How to
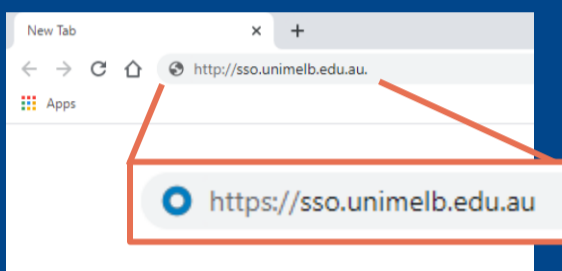# Setup Google Authenticator

This visual guide will help you quickly and easily configure Google Authenticator as a backup verification factor <u>following successful enrolment with Okta Verify</u>.
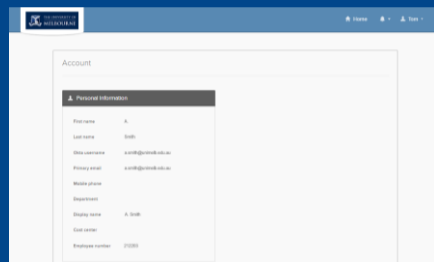**You will need <u>internet access on a desktop or laptop</u> and <u>a compatible smartphone</u>.**
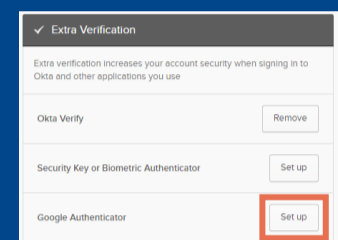
Step 1

On your preferred web browser, visit **http://sso.unimelb.edu.au** and login with your University credentials.
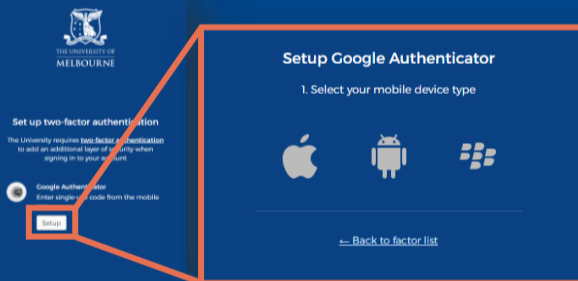
Step 2

You will be signed into your MFA self-service dashboard.
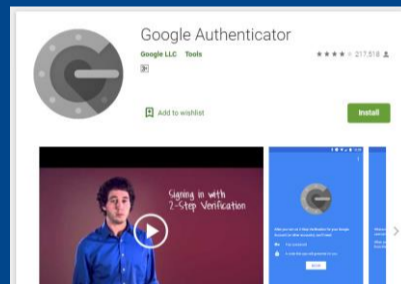
Step 3

Navigate to the Extra Verification settings and select **Setup** next to Google Authenticator. Google Authenticator becomes available <u>after successful enrolment with Okta Verify.</u>
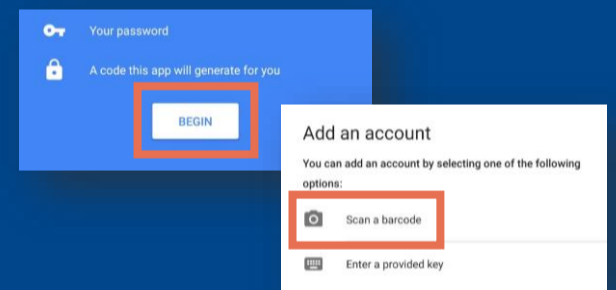
Step 4

From the 'Set up Multifactor Authentication' screen, select **Setup**. Then your device type.

Step 5

Download and install the Google Authenticator app on your smartphone from the relevant app store.
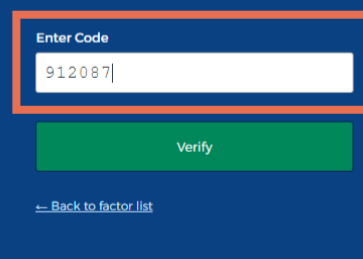
Step 6

Open Google Authenticator on your smartphone. Tap **Begin** then **Scan a Barcode.**
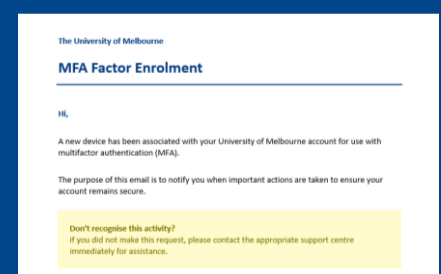
Step 7

When prompted, use your smartphone camera to scan the generated QR code.

Step 8

Enter the 6-digit code on your web browser into the Google Authenticator app on your smartphone.

Step 9

Congratulations!
You are now enrolled with Google Authenticator and will receive a confirmation email.

For information on cybersecurity, visit
Unimelb.edu.au/cybersecurity

Need help with MFA? If you require further assistance, please contact the Service Centre (Staff) or Stop 1 (Students).