

# Multi-Factor Authentication (MFA) with Microsoft Authenticator - install, setup, and phone change

---

This article is to provide users with instructions for setting up **Microsoft Authenticator** as the preferred and the alternate MFA method and help on what to do if you change your phone.

There are four processes:

[Process 1: Install Microsoft Authenticator App on your mobile device](#)

[Process 2: Set up MFA for your devices](#)

[Process 3: Set up MS Authenticator as the alternative MFA method](#)

[Process 4: Set up MS Authenticator when you change the mobile device](#)

You should set up an alternative MFA method such as SMS One-Time Passcode in case you change your mobile device. This will ensure continued access to your UOW account.

## **Process 1: Install Microsoft Authenticator App on your mobile device**

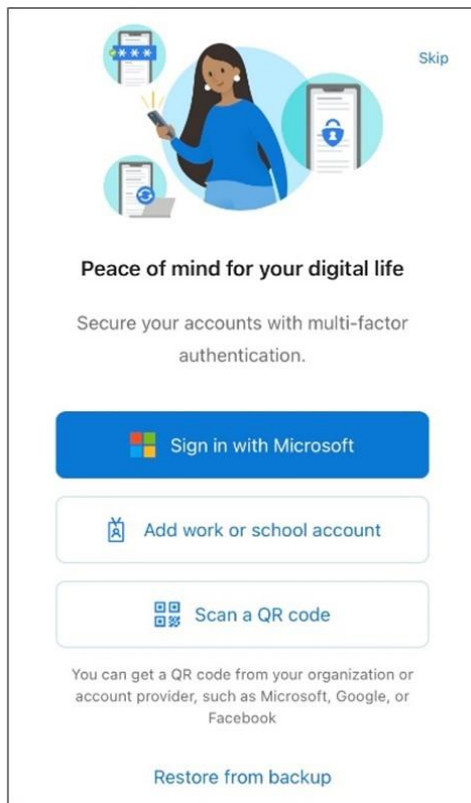
**A prerequisite for this set up is to download and install the Microsoft Authenticator App to your personal device.**

If the MS Authenticator App is already installed go to Process 2 - Set up MFA in your Security Info.

1. Download the MS Authenticator App, use the following links:

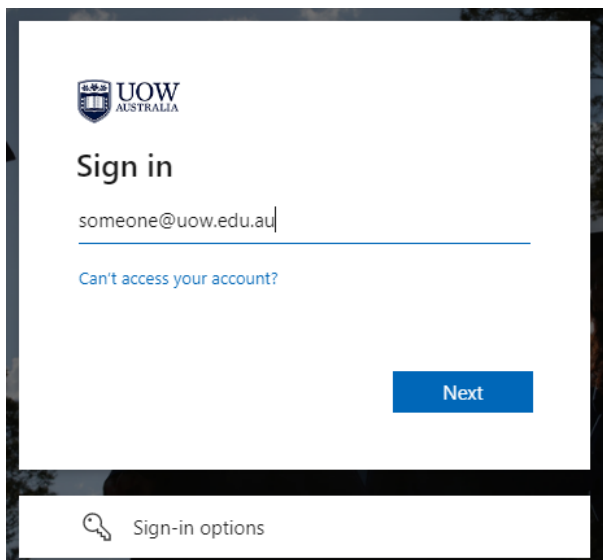
- Google Android. On your Android device, go to Google Play Store to [download and install the Microsoft Authenticator app](#).
- Apple iOS. On your Apple iOS device, go to the App Store to [download and install the Microsoft Authenticator app](#).
- If you don't have access to one of these smartphone stores user your manufacturer provided store.
- For Chinese students, you can [download MS Authenticator app](#) and scan the QR code shown to install the Lenovo app store on your smartphone. Tap Allow to give permission for the app to install and then tap Continue to proceed. Once the Lenovo app store is installed, search for the free Microsoft Authenticator app and download it onto your phone.

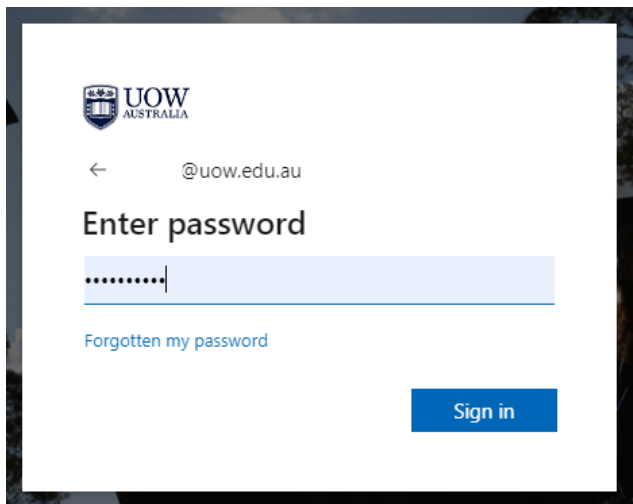
**NOTE: This is a free application and payment is not required.**



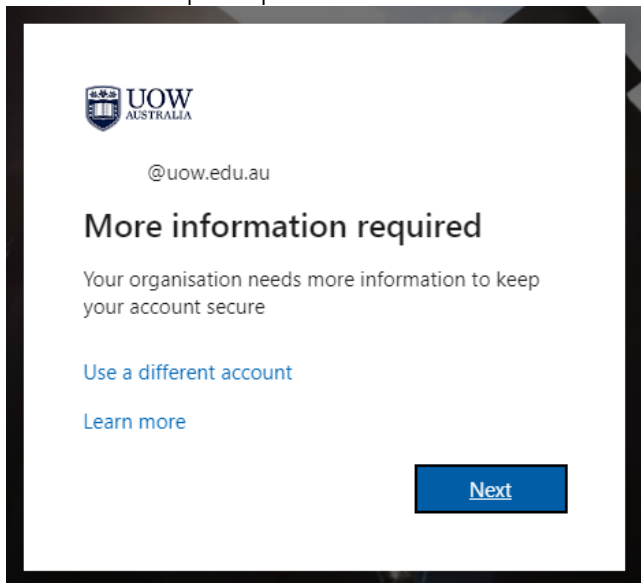
## Process 2: Set up MFA for your devices

1. **On your PC/ Laptop:** When prompted to set up MFA, you will be asked to enter UOW username and password and click '**Sign in**'.

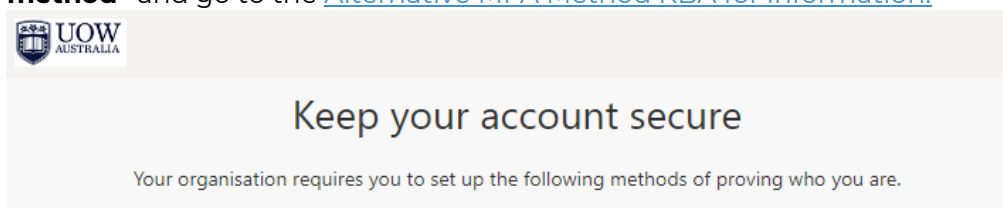




2. You will be prompted for more information. Click **'Next'**



3. When you receive the following dialogue box, click **'Next'** to set up the MS Authenticator app. If you would like to set up SMS or call back phone as your preferred MFA method, click on **"I want to set up a different method"** and go to the [Alternative MFA Method KBA for information.](#)



## 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

[I want to set up a different method](#)

4. Click 'Next' to set up your account and receive your QR Code.

✕  
 ?  

## Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

### Microsoft Authenticator

**Set up your account**

If prompted, allow notifications. Then add an account, and select "Work or school".

Back Next

[I want to set up a different method](#)

## Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

### Microsoft Authenticator

#### Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".



Can't scan image?

Back

Next

[I want to set up a different method](#)

5. **On your mobile device**, return to the MS Authenticator app and select '**Scan a QR Code**'. The app will use your mobile camera to scan the QR code provided on your PC/Laptop in step 4. Follow the prompts until this set up is complete.



Skip

## Peace of mind for your digital life

Secure your accounts with multi-factor authentication.



Sign in with Microsoft



Add work or school account



Scan a QR code

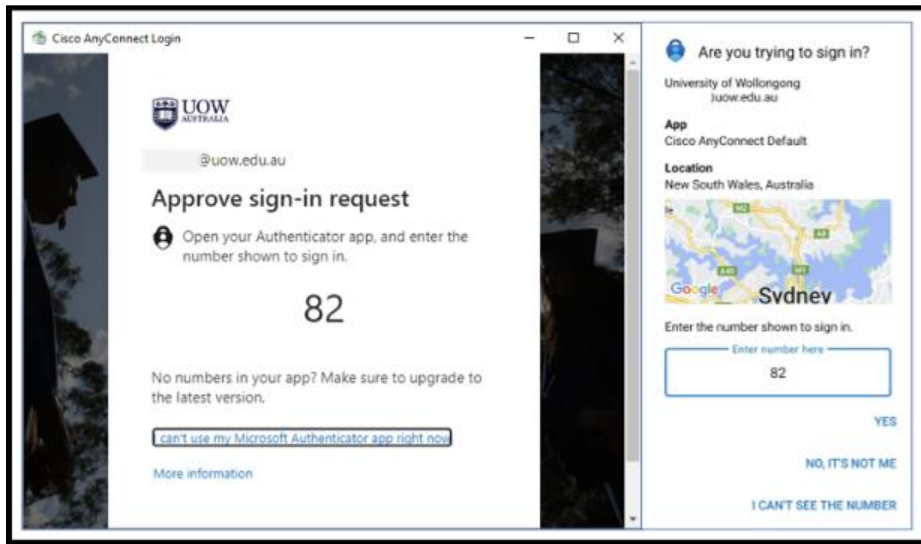
You can get a QR code from your organization or account provider, such as Microsoft, Google, or Facebook

Restore from backup

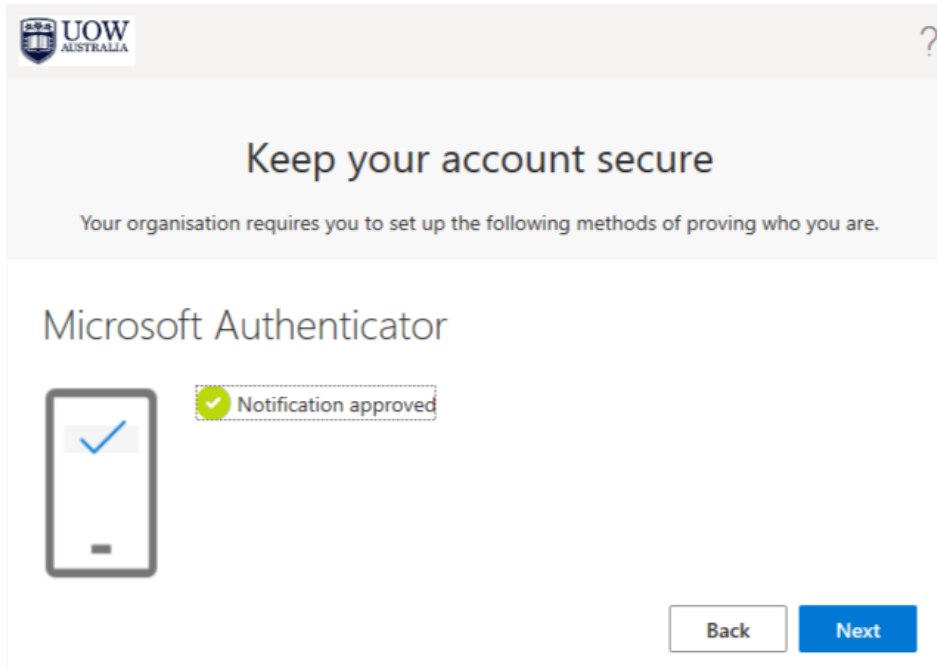
6. **On your PC/Laptop**, click **'Next'** in the dialogue box with the QR code. A notification will be sent to your mobile device. Open the notification.

7. You will now receive a code to 'Approve your sign in request' via the Microsoft Authenticator app. Enter your code on your mobile phone. Click **'Yes'**. You may also need to verify your identity using your phone Pin or biometrics.

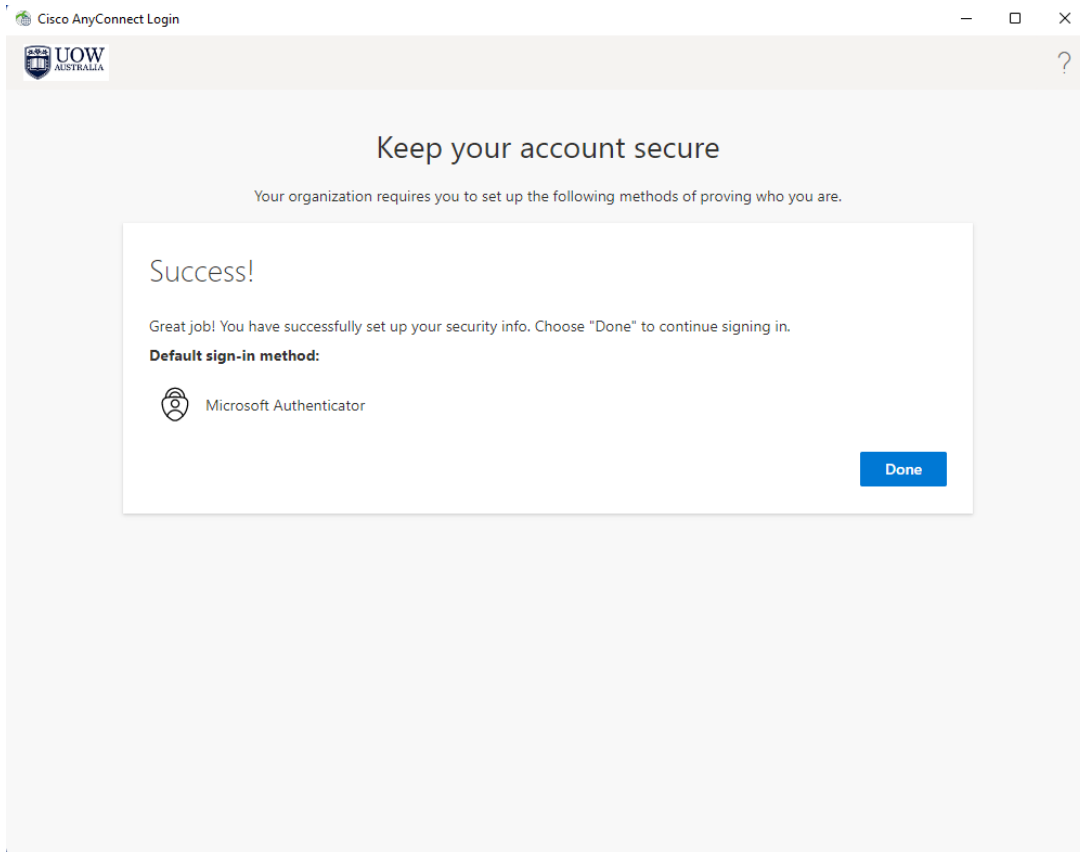
**Note:** Should you ever receive an authentication request that was not initiated by yourself, click **'No, it's not me'** instead of 'Yes'.



8. Once approved, you will receive the following dialogue box on your PC/laptop. Click **'Next'**.



9. When you receive the success notification, click **'Done'**.



**The set up is now complete.**

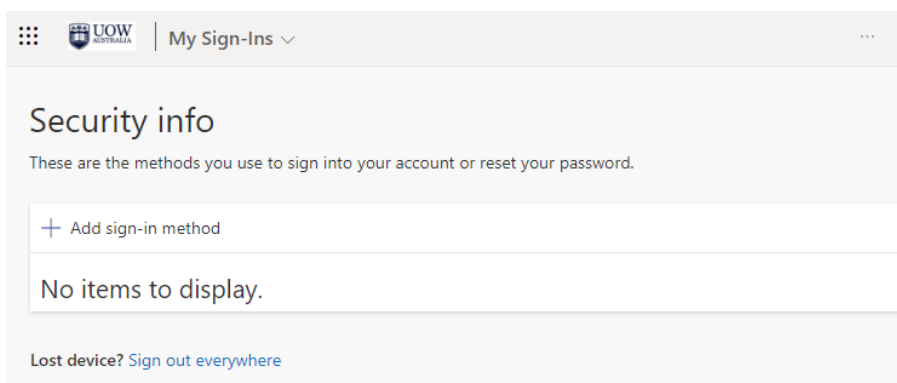
To review/manage your MFA settings or add alternative methods, go to [www.aka.ms/mfasetup](http://www.aka.ms/mfasetup)

### **Process 3: Set up MS Authenticator as the alternative MFA method**

1. Go to your Microsoft Account Security Info [www.aka.ms/mfasetup](http://www.aka.ms/mfasetup)
2. Enter the UOW username and password when prompted.

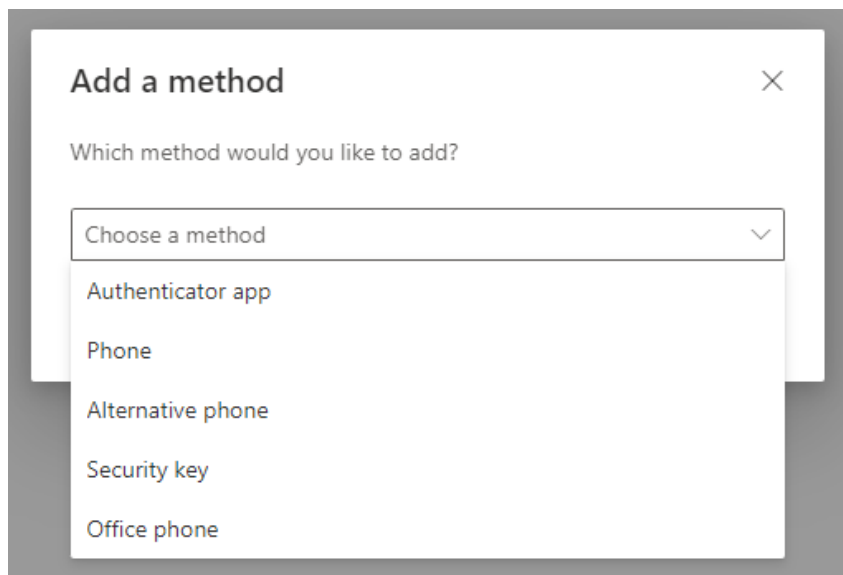
**Note:** If you have changed your phone since your last authentication, you will no longer be able to log in with Microsoft Authenticator. Please contact the Service Desk for further a Temporary Access Pass.

3. You will be directed to the **Security info** page. Click on **'+Add sign-in method'**.



4. The **'Add a Method'** drop-down selection box will appear. Select your alternative method (e.g., **'Phone'** for SMS or **'Alternative phone'** for a callback) from the dropdown and click **'Add'**.





5. Go to **step 3 in Process 2** to continue.

### **Process 4: Set up MS Authenticator when you change the mobile device**

When changing the mobile device (phone or tablet), the MS Authenticator app set up in the Security Info will not work on the new phone. There is a three-step process to rectify this.

1. **On your new phone**, download the MS Authenticator App via the links provided in Process 1. Open the MS Authenticator App and click on the '+' symbol on the top to open the 'Add account' section. Select **'Work or school account'**. This opens a dialogue box, click on **'Scan QR code'** or **'sign in'**. For the 'sign in' option click **'use another account'**. This will take you to the normal sign-in screen described in Process 2, Step 1. Add your UOW username and password to create the linkage.

2. Go to your Microsoft Account Security Info at [www.aka.ms/mfasetup](http://www.aka.ms/mfasetup).

Click on **'Sign out everywhere'** to close all current MFA sessions.

Click on **'Delete'** for the current MS Authenticator app. This will remove the old App linkage.

Click on **'+Add sign-in method'**, then select **'Authenticator App'** from the drop-down box as described in Process 3. This will add MS Authenticator again so it can point to your new phone.

**Note:** If you still have access to your old phone, it is best practice to remove the University of Wollongong email account. Open the MS Authenticator app. Click on the **'University of Wollongong email account'** and open the **'Setting'** symbol in the top right corner. Then click on **'Remove account'** and uninstall the app from your old phone.