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:

- Require the installation of an app on your phone
- Set-up 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

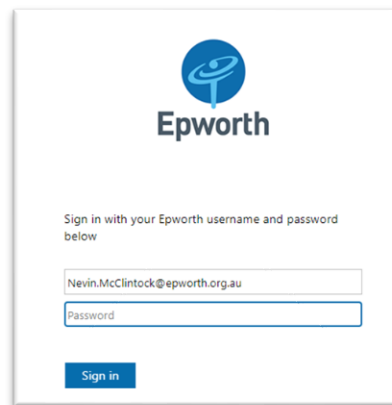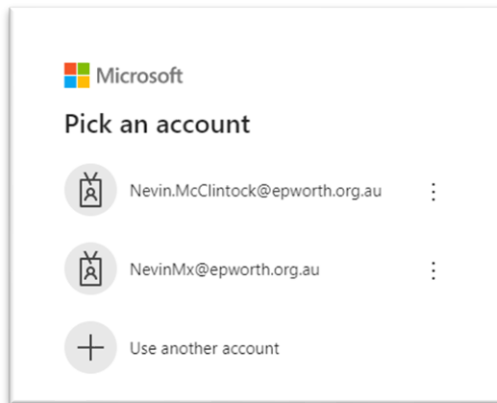These instructions require you to:

- **Be connected** to the Epworth network either by:
    - Being physically within the Epworth environment
    - 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.
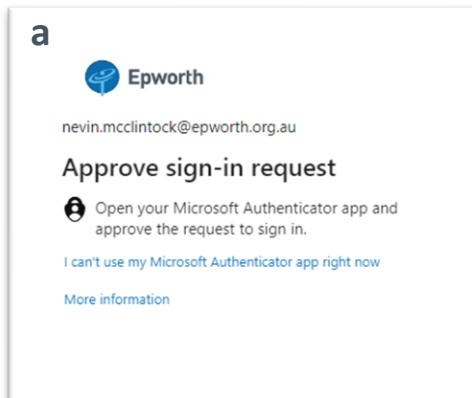
Follow the steps on the next pages to complete your registration:

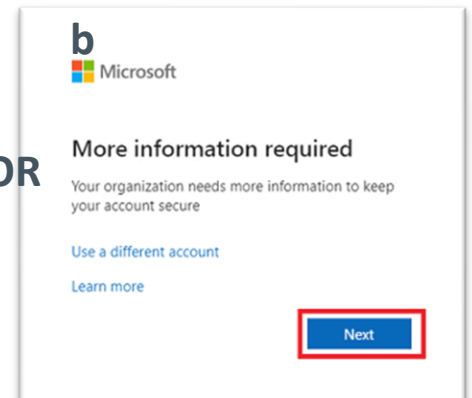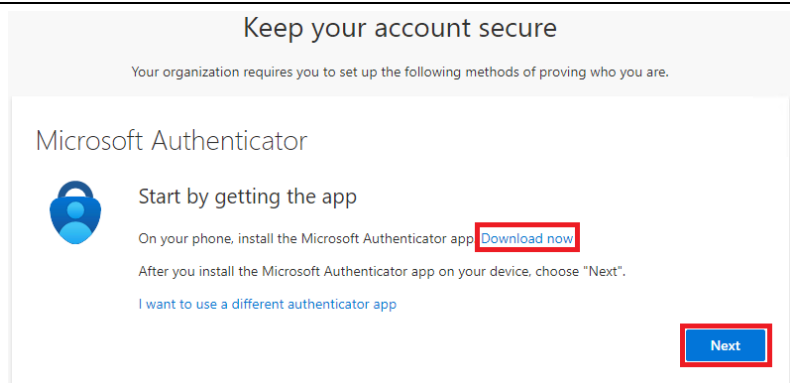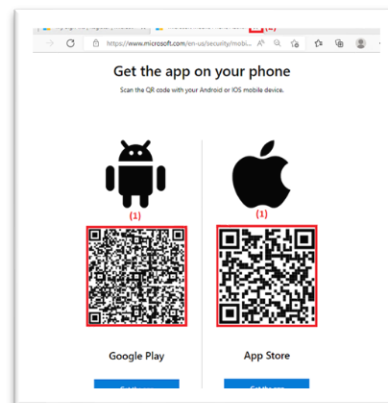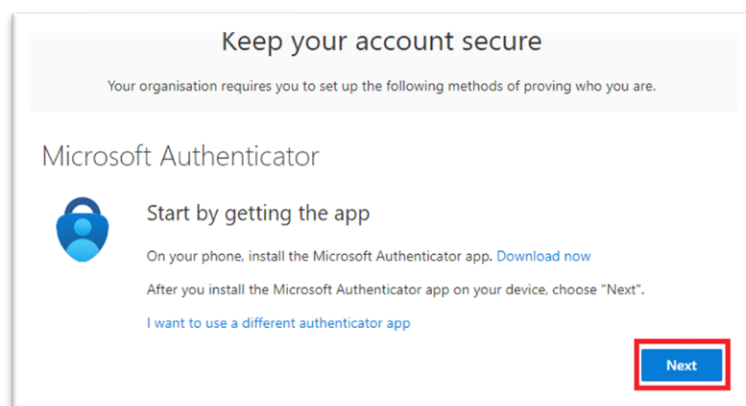|	
1. **From your Epworth laptop or session** visit the following webpage - https://aka.ms/mfasetup • If you are asked to 'pick an account', select your normal user account (first.last@epworth.org.au), enter your password if required • If you are asked to sign in with your Epworth username and password, enter your normal user account details (first.last@epworth.org.au)	![Microsoft Pick an account screen and Epworth sign-in screen] **Microsoft** **Pick an account** Nevin.McClintock@epworth.org.au NevinMx@epworth.org.au + Use another account **Epworth** Sign in with your Epworth username and password below Nevin.McClintock@epworth.org.au Password Sign in
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	**a** **Epworth** nevin.mcclintock@epworth.org.au **Approve sign-in request** 🔒 Open your Microsoft Authenticator app and approve the request to sign in. I can't use my Microsoft Authenticator app right now More information **OR** **b** **Microsoft** **More information required** Your organization needs more information to keep your account secure Use a different account Learn more Next

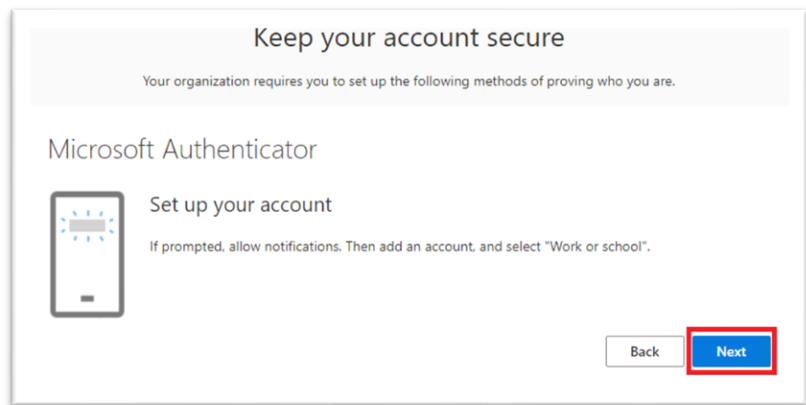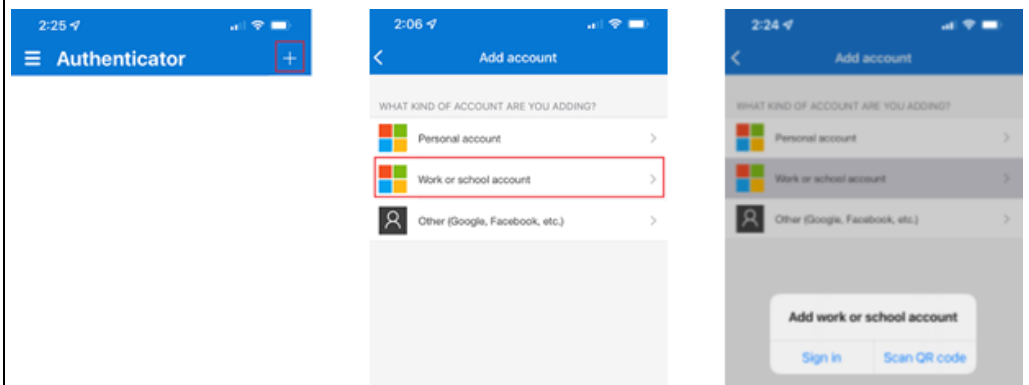|	

3. The next page indicates that the Microsoft Authenticator is required for enrolment
 	
• If you don't have it installed:
 	
    o Press ***Download now*** for links to your app store to download the app if required (Step 4)
 	
    o 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
	Keep your account secure
	Your organization requires you to set up the following methods of proving who you are.
	
	Microsoft Authenticator
	
	Start by getting the app
	
	On your phone, install the Microsoft Authenticator app. Download now
	
	After you install the Microsoft Authenticator app on your device, choose "Next".
	
	I want to use a different authenticator app
	
	Next

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	**Get the app on your phone** Scan the QR code with your Android or iOS mobile device. Google Play App Store
5. Select ***Next***	**Keep your account secure** Your organisation requires you to set up the following methods of proving who you are. **Microsoft Authenticator** Start by getting the app On your phone, install the Microsoft Authenticator app. Download now After you install the Microsoft Authenticator app on your device, choose "Next". I want to use a different authenticator app **Next**

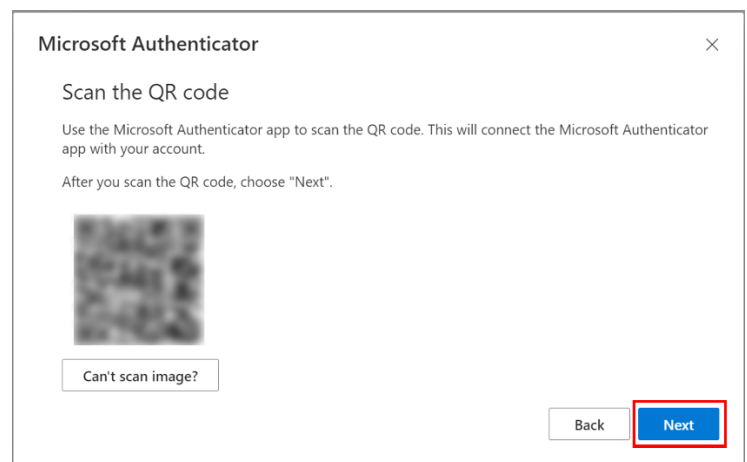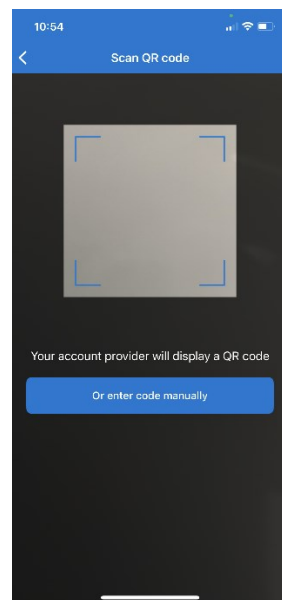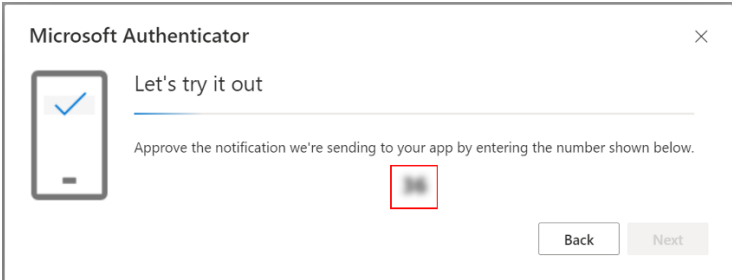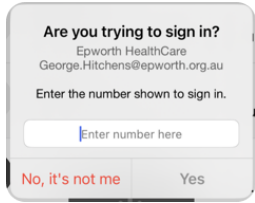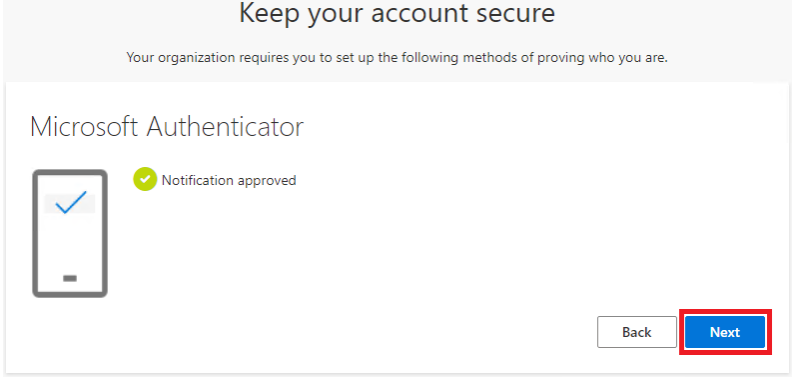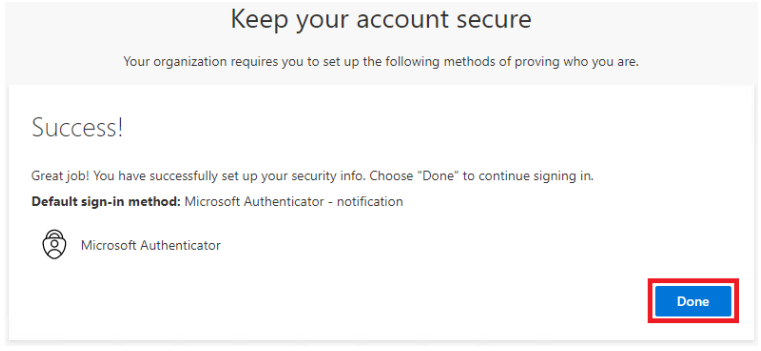|	
6. Instructions are then provided to setup the authenticator • Open the Microsoft Authenticator app on your phone • Press *Next* in the web browser to continue	
7. From the mobile application, accept any prompts to display notifications and press • the *+ (plus) sign* on iOS or the 3 dots on Android • 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	

9. The web page advises that a notification is sent to your device to enter the number pictured on your screen into the app • On your device open the notification *This will launch the Microsoft Authenticator* • Enter the number shown and tap 'yes' to confirm the link between your device and the authentication method	
10. Confirmation will be provided in the web browser • Press **Next** to finalise the configuration	
11. A summary will be presented to confirm that you have finished the enrolment • Press **Done** and close the web browser	
12. You are now enrolled with Multi-Factor Authentication to protect your @epworth.org.au account • In the future when you access Epworth services from outside of the Epworth network, you will need to enter the number shown on screen into your Microsoft Authenticator app	