Getting started with MFA
For Executive Assistants

Multifactor Authentication (MFA) is an additional security step to verify users' identities when they login to key University applications. This extra layer of security protects user accounts from unauthorised access.

Enrolment for Executive Assistants

University Executives and Executive Assistants must enrol for Multifactor Authentication with Okta Verify. You will need internet access on a web browser, the Executive's smartphone and the Executive Assistant's smartphone.

Step 1:
Check compatibility of both the primary and secondary user's smartphones at **unimelb.edu.au/cybersecurity**

No smartphone or devices not compatible? Please contact the VIP Hotline for assistance.

Step 2:
Decide who will use Okta Verify (primary user) and who will use Google Authenticator (secondary user).
Please note: Okta Verify is the recommended primary factor for Executives.

Primary User
(Recommended as Executive)

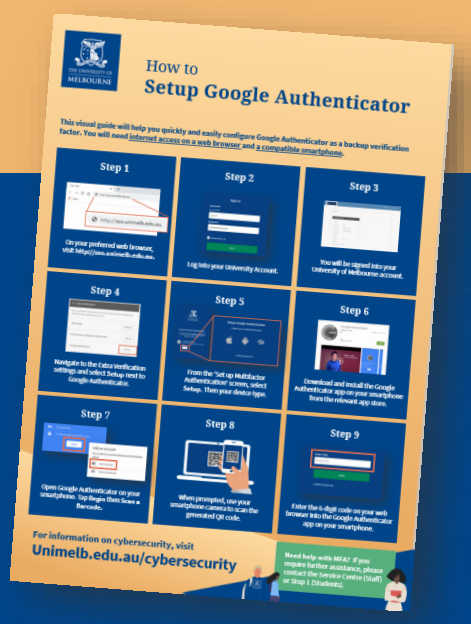
Secondary User
(Recommended as Executive Assistant)

VIP Hotline:
40555
(7:30am – 7:30pm weekdays)

Step 3:
The primary user must be enrolled first, following the steps in **How to Setup Okta Verify guide** attached.

Step 4:
Once the primary user has enrolled with Okta Verify (see Step 3), Google Authenticator will become available as a recommended backup authentication factor in their MFA self-service dashboard at ss**o.unimelb.edu.au.**

Please enrol with Google Authenticator on the secondary user's smartphone following the steps in the attached **How to Setup Google Authenticator** guide.



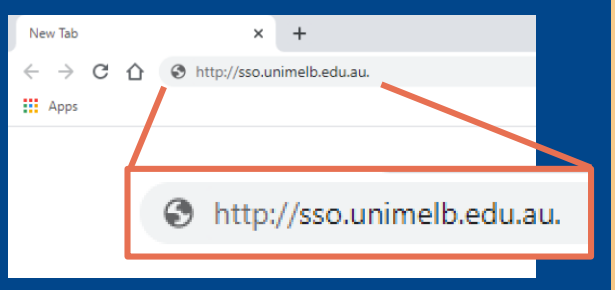
Congratulations! You have successfully configured MFA.

Need assistance? Please contact the VIP Hotline on 40555 (7:30am – 7:30pm weekdays)

How to
Setup Okta Verify

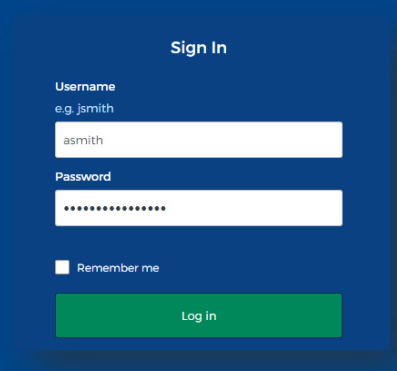
This visual guide will help you quickly and easily enrol your smartphone for Multifactor Authentication. You will need internet access on a web browser and a compatible smartphone (iOS 11.0 compatible device, Android version 4.4+, Windows Phone version 8.0+).

Step 1



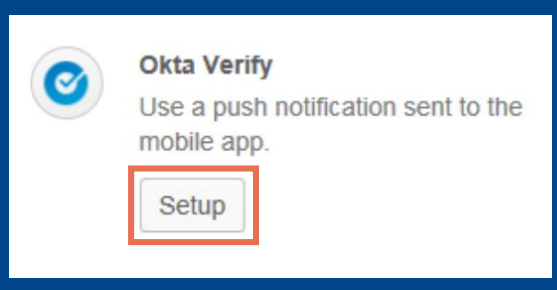
On your preferred web browser, visit **http://sso.unimelb.edu.au.**

Step 2



Login with your University credentials.

Step 3

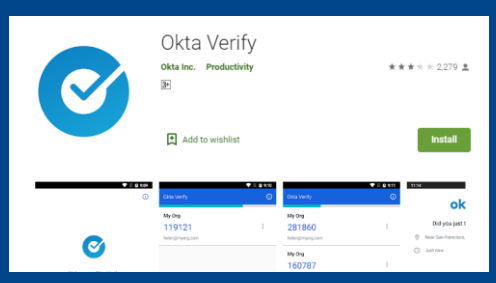


To get started with enrolment, click the **Setup** button.

Step 4

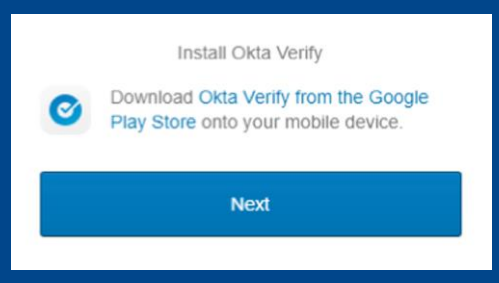
Select your device type.

Step 5



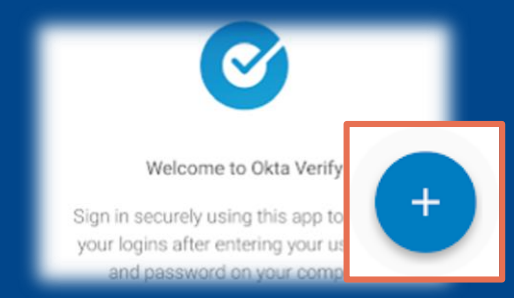
On your smartphone, search for the **Okta Verify app** on the relevant app store, download and install it.

Step 6



On your computer, click **Next** to commence enrolment.

Step 7

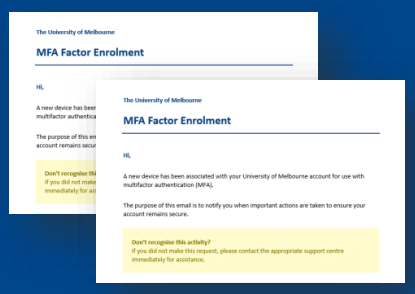


Open Okta Verify on your smartphone and tap the "Add Account" or + **button.**

Step 8

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

Step 9



Congratulations!

You are now enrolled with Okta Verify and will receive two enrolment confirmation emails.

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

Need assistance? Please contact the VIP Hotline on 40555 (7:30am – 7:30pm weekdays).

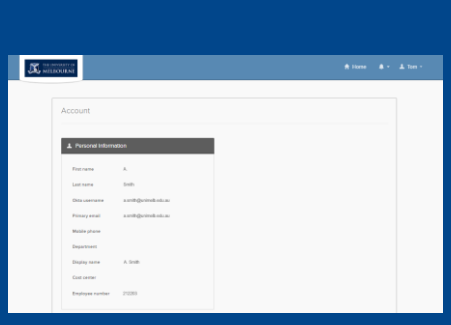
How to
Setup Google Authenticator

This visual guide will help you quickly and easily configure Google Authenticator as a backup verification factor. You will need internet access on a desktop or laptop and a compatible smartphone (Android version 2.3.3+, iOS version 7.0+).

Step 1

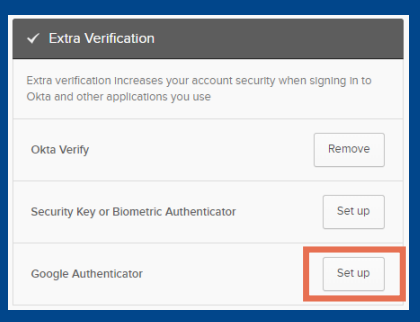
The Primary User must first be enrolled on Okta Verify as detailed in the **Getting started with MFA For Executive Assistants guide.**

Step 2



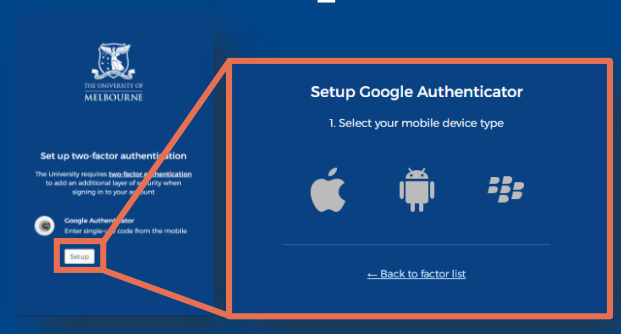
Access the primary user's MFA self-service dashboard (**sso.unimelb.edu.au**).

Step 3



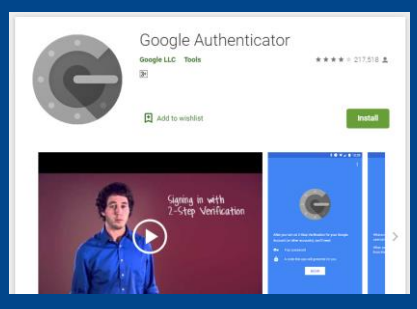
Navigate to the Extra Verification settings and select **Setup** next to Google Authenticator.

Step 4



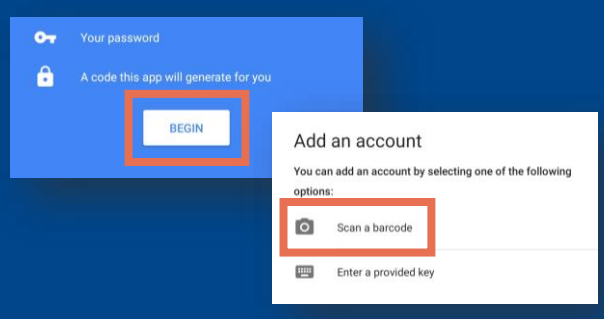
From the 'Set up Multifactor Authentication' screen, select **Setup**. Then the secondary user's device type.

Step 5



Download and install the Google Authenticator app on the secondary user's smartphone.

Step 6

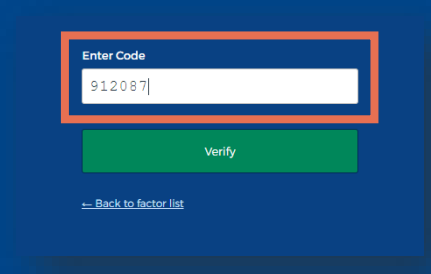


Open Google Authenticator on the secondary user's smartphone. Tap **Begin** then **Scan a Barcode.**

Step 7

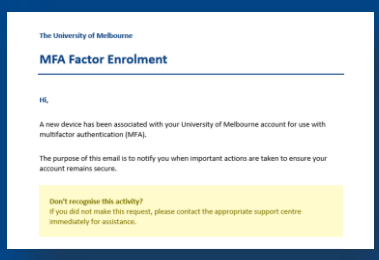
When prompted, use the secondary user's smartphone camera to scan the generated QR code.

Step 8



Enter the 6-digit code on the web browser into the Google Authenticator app on the secondary user's smartphone.

Step 9



Congratulations!

You are now enrolled with Google Authenticator and will receive an enrolment confirmation email.

For information on cybersecurity, visit

Unimelb.edu.au/cybersecurity

Need assistance? Please contact the VIP Hotline on 40555 (7:30am – 7:30pm weekdays).