UNSW
SYDNEY

Set up MFA when Microsoft Authenticator app is unavailable in your smartphone’s app store

Multi-Factor Authentication (MFA)

Updated: 14 July 2022

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

Only use this guide when the Microsoft Authenticator app is not available in your smpp gcaotctph(( )Tjmpp n y)-1.

Note: When accessing a single sign-on application such as Moodle, if you are presented with a **More information required** window (see image), it is an indicator that you have not set up MFA and MFA is enforced on your zID account.

At this point you must set up MFA before you can access the SSO application.

If the screen contains a counter, then you have a limited amount of time to defer the set up. Once the counter expires you will not be able to ac .

This instruction to set up MFA is in two parts: Part 1 is the installation of the app on your smartphone and Part 2 is to finish the registration using your computer.

If you already have Microsoft Authenticator app on your smartphone, please start from Part 2.

Part 1 : Install the Microsoft Authenticator app on your smartphone (when you do not have access to the app in your smartphone app store).

1. Go to Authenticator (lenovomm.com) and scan the QR code shown to install the Lenovo app store on your smartphone.

Part 2 : Register Microsoft Authenticator on your computer .

1. On your computer , open a web browser, (E.g., Chrome,
1.r.4 (e,i1 (r)-1.6 (r)-17 (om)-1.7 (eroft 1.3 (.gdge]TJ 0 Tc 0 Tw (4)1.3 (o)0..4 (p)r]TJ 0 T01 Tc -0.001 Tw 12

5. On your computer , at the Set up your account