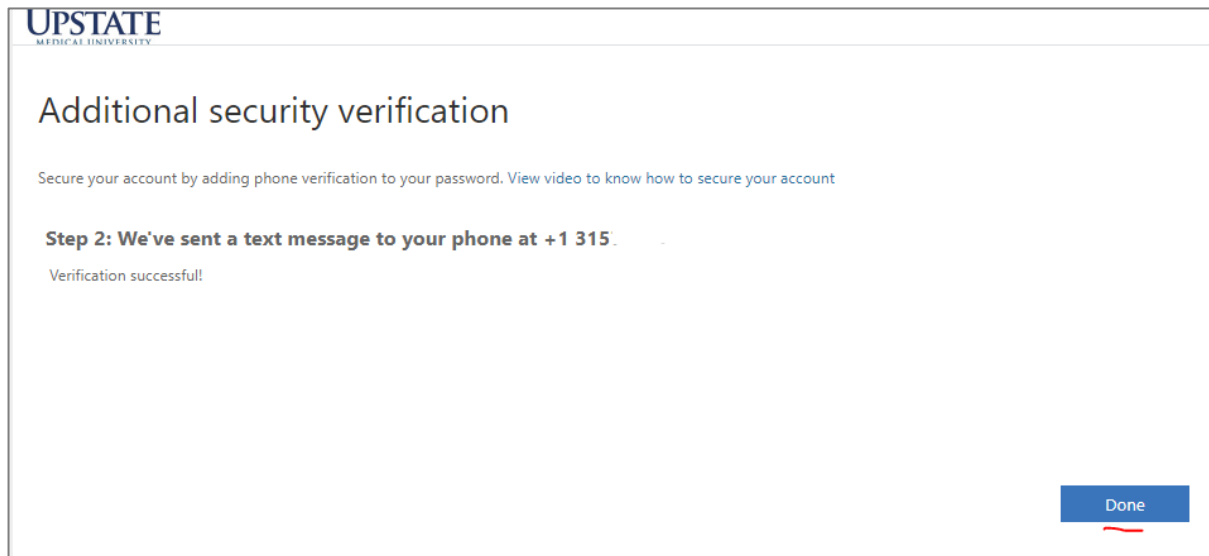(This message will appear on your cell phone, not your computer)
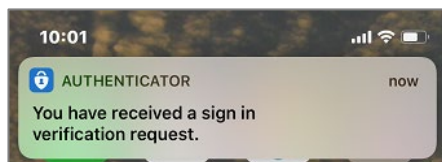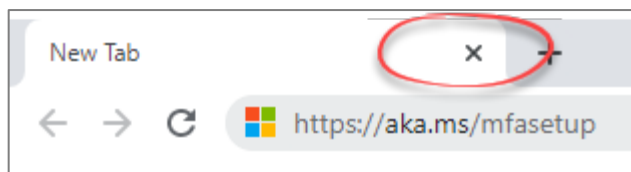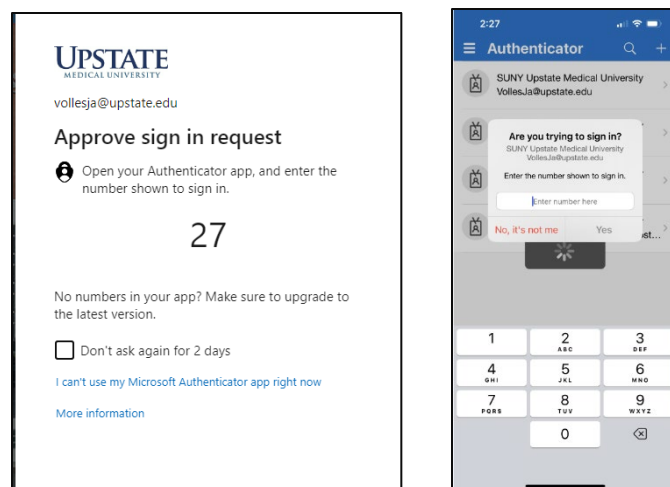

iPhone

Android

10. If you see the screen below, you have successfully enabled MFA for your account!

11. Click **Done** and close your browser (click on the tab's x).

12. When you sign in from on campus, only your password will be required. When attempting to sign in remotely, you will need to approve the request from your mobile device using a verification code as shown below:

Alternative Method 1: Text Message

If you choose to NOT use the recommended method above, you can text a code to your mobile device. When you specify this method, instead of using the multi-factor authentication method, you'll get a verification code as part of a text message on your mobile device. You must enter this code into the verification prompt for your work or school account.
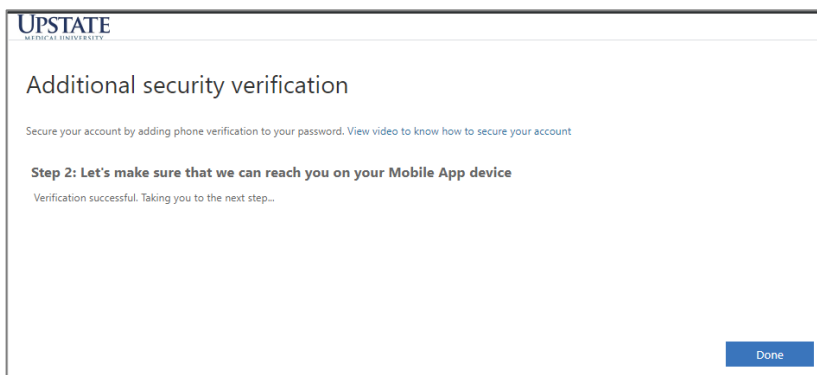
1. From a workstation, open a new web browser window and type https://aka.ms/mfasetup , then press **Enter**.

2. You will be notified that you must provide additional information, click **Next**.
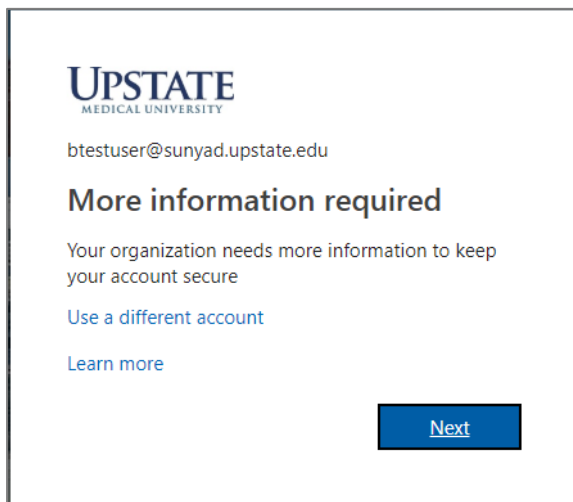
3. From the drop down ensure "**Authentication phone**" is selected.
4. Set your phone number and country code.
5. Switch the radio button to **Send me a code by text message.**

6. Click **Next.**

7. You'll receive a code to your cellphone, enter that number on the next screen and click **Verify.**
8. Give it some time to validate, don't close the screen until you see this screen. You can now click **Done.**
9. At the **Additional security verification** screen, close your web browser.

Alternative Method 2: Validate with a Phone Call

If you choose to use this method, you will not use the recommended method (through the authenticator app, or the text code method above). When you use this method, you'll get a phone call on your mobile device, asking you to verify your information.

1. From a workstation, open your web browser (Chrome, or FireFox, etc.) and type into the url address window: https://aka.ms/mfasetup, then press **Enter**.

2. You will be notified that you must provide additional information, click **Next.**

3. From the drop down ensure **Authentication phone** is selected. This should be your mobile device.
4. Set your phone number and country code.
5. Switch the radio button to **Call me** and click **Next**.

6. Give it a moment to call your phone. When you receive the call, follow the instructions (they should say press **#** to continue). Once the screen switches to **Verification successful**, click **Done**.
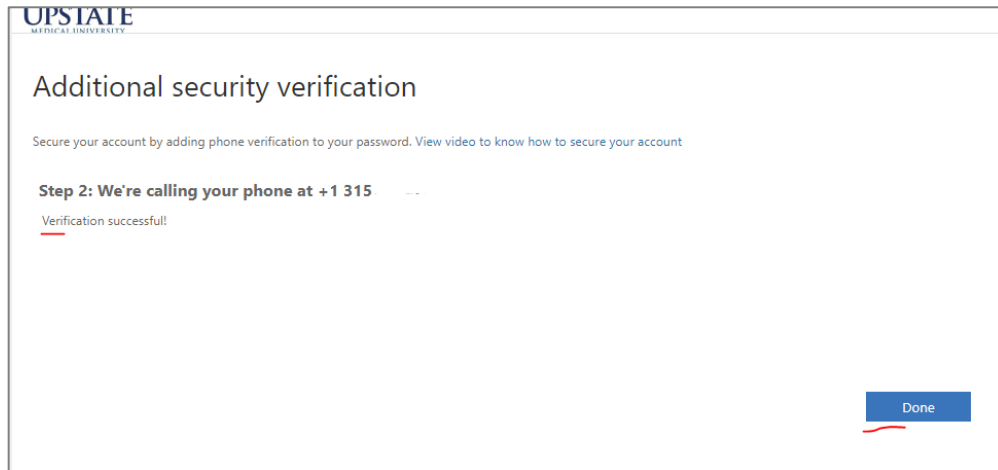
7. You'll be taken back to the **Additional security verification** home page now. Close your browser by clicking the X on the web browser tab.