



# Michael Garron Hospital Microsoft Authenticator Setup

## Multi-Factor Authentication (MFA)



This guide includes 2 methods for completing the MFA setup.



If you do not have access to a computer, use the phone-only setup instructions.



If you need help, please contact the IT Help Desk at 416-469-6580 ext. 2000 or [helpdesk@tehn.ca](mailto:helpdesk@tehn.ca).

# Before you begin

A few important things to know before setting up or testing Microsoft Authenticator.



## After you complete this setup

Performing any of these actions will prevent Authenticator from working.



Deleting Authenticator



Disabling notifications for Authenticator



Removing your account from Authenticator



Replacing your mobile device



## Existing Staff



If you have not used your Authenticator for some time, you should test it by **disabling your Wi-Fi**, and opening an app like Teams or Outlook connected to your work account.



**Note:** Disabling your Wi-Fi for the test is only required while connected to MGH Wi-Fi.



### Need help?

If you run into any issues, please contact the IT Help Desk.



416-469-6580 Ext. 2000



helpdesk@tehn.ca



iCare > All Staff > IT Resources



Authenticator  
setup using  
your phone  
and a  
computer.

# Download Authenticator (and Intune\*)



iOS / Apple  
App Store



\*Only  
Android  
requires  
Intune



Android/ Google  
Play Store

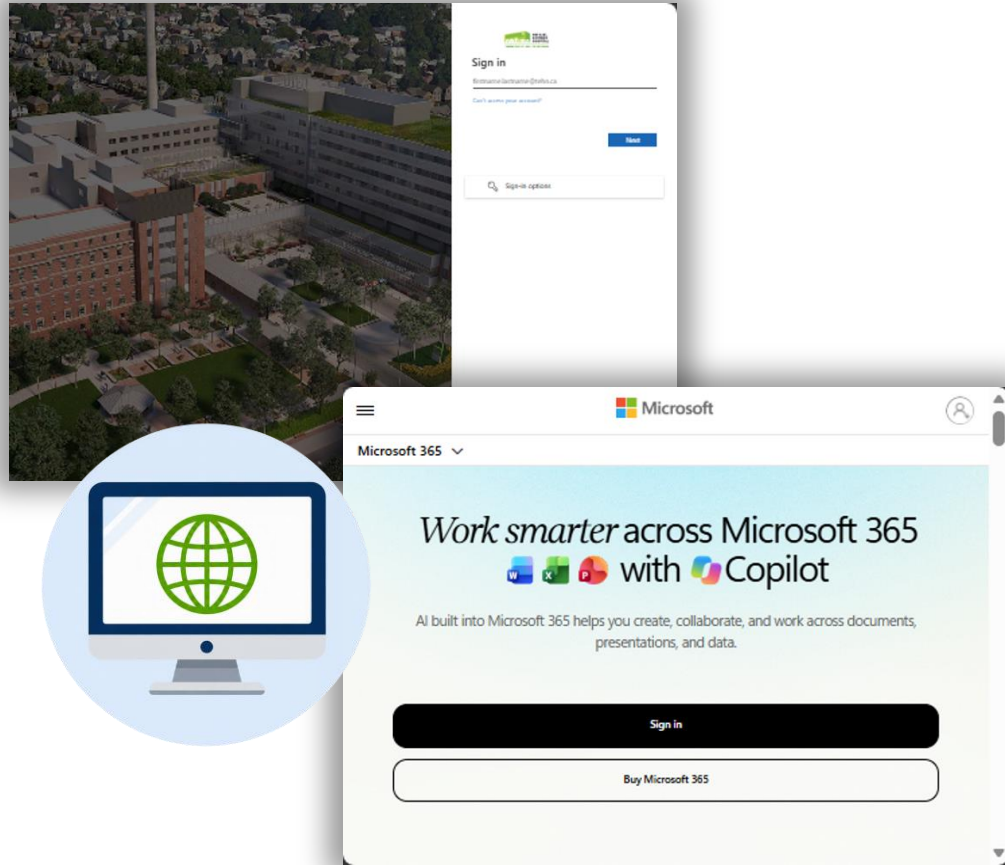


**DO NOT  
sign into  
Intune**



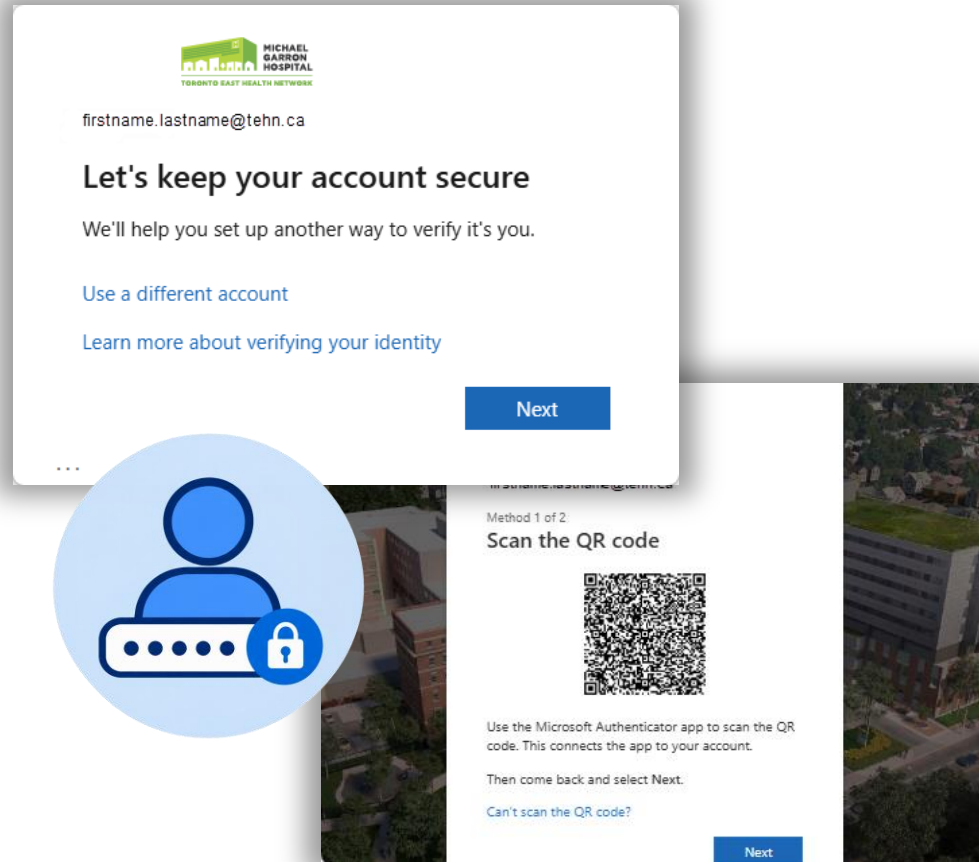
\*Only  
Android  
requires  
Intune

# 1. Setup using a computer web browser.



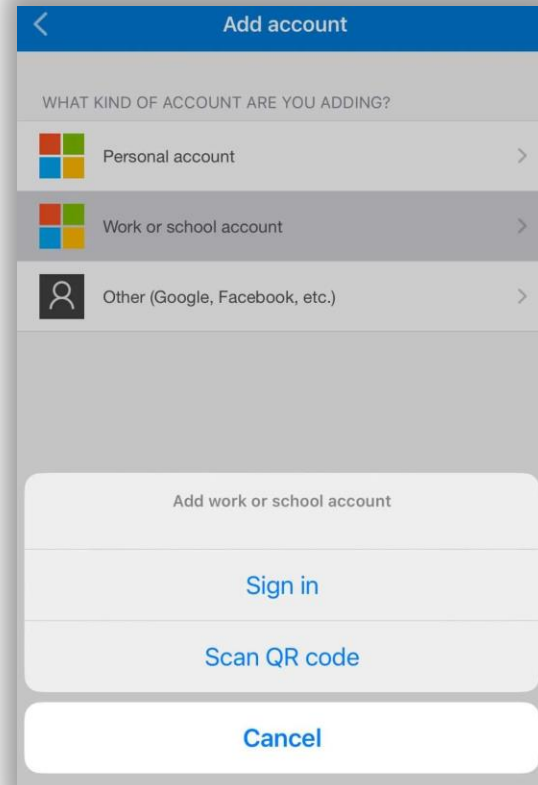
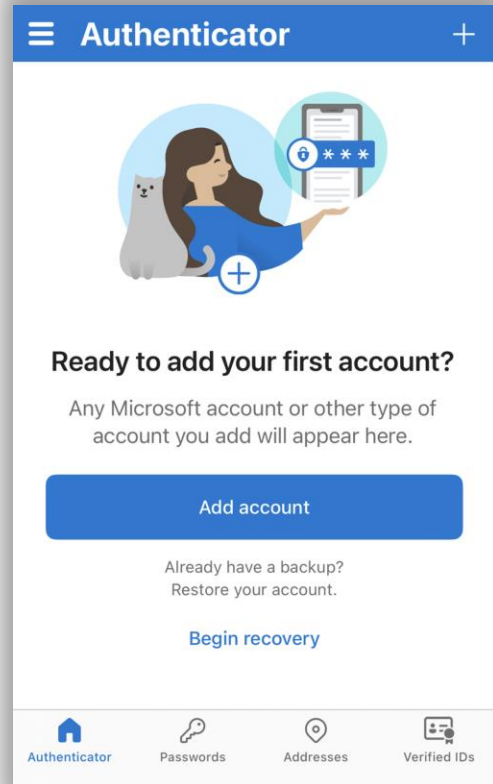
- Visit [www.icare.then.ca](http://www.icare.then.ca) or [www.office.com](http://www.office.com) using a computer browser.
- Once you visit either of these sites and begin the login process, you will be asked for your **email** and **password**.
- **firstname.lastname@tehn.ca** is the proper email format.

## 2. Log in with your work credentials



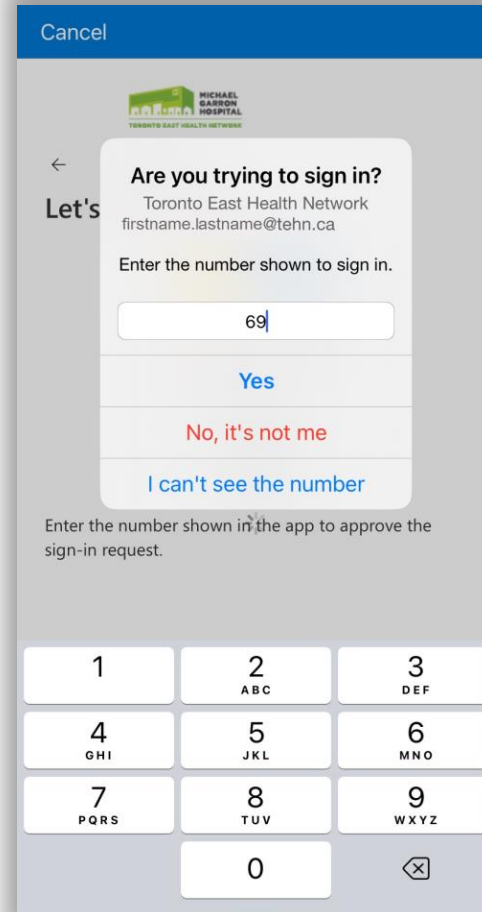
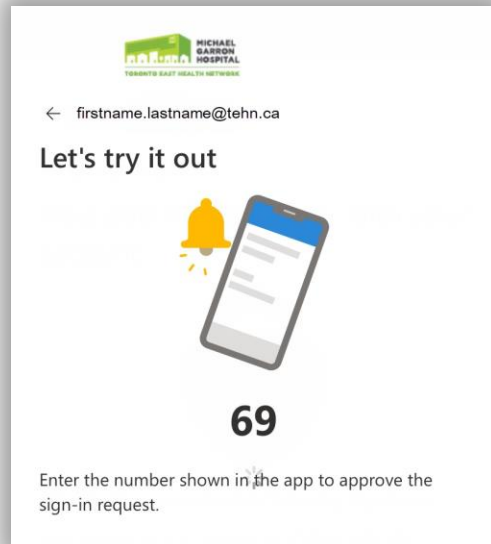
- Starting on the “Let’s keep your account secure” popup, click **Next** until a QR code appears.
- Open the Microsoft Authenticator app on your mobile device.

# 3. Open Microsoft Authenticator



- **\*\*IMPORTANT NOTE\*\***  
Notifications must be enabled for Authenticator to work, so if asked to enable Notifications, choose “**Yes**”/ “**Enable**”.
- On the front page, select the **+** icon on the top right.
- On the next screen tap **Work or school account** and then **Scan QR Code**, then center the phone camera on the barcode on screen.

## 4. Confirm the Authenticator App



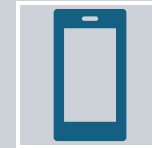
- The barcode will change to a popup requiring confirmation, **Click Next** to continue.
- The next screen will provide a 2-digit number, make note of this number.
- Your phone should alert you, requesting you to approve the sign-in. You would then **enter the 2 digits** into the app, then **Tap Yes**.

# Your Authenticator setup is complete.

- You can now test your applications that require MFA.
- **Phone only** directions begin on the **next page**.

## Notes:

- Connecting to MGH or Microsoft sites while connected to the MGH internet will NOT prompt you for Authenticator unless accessing sensitive profile sections like the security settings on your account page.



A **test** can be done by **disabling Wi-Fi** on your mobile device and connecting to an app like Teams or Outlook.



You will be asked to **create a pin** when opening those apps which will be required once daily.

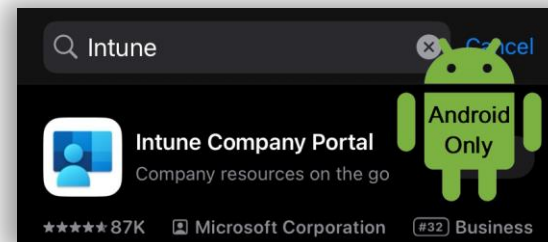
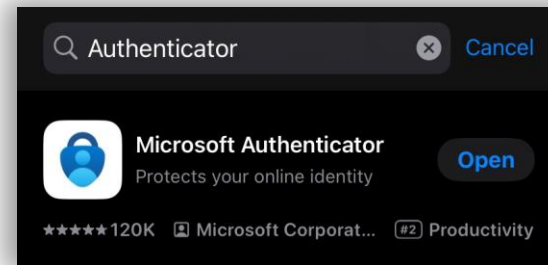


The apps may also close on their own during the initial setup to configure app security.



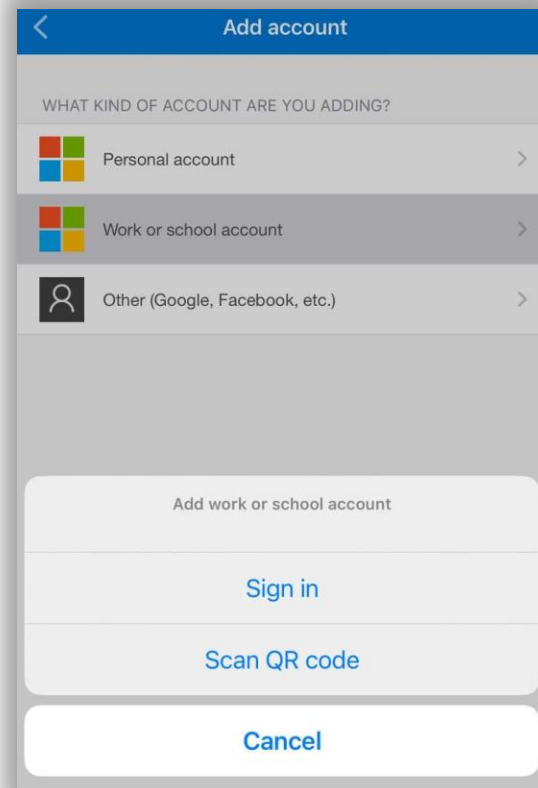
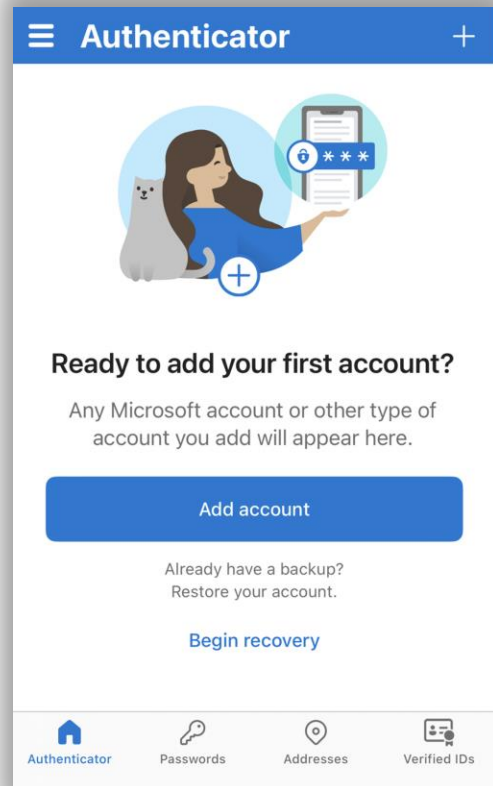
Authenticator  
Setup using  
**only** your  
phone.

# Download Authenticator (and Intune\*)



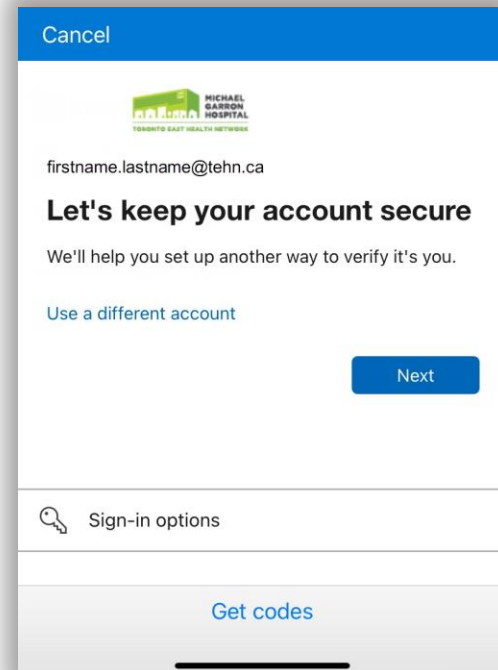
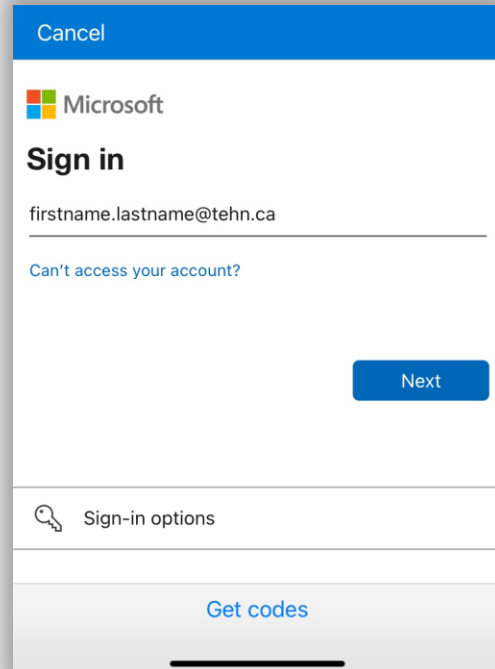
- Be aware if searching manually for these apps, that you are downloading official Microsoft applications.
- Apple / iOS only requires Authenticator.
- Android / Google requires Authenticator and Intune.
- **\*DO NOT SIGN INTO INTUNE**

# 1. Open Microsoft Authenticator



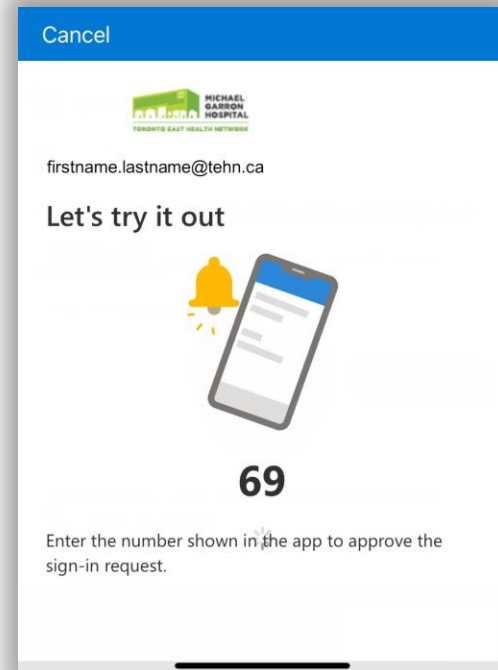
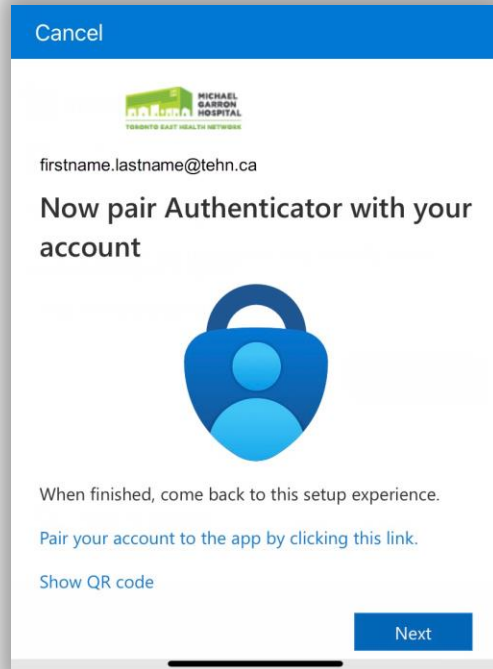
- **\*\*IMPORTANT NOTE\*\***  
Notifications must be enabled for Authenticator to work, so if asked to enable Notifications, choose **“Yes”/ “Enable”**.
- On the front page, select the **+** icon on the top right.
- On the next screen tap **Work or school account** and then **Sign In**.

## 2. Sign in with your work login.



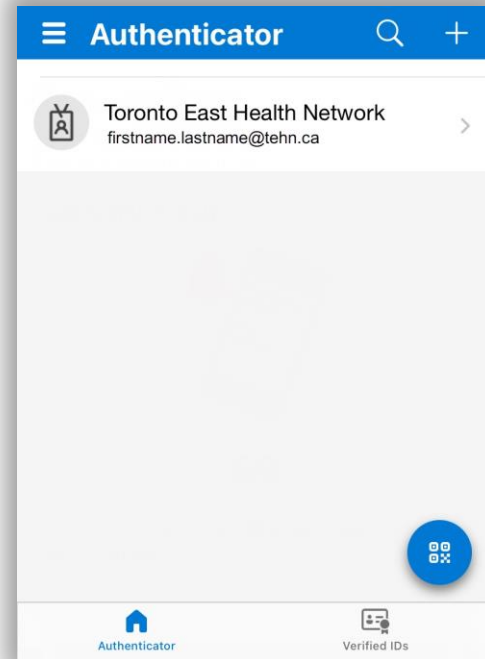
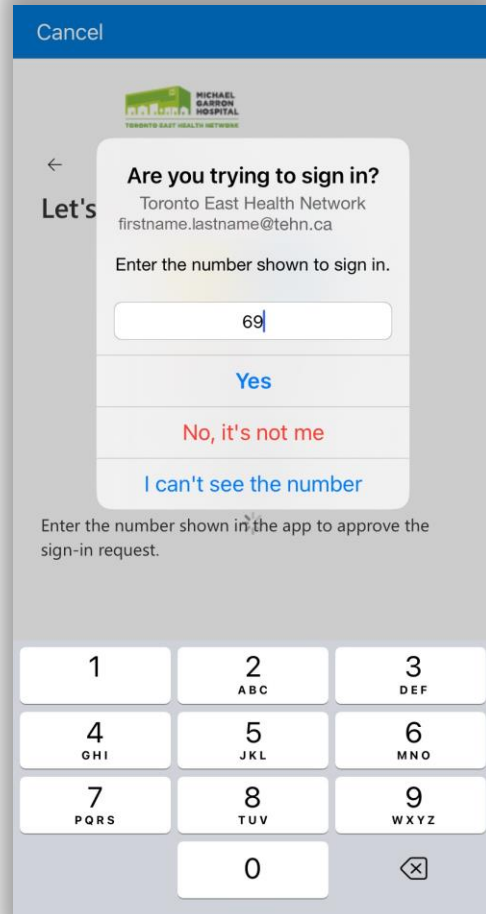
- Sign in to Authenticator using your work email and password.
- **firstname.lastname@tehn.ca** is the proper email format.
- **Click Next** on the page with an MGH Icon at the top saying **Let's keep your account secure.**

### 3. Pair your Authenticator



- On the **Now pair Authenticator with your account** screen, tap **Pair your account to the app** by clicking this link.
- Authenticator will then provide a number to enter, then automatically bring up the screen to enter the number.

## 4. Confirm the Authenticator App



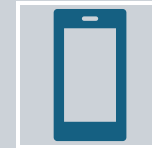
- The next screen will provide a 2-digit number, make note of this number.
- If you missed the number, tap **I can't see the number** and once you have it, tap **Enter Number** on the top right.
- **Enter the 2 digits** into the app, then **Tap Yes**.

# Your Authenticator setup is complete.

- You can now test your applications that require MFA.

## Notes:

- Connecting to MGH or Microsoft sites while connected to the MGH internet will NOT prompt you for Authenticator unless accessing sensitive profile sections like the security settings on your account page.



A **test** can be done by **disabling Wi-Fi** on your mobile device and connecting to an app like Teams or Outlook.



You will be asked to **create a pin** when opening those apps which will be required once daily.



The apps may also close on their own during the initial setup to configure app security.