Student MFA Quick Setup

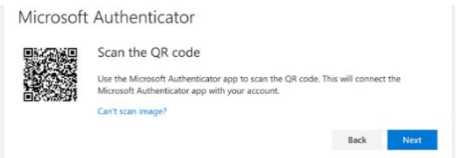
Multi-factor Authentication (**MFA**) is now a **Mandatory** service for Students to help secure your Identity and data on your devices and in the cloud whilst studying at UWA. In addition, UWA also offers a Self-Service Password Reset (SSPR) facility that uses MFA to verify who you are to reset your password or unlock your account if required, anytime, from any browser. This guide shows you how to setup MFA so you can protect your account as well as for use with SSPR in the future.

Prerequisites

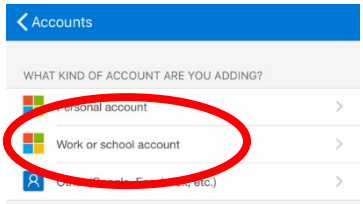
- Ensure you are using Office 365 Pro Plus (or minimum Office 2016) on your PC or Mac to work with MFA. Office 365 Pro Plus is offered to Students at No Cost whilst studying at UWA. Visit https://portal.office.com using your Uni-ID (studentnumber@student.uwa.edu.au) to Install a copy.
- For a consistent experience, Uni IT also recommend using Outlook and the other Office Apps such as OneDrive and Microsoft Teams on your mobile devices. If you wish to continue to use Apple or Android mail products, you may need to upgrade to the latest iOS or Android OS versions for their Apps that support MFA. Older versions do not understand MFA processes.
- It is recommended you pre-install the **Microsoft Authenticator** App on your Mobile for the best experience. Ensure you "**Allow Notifications**" when prompted on first install of the app.

Setup MFA with Authenticator App

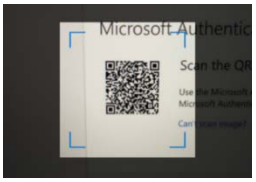
1. Go to **https://aka.ms/mfasetup** using a browser **on your PC/Laptop or Mac** and log in with your **Uni-ID** (e.g. studentnumber@student.uwa.edu.au) credentials when the Sign-In screen appears using your current Pheme password. With **More information required** or to **Stay signed in.** Click **Next.**
2. **If prompted,** select **Security Info.** then **Add method,** then Select **Authenticator app**
3. As you already have **Microsoft Authenticator** installed on your smartphone, click **Next**
4. As we have already allowed **Notifications**, click **Next**
5. You will be presented with a **QR code**. Leave this page open.



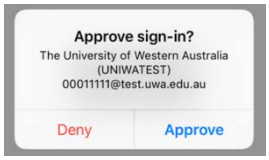
6. Moving back to your **smartphone**, open the **Microsoft Authenticator App**, and click **Add account**. Then, **Select Work or school account**



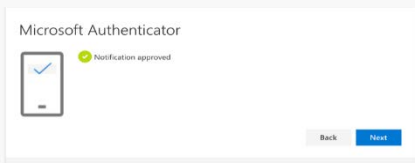
7. Your Phone's Camera will open. Select **Allow** the Use the camera to view the **QR Code.** The **Microsoft Authenticator** application will recognise the **QR Code**



8. Back on your computer **Browser** **Click** **Next**.



9. On your **Microsoft Authenticator** app **Notification**; click **Approve.**
10. On your **Browser** you will see a Notification approved message; **Click** **Next** and you should see a **Success** note. Click **Next**.

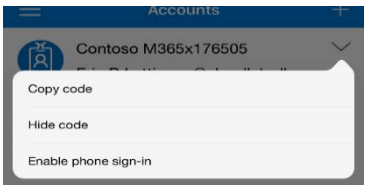


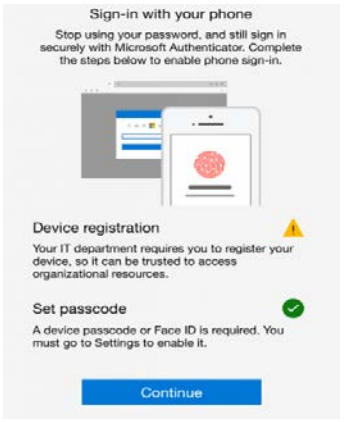
If you get a failed setup or it hangs for more than a couple of minutes at any stage during this process, you can delete and go back to step 1 to try again. If unsure, contact the Library for support. Continue on otherwise.

Student MFA Quick Setup

11. To **improve your MFA experience**, we highly recommend that you now register your device with UWA. On the main Authenticator screen, press on the down chevron or 3-dot symbol, and choose **Enable phone sign-in**. When you see the 2nd screen below, press **Continue**. This will register your device with UWA and the Device registration yellow warning triangle should turn to a green tick thereafter.

This step can take a couple of minutes but if longer, cancel and try again.





Set up Phone SMS as another method.

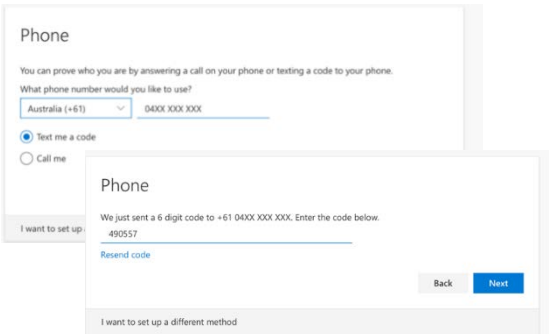
Your Authenticator App should be set as the Default. We recommend that you set up **your Mobile Phone Number** as a backup method should the Notification and "Approve" not work.

12. On the main Security Info page, choose **Add method,** then from the drop-down list, Select **Phone**

13. Enter your mobile details – **Area code** and **mobile number.** Select **Text me a code** and click **Next.**

14. A 6-digit code will be sent to your smartphone via text. Enter the **6-digit code** and click **Next**

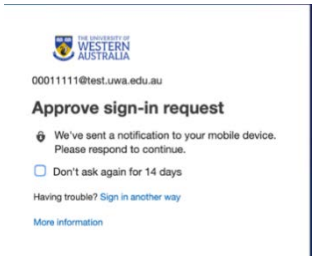
15. Your 6-digit code will be verified, once complete click **Next** and you should see a Success screen**.**



Using MFA

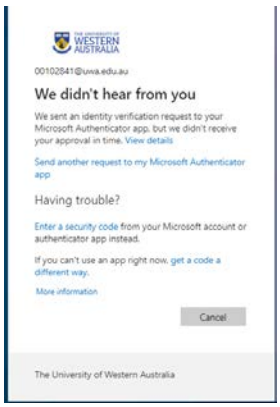
MFA challenges will be prompted for any Application or Website access deemed required by UWA and when deemed necessary. Every separate device will require MFA validation.

You may see initially a Sign-In screen or if you are on your own device, a Password screen with UWA branding. Once your password is cached, this screen may stop appearing on your own device and will move straight to the next Approve screen.



With this **Approve sign-in request screen** up, click on the "Don't ask again for 14 days" checkbox **before** accepting the MFA challenge request on your Phone.

On your phone, you will then experience the Approve request pop-up if defaulting to the App or receive a SMS if it is your default MFA method.



If the MFA fails for any reason, you will be prompted to retry, or try one of the alternative methods you should have setup. This may appear as a link to "Sign in another way" or "get a code a different way".

Please contact the **Library** for any issues. You can return to **https://aka.ms/mfasetup** anytime to change your settings. **If you lose or change your Phone**, you will need to contact the **Library** to have your **MFA Reset.**