

August 2022



Epworth Healthcare

Multi-Factor Authentication Setup

Introduction

Epworth systems contain sensitive employee and patient data. Epworth has a responsibility to ensure this data is protected.

One of the ways we can do this is by requiring the use of Multi-Factor Authentication (MFA), before access is granted to Epworth applications and data when a user is outside of the Epworth network. This ensures that the user is who they say they are (and not a hacker who has stolen a username/password).


Currently this is done through an older system. With Epworth's migration to cloud, the MFA system is also moving, which will:

- Installation of an app on your phone
- Set-up of your Microsoft cloud account
- Provide a new experience when remotely accessing Epworth applications

This guide steps through the process to enrol in Epworth's new MFA system to protect your @epworth.org.au account, this should only take **5 minutes** to complete.

Pre-requisites

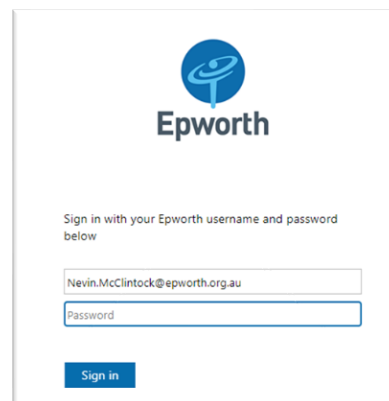
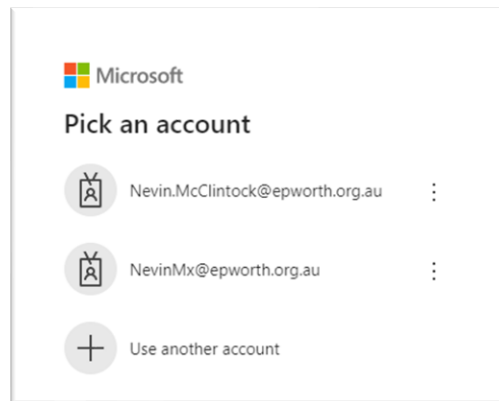
These instructions require you to:

- **Be connected** to the Epworth network either by:
 - Being physically within the Epworth environment
 - Connected via VPN from an Epworth laptop (look for this icon in system tray )
 - Or connected via a Citrix session
- Have an individual iOS / Android phone or tablet (i.e. not shared). Access to your @Epworth.org.au account. Do not follow these instructions on your phone/tablet.

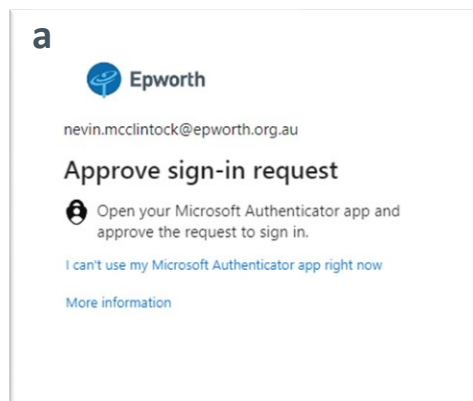
If you cannot meet these requirements, please contact the MFA project team at MFAProject@Epworth.org.au for assistance.

Follow the steps on the next pages to complete your registration:

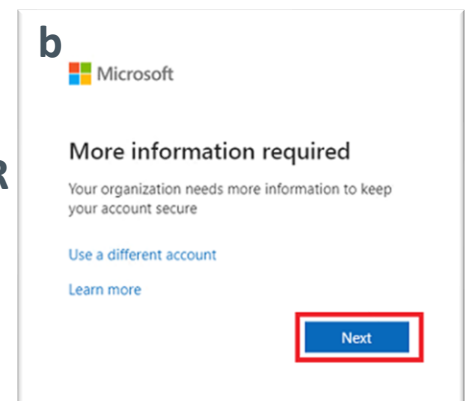
1. **From your Epworth laptop or session** visit the following webpage - <https://aka.ms/mfasetup>
- If you are asked to 'pick an account', select your normal user account (first.last@epworth.org.au), enter your password if required
 - If you are asked to sign in with your Epworth username and password, enter your normal user account details (first.last@epworth.org.au)



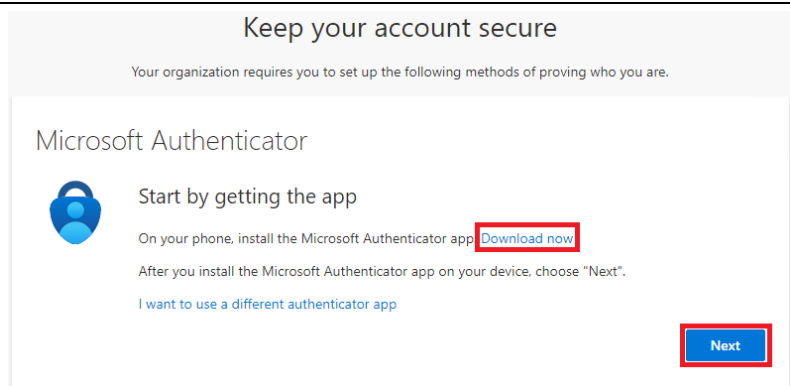
2. a. If you receive this message and get a push notification to your phone, then you are registered and don't need to go any further
- b. If you receive this message, then click **Next** to continue to register your app and account for MFA



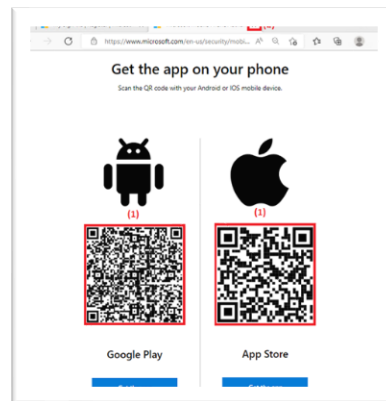
OR



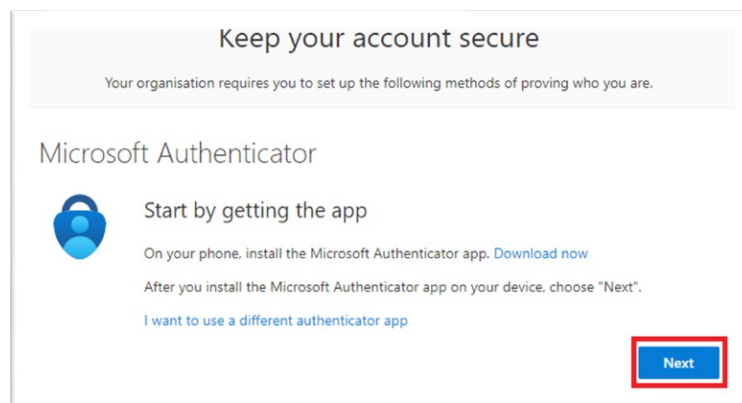
3. The next page indicates that the Microsoft Authenticator is required for enrolment
- If you don't have it installed:
 - Press **Download now** for links to your app store to download the app if required (Step 4)
 - Go to your phone's App Store and search for Microsoft Authenticator and Install
 - If you already have the authenticator press **Next** to continue and go to step 5



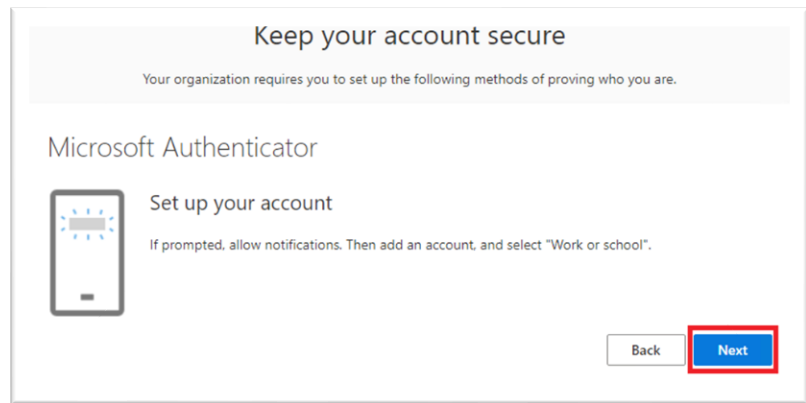
4. Scan the appropriate QR code with your phone (you may need to scroll down)
- This will take you to your mobile phone's app store to download the application
 - Download the appropriate application
 - Close the tab with the QR Codes



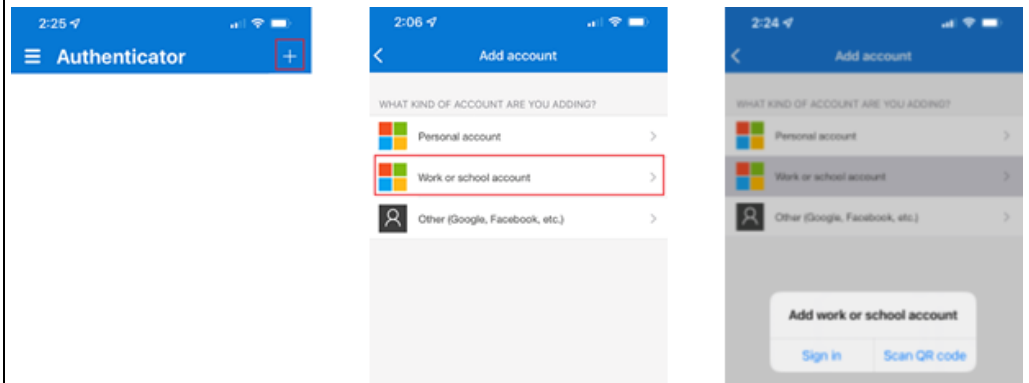
5. Select **Next**



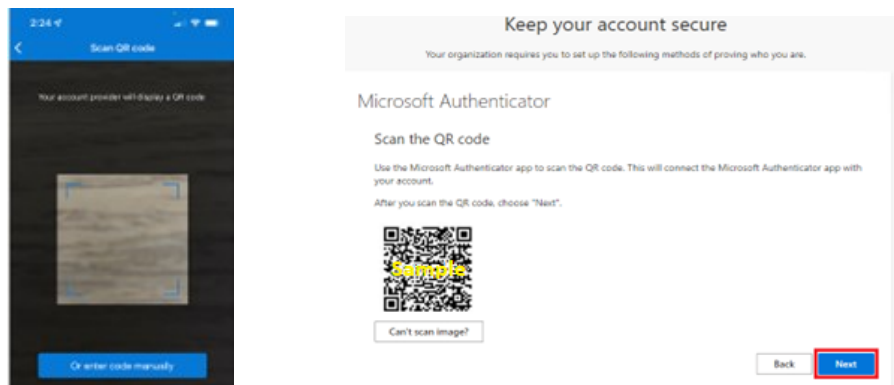
6. Instructions are then provided to setup the authenticator
- Open the Microsoft Authenticator app on your phone
 - Press **Next** in the web browser to continue

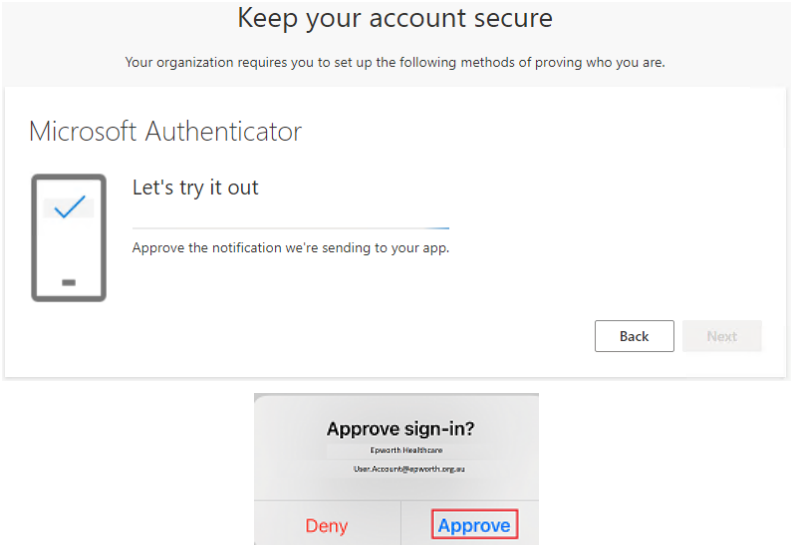
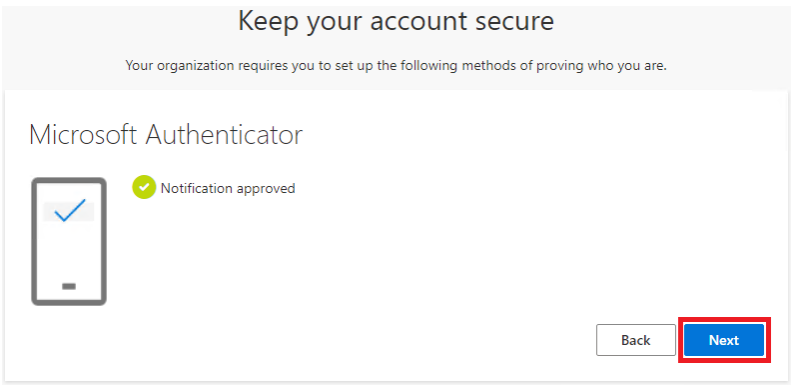
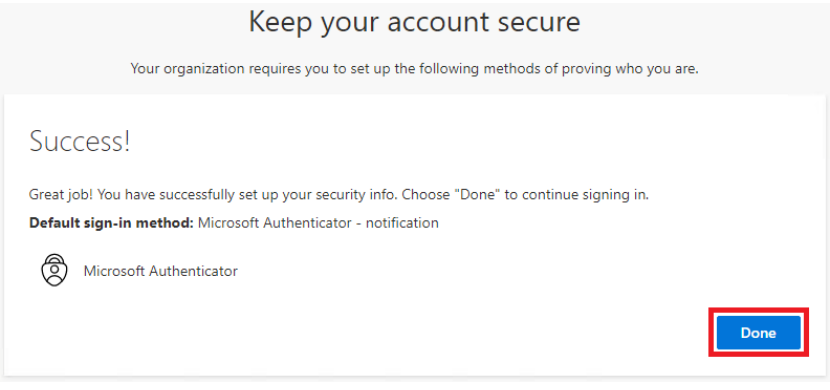


7. From the mobile application, accept any prompts to display notifications and press
- the **+** (**plus**) **sign** on iOS or the 3 dots on Android
 - Select Add Account
 - Tap **Work or School** on your mobile
 - select **Scan QR code**



8. A QR code is generated, your mobile should automatically have changed to the camera view at step 7
- If prompted allow Microsoft Authenticator to access the camera
 - Scan the QR code presented on your web browser
 - After scanning the QR code with the Microsoft Authenticator the mobile application will update its settings and return to its home screen
 - Press the **Next** button on the web browser to continue



<p>9. The web page advises that a push notification is sent to your device to confirm enrolment</p> <ul style="list-style-type: none"> On your device open the notification <i>This will launch the Microsoft Authenticator</i> Press Approve on your mobile to confirm the link between your device and the authentication method 	
<p>10. Confirmation will be provided in the web browser</p> <ul style="list-style-type: none"> Press Next to finalise the configuration 	
<p>11. A summary will be presented to confirm that you have finished the enrolment</p> <ul style="list-style-type: none"> Press Done and close the web browser 	
<p>12. You are now enrolled with Multi-Factor Authentication to protect your @epworth.org.au account</p> <ul style="list-style-type: none"> In the future if you access Epworth services from outside of the Epworth network/VPN, you will need to Approve your sign-in on your mobile device 	