Use Microsoft Authenticator

Multi-Factor Authentication (MFA)

Updated: 18 January 2023

Multi-Factor Authentication (MFA) is a requirement to access UNSW single sign-on applications. MFA provides an additional layer of security to protect the University and your zID account from unauthorised access.

Use this guide to help you use the Microsoft Authenticator app once installed and set up correctly.

For help with MFA call the **IT Service Centre on 02 9385 1333** or alternatively visit the MFA website to access support guides such as how to use Microsoft Authenticator when you do not have a data/internet connection on your smartphone.

Below there are instructions for signing in from your computer or signing in from your phone.

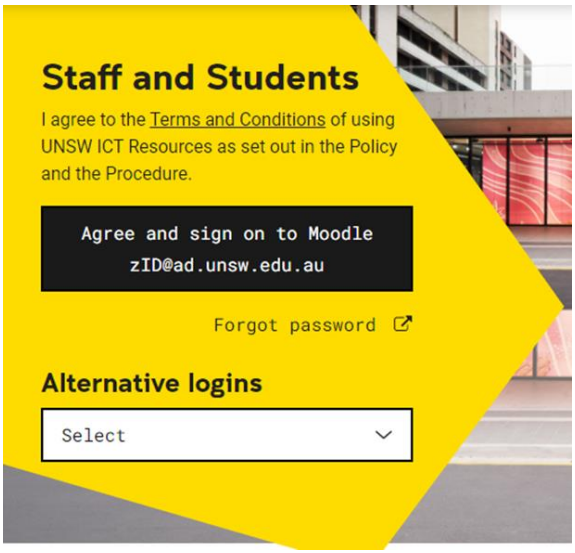
To complete this task, you will need

- To have previously set up MFA using Microsoft Authenticator.

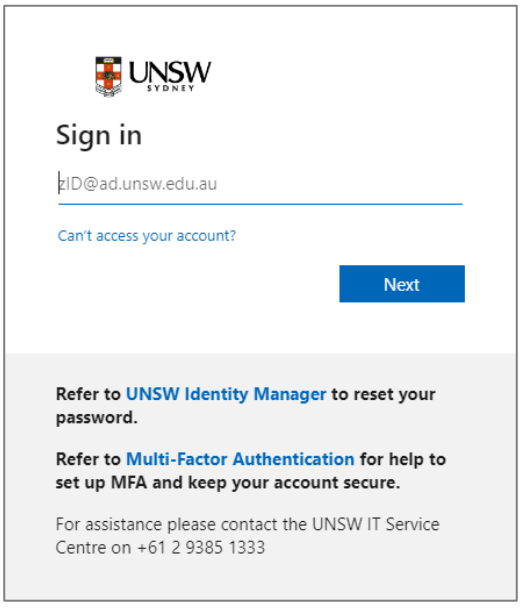
Signing in from your Computer

Follow these instructions to use the Microsoft Authenticator app to verify your sign-in to University single sign-on (SSO) applications when prompted.

1. **On your computer**, access your UNSW single sign-on (SSO) application. If prompted, sign-in using your zID@ad.unsw.edu.au and password and click **Next**.



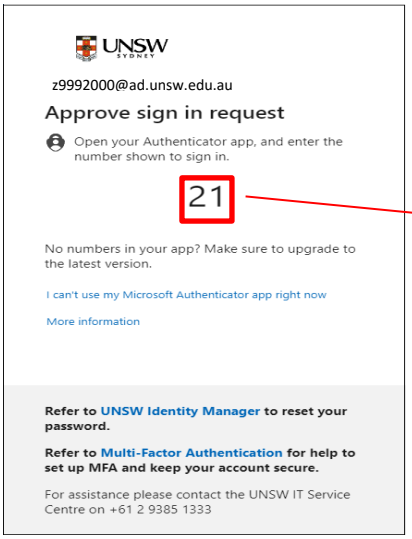
Moodle sign-in screen shown as an example of an SSO application



2.

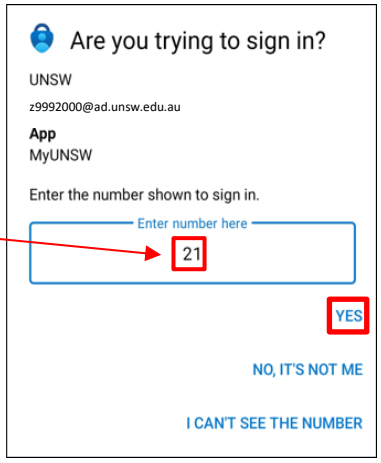
On your computer

When **MFA** is triggered, you will be presented with the *Approve sign-in request* window which includes a 2-digit number. Now a push notification will be sent to your smartphone.



On your smartphone

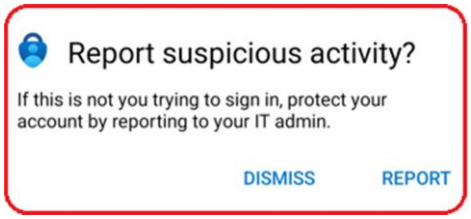
A push notification will ask you to verify your sign-in, enter the 2-digit number from the computer/sign-in screen into your smartphone & click YES.



If the push notification is not immediately visible, open the Microsoft Authenticator app.

Note, the 2-digit number is not your 6-digit one-time password code (OTP).

Security note: *If you receive a push notification on your smartphone but you know it isn't you trying to sign-in, please tap* **NO, IT'S NOT ME** *&* **REPORT** suspicious activity**.** If in doubt report it, this will help UNSW Cyber Operations to determine if there's a risk.



Note: *If the push notification does not immediately come up, even when opening the app, your phone could be without data/internet connectivity. Please follow the guide: Use Microsoft Authenticator without data/internet connection.*

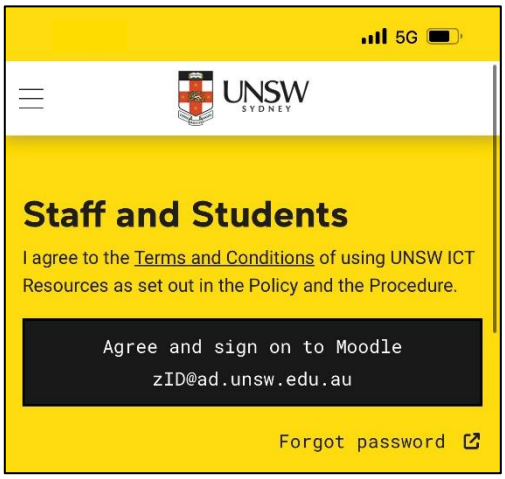
Note*:* If you are presented with a **More information required** *window. It is an indicator that you have not set up MFA. At this Point you must set up MFA before you can access the SSO Application.*

Congratulations, you have just verified your log in, and the UNSW application has opened.

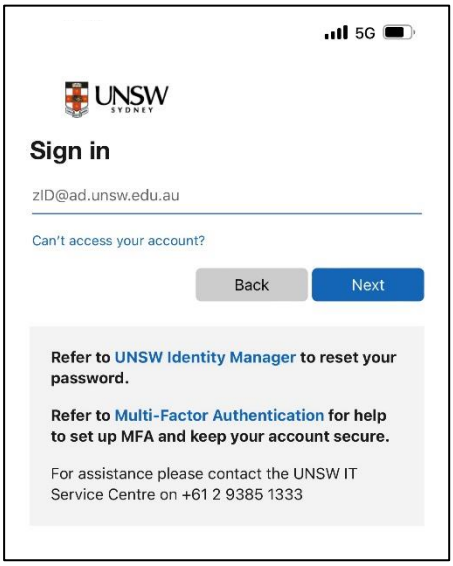
Signing in from your Smartphone

Follow these instructions to use the Microsoft Authenticator app to verify your sign-in to University single sign-on (SSO) applications when prompted.

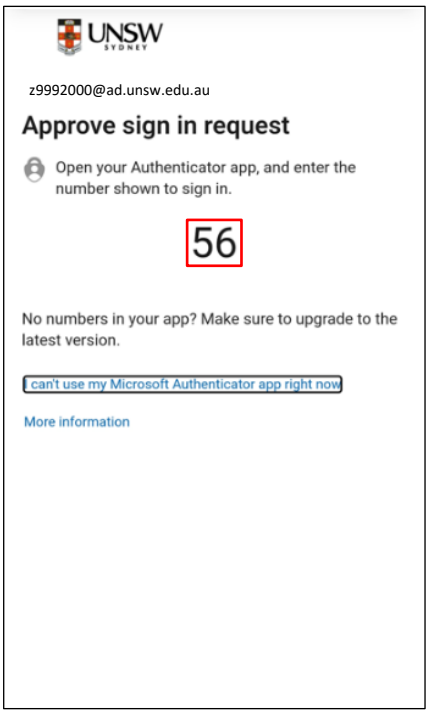
1. **On your smartphone**, access your UNSW single sign-on (SSO) application. If prompted, sign-in using your zID@ad.unsw.edu.au and password and click **Next**.



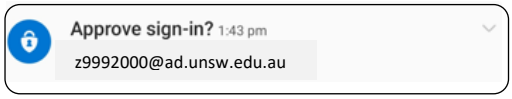
Moodle sign-in screen shown as an example of an SSO application

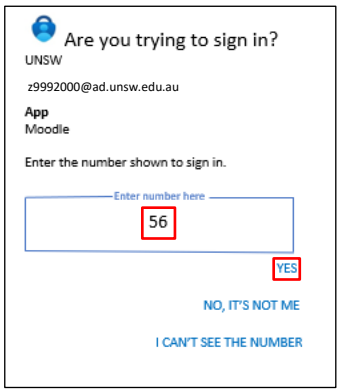


2. **On your smartphone**, you will be presented with the *Approve sign-in request* window which includes a 2-digit number.

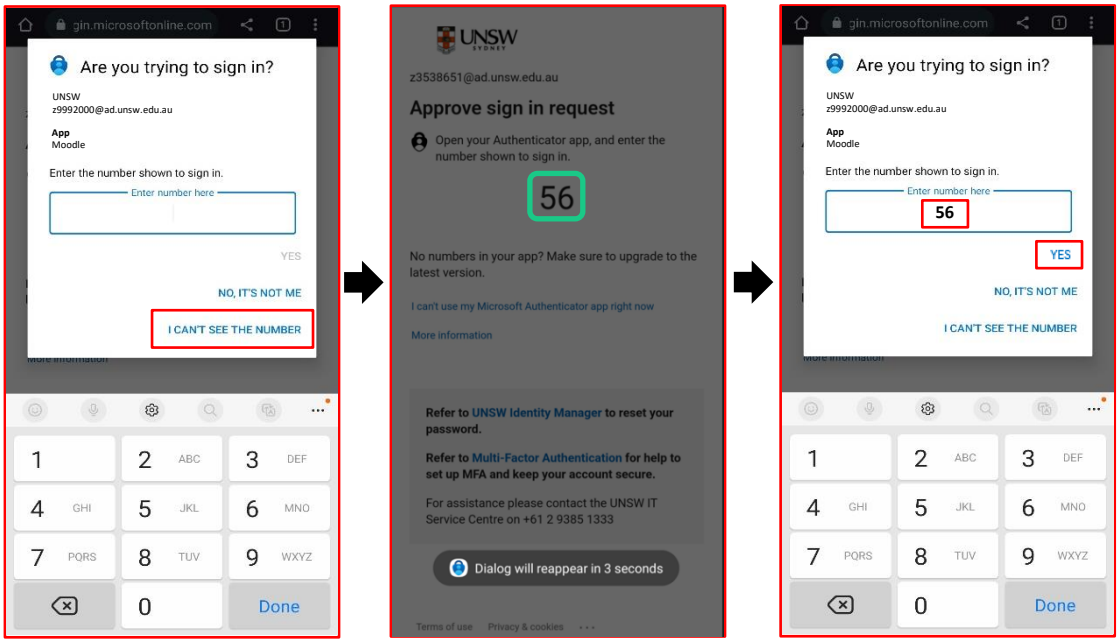


3. **On your smartphone,** an Approve sign-in notification will appear, tap on it, enter the 2-digit number then and click **Yes.**





Usability Note, if *Approve sign-in request* window disappears before you take note of the 2-digit number then tap **I CAN'T SEE THE NUMBER** which will bring the dialog window again.



Note, the 2-digit number is not your 6-digit one-time password code (OTP).

Congratulations, you have just verified your log in, and the UNSW application has opened.