Use Microsoft Authenticator app without a data connection or if push notifications are unavailable

Multi-Factor Authentication (MFA)
Updated: 4 July 2022

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 verify your sign-in to UNSW single sign-on applications using the Microsoft Authenticator app when you do not have internet/data connectivity or when the push notifications are disabled/blocke/d unavailable on your smartphone.

For help with MFA contact the IT Service Centre on 02 9385 1333 or alternatively visit the MFA website to access support guides and all information.

To complete this task, you will need
- To have set up MFA using Microsoft Authenticator.

Instructions

When your smartphone doesn’t have data/internet connectivity, you can follow these instructions to verify your sign-in to UNSW single sign-on (SSO) applications when prompted. Within the Microsoft Authenticator app, under your zID account, you can use the One-Time Password, a 6-digit code that changes every 30 seconds.

1. **On your computer**, access your UNSW SSO application and when prompted, sign-in using your zID and password.
2. On your computer, when presented with the Approve sign-in request screen, click I can't use my Microsoft Authenticator app right now.

3. On your computer, click Use a verification code.

4. On your smartphone, open the Microsoft Authenticator app and tap on your zID account to see the One-time password code.

Note: The one time 6-digit code changes after 30 seconds. If this happens when you are entering it, use the next code that appears.

5. On your computer, enter the 6-digit One-Time password code shown in the app and click Verify.

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