How to Set Up MFA – Multi-factor Authentication – using the Microsoft Authenticator App – for Students

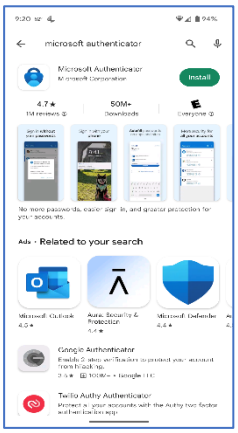
For assistance, please call the DormNet Help Desk – (501)279-4545

To set up MFA using the Microsoft Authenticator app, you will need the following:

- ❑ **Computer** – laptop or desktop
- ❑ **Mobile Device** – smart phone or tablet with a camera that is capable of installing the Microsoft Authenticator app – this is the device you will use each time you authenticate your log in

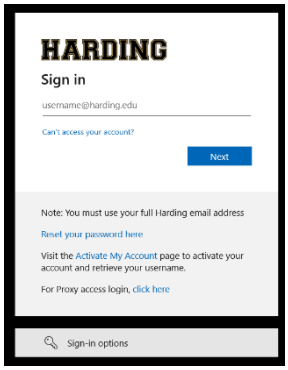
STEP ONE – Use your MOBILE DEVICE

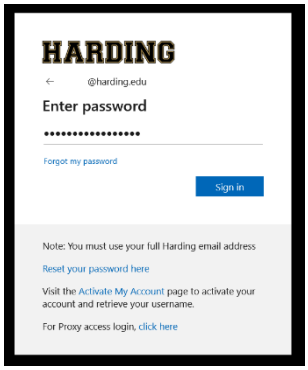
- ❑ Download and install Microsoft Authenticator
- ❑ **DO NOT OPEN THE APP until later**



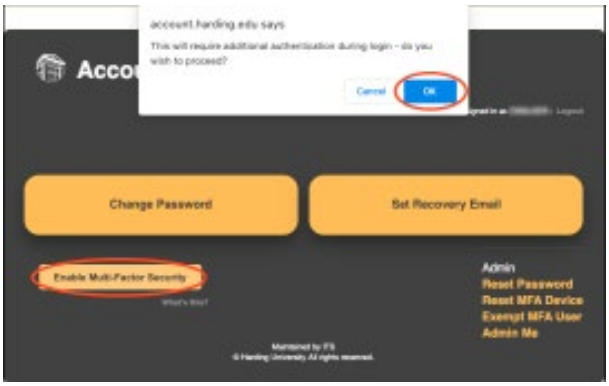
STEP TWO – Use a COMPUTER

- ❑ **For best results, use an incognito browser window/private browser window**
- ❑ Open a browser and type in ***account.harding.edu*** in the address bar
- ❑ Sign in with your Harding email address and your password



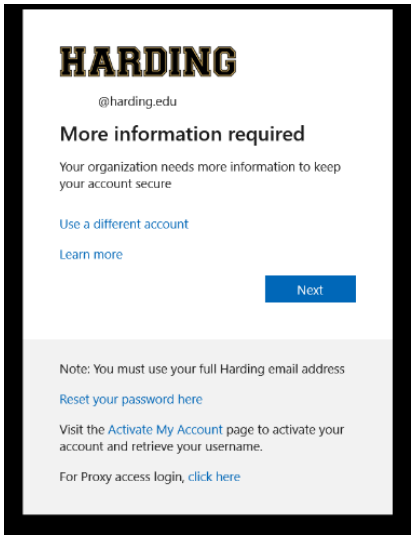


- ❑ Click ***Enable Multi-Factor Security*** and click ***OK*** on the screen that pops up

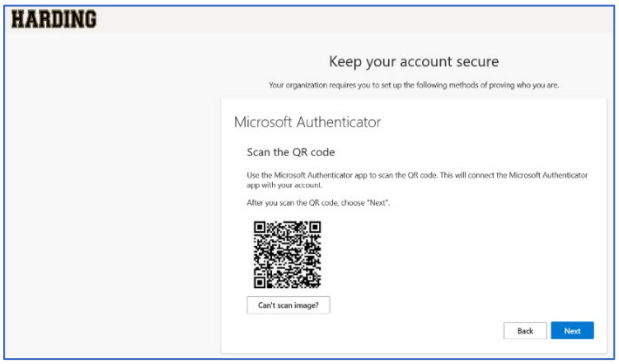


- ❑ When you see the message "***You signed out of your account***", close all open browser windows
- ❑ Open a new browser window and type in ***connect.harding.edu*** in the browser window

- ❑ Sign in again with your Harding email address and password
- ❑ You will be asked for more information – click ***Next***

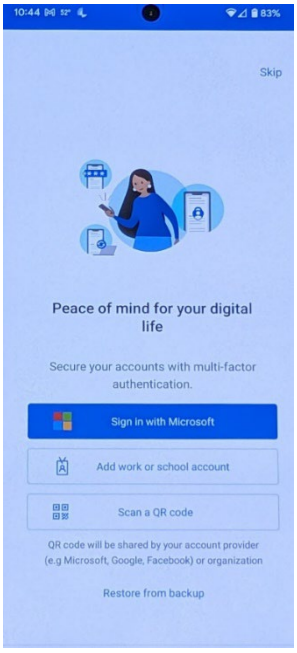


- ❑ Click on ***Next*** through the next two screens until you see this screen

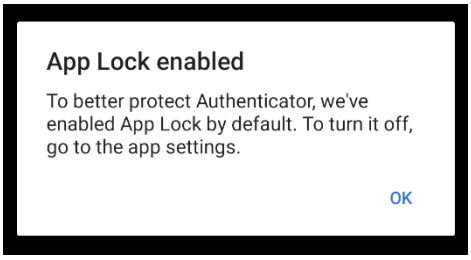


STEP THREE – Use your MOBILE DEVICE

- ❑ Open the Microsoft Authenticator app on your mobile device
- ❑ You may be prompted to allow Authenticator:
  - Send you notifications – click on ***Allow***
  - Allow access to your camera – click on ***While using this app*** or ***OK***
  - Use FaceID – click on ***OK***
- ❑ You will be asked to accept the Privacy Statement – click on ***Accept***
- ❑ Click ***Continue*** when prompted
- ❑ Click ***Scan a QR code***
- ❑ Point your mobile device's camera at the screen – it will scan the QR code

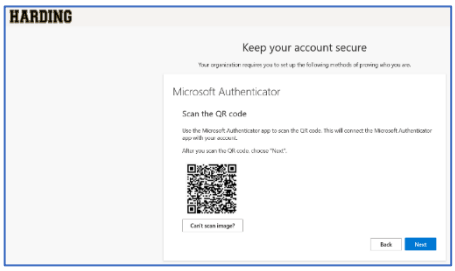


❑ App Lock may be turned on by default – click ***OK*** – you can change this later



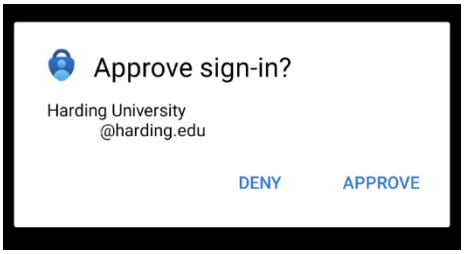
STEP FOUR – Use your COMPUTER

❑ After the QR code has been scanned, click on ***Next***



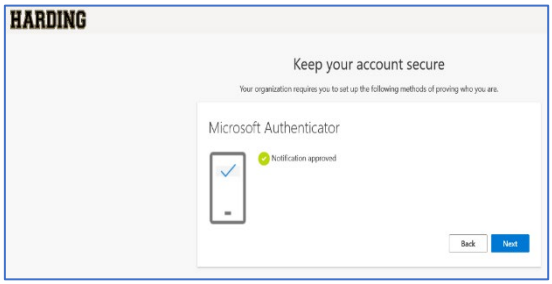
STEP FIVE – Use your MOBILE DEVICE

❑ Click on ***Approve***
❑ If prompted, enter your biometric data or use your PIN to sign into your mobile device

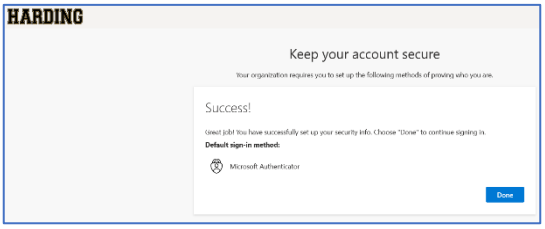


STEP SIX – Use your COMPUTER

❑ Your notification should be approved – click ***Next***

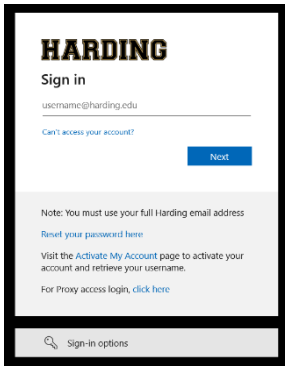


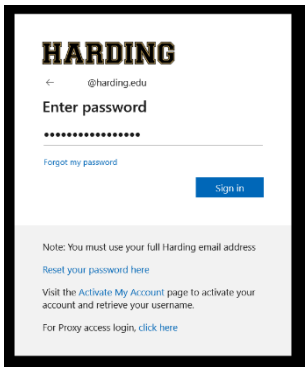
❑ Click ***Done***
❑ You should now be logged in



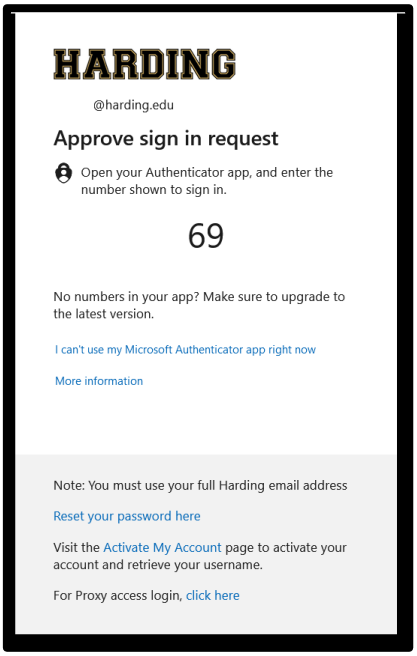
❑ On the "Stay signed in?" screen, answer ***No*** on any shared/public computer

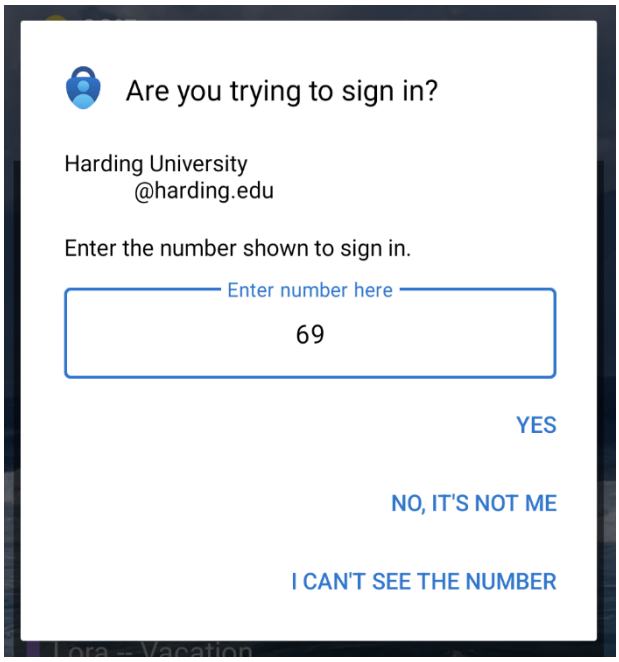
- ❑ Sign in with your Harding email address and your password





- ❑ You will then be prompted to "approve" the sign in request
- ❑ Type in the number you see into your approval screen on your mobile device (it will probably be different than what you see here)
- ❑ Click **Yes**





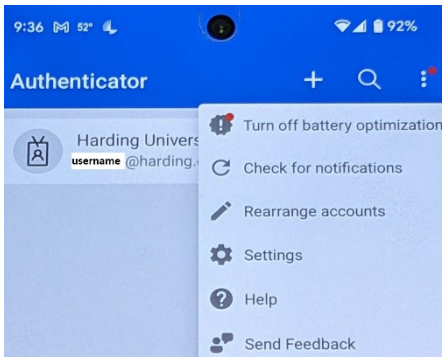
- ❑ You should now be logged in

To Turn Off the App Lock Feature

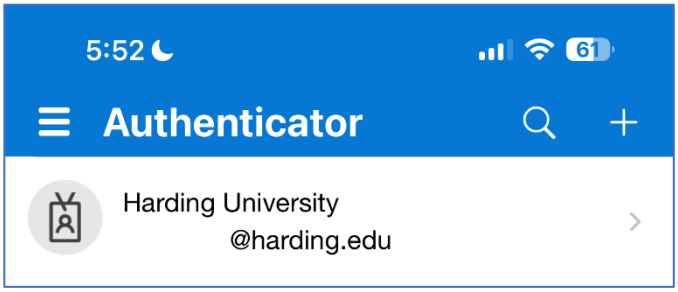
STEP SEVEN – Use your MOBILE DEVICE

To turn off the App Lock feature:

- ❑ Open the Microsoft Authenticator app



Android: Click on the ***three dots*** on the top right



Apple: Click on the ***hamburger menu*** on the top left

- ❑ Click on ***Settings***
- ❑ Under Security, turn off App Lock
- ❑ Now, you should no longer be required to enter your biometric data or PIN when signing in to Authenticator