

Microsoft Authenticator Setup

Multi-Factor Authentication (MFA) is a requirement for all faculty, staff and students to access university resources and services. MFA is a way of confirming your identity and is a critical security protocol.



To begin this setup, you will need your cell phone and a PC/laptop so that you can scan QR codes with your phone.

Setup Process:

Download and install the Microsoft Authenticator app from your mobile device app store or scan the QR code below based on your operating system:

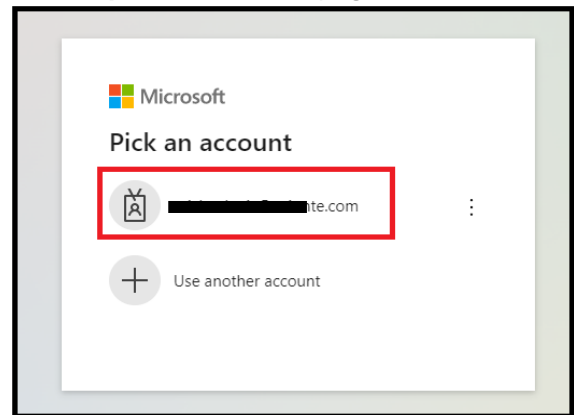
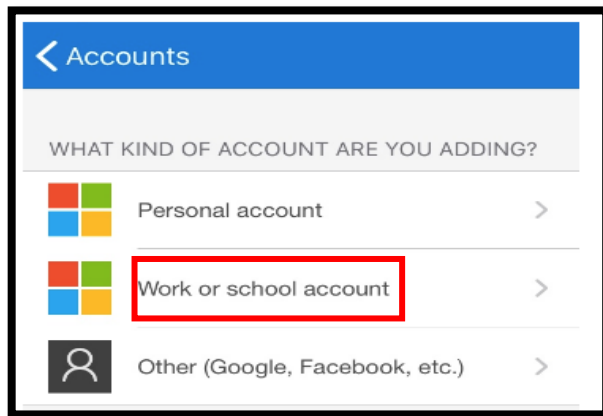
Android:



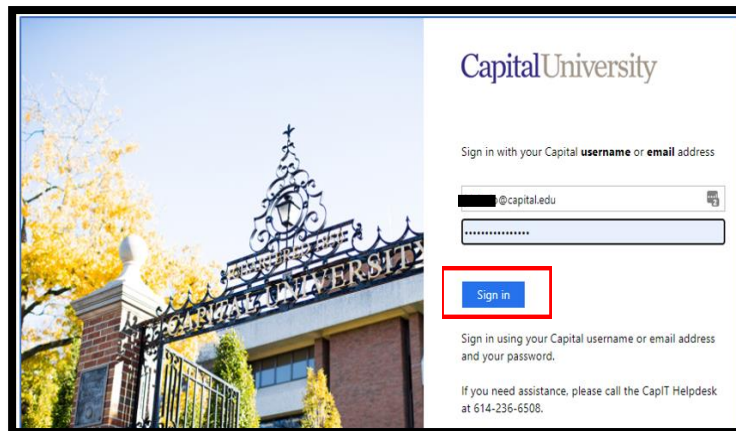
Apple iOS:



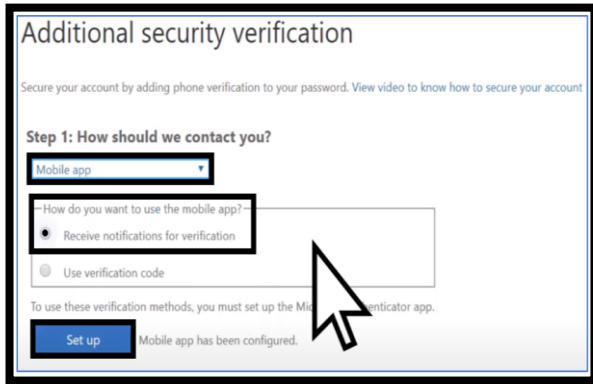
1. Open the app. Tap “next” until you see “add work or school account”. Choose **allow notifications**. Put this screen on **hold** and move to next step. We will come back.
2. Go to your PC/laptop, open a web browser and type <https://aka.ms/mfasetup>. Select your Capital email address. You will be re-directed to the “Capital Gate” web page.



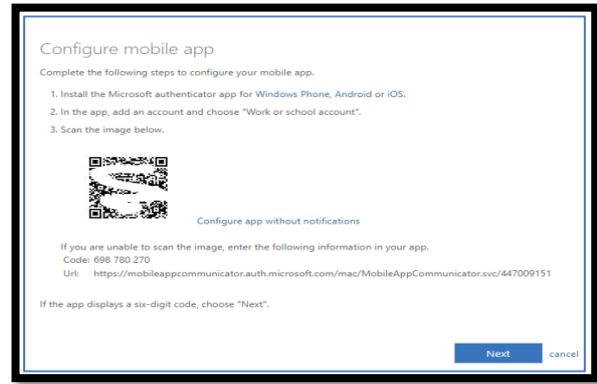
3. Enter your Capital University email username and password credentials and hit “sign in”



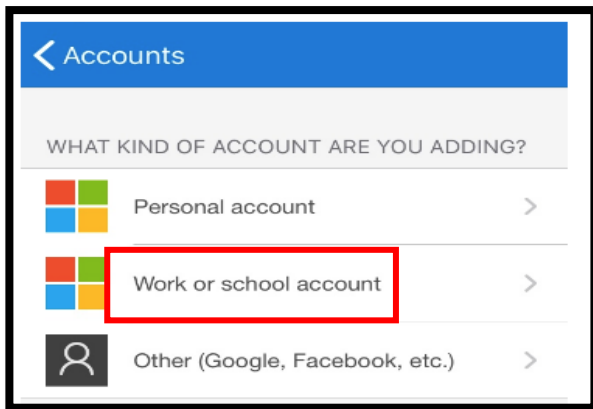
4. Select **“mobile app”**, **“receive notifications for verification”** and then hit **“set up”**



5. You will see a QR code on the screen. This QR code is personalized for you only



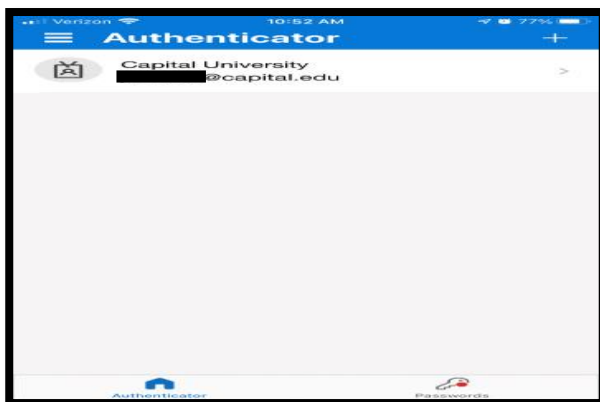
6. Go back to your phone; go to the authenticator app and select **“work or school account”**



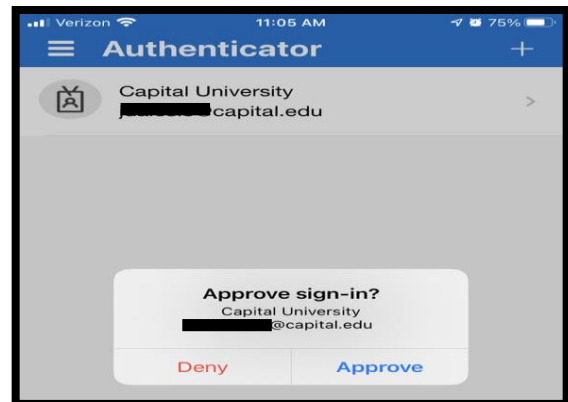
7. Scan the **“QR code”** on your PC with the *authenticator app’s* QR scanner on your cell



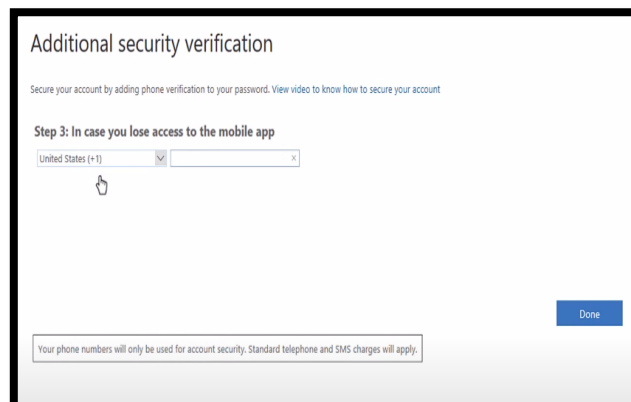
8. Your account should now be setup on the app after scanning the QR code



9. On your PC screen with the QR code, click **“next”**. Then select **“approve”**



10. Enter a phone number just in case you lose access to the app, then click **“done”**



Microsoft Authenticator
Setup 2025/OneDrive