Multi-Factor Authentication – Frequently Asked Questions (FAQs)

The University of Canterbury (UC) has enabled Multi-Factor Authentication (MFA) for all UC Microsoft 365 applications (e.g., Outlook, Word, Excel, OneDrive, PowerPoint, SharePoint, Teams).

Who will need to use MFA?

All students, staff, visitors, and alumni are required to have their accounts protected with MFA.

What is MFA?

MFA is a quick, easy way to confirm your identity when logging into online services such as Microsoft 365, banking, social media accounts, and online grocery shopping.

MFA uses a second method of authentication alongside your password to ensure it's actually you logging in to your account. This 'second check' confirms that you are who you say you are and can be done through:

- Microsoft Authenticator
- An authentication app
- Passkey (specific YubiKeys)

What applications require MFA?

All UC Microsoft 365 applications will require MFA, such as Outlook, Teams, OneDrive, Word, Excel, SharePoint, Forms and PowerPoint.

What are my authentication options?

You can choose up to four methods; we recommend using one primary and one backup method.

In order of preference and level of security:

- Notification or number matching through the authenticator app
- Passkey
- Verification / one-time passcode from the authenticator app

Users in China have some restrictions on options. For guidance for users based in China, please see the advice on the webpage.

Why are we doing this?

Every week, numerous threat actors attempt to compromise UC accounts through methods such as phishing emails and password-spray attacks. MFA establishes a second line of defence, ensuring cybercriminals will require more than just an email and password to access your account.

How often will I need to use MFA?

You will be asked to MFA when you access any of your UC Microsoft 365 applications.

If you use the web browser to access your M365 account (e.g., www.office.com) you may be asked more frequently depending on your local browser settings. The best experience is to use the Microsoft Outlook application on your device, or the Google Chrome browser.

How do I know if I have registered for MFA correctly?

You can use these instructions to review your MFA registration.

Why am I being re-prompted for MFA regularly?

There are scenarios where users may be re-prompted for MFA if they:

- Sign out and sign in again to any Microsoft 365 apps
- Don't logon for an extended period of time
- Use multiple different devices
- Swap between multiple accounts e.g, a personal account and your UC student account
- Use multiple different web browsers (such as Chrome and Firefox)
- Unexpected activity is detected (such as sign-in from another country)

What is Risky sign-in?

You may also be asked to MFA if risky sign-in activity is detected on your account.

Such scenarios could include; when you're accessing Microsoft 365 on a new or different device, or your credentials have been reported as, or have been, compromised.

In that case, then you may be asked to verify that it's really you via MFA.

Do I have to use the Microsoft Authenticator app? What are the alternatives?

You could use other authenticator apps such as Ente Auth. Please note that the Microsoft Authenticator app is the only application supported by the IT Service Desk should you encounter any issues that require technical assistance.

Can I opt-out of MFA?

No, all UC staff, students, visitors, and alumni UC M365 accounts are required to be protected with MFA.

MFA is a measure to protect you against unauthorised access to your UC account.

I do not own or regularly use a mobile phone, or I do not want to use my mobile phone for work.

That's no problem; we recommend that you look to purchase a YubiKey and register it via aka.ms/mfasetup.

What happens when I sign in using MFA?

Your experience will differ depending on what you choose to use as your MFA method; please see below for a synopsis of each method available.

First, you'll need to sign into your UC Microsoft 365 using your username and password.

- an authentication app number matching/push notification
    1. A number will appear on the device screen, please enter the number shown. You will also see the IP location from the sign-in
    2. A push notification with a message such as: 'approve/deny' appears on your smartphone
    3. Tap 'approve or deny.'

- a verification/one-time code via the authenticator application
    1. Open the authenticator app on your smartphone
    2. Select your University of Canterbury account
    3. Find the verification / one-time passcode (time-sensitive)
    4. Enter the verification / one-time passcode in the box provided on the sign-in page.

Privacy questions

Please see the privacy considerations FAQ section on our webpage.

What do I do if I can't get into my account? I have lost my phone. I have left my phone at home. Or I don't have my mobile device with me.

This happens. Please get in touch with the IT Service Desk on 03 369 5000 or 0508 824 843 (after hours).

If you are unable to use a phone:

Students

- Go to Te Pātaka, Student Services Hub, located in the centre of Ilam campus on levels 2 and 3 in Puaka-James Hight Central Library for in-person help, or to use a phone to call the IT Service Desk.

Staff

- Go to Matariki, Ground Floor, for in-person help (10 am – 4 pm, Mon-Fri).

Why is the Authenticator app more secure?

The primary reason is that it is easier for a hacker to gain physical access to your mobile phone. It is very easy to perform SIM swapping (stealing your phone number) and intercept any incoming SMS text messages, or phone calls received for authentication.

With the Authenticator App, the codes are generated and stored temporarily on your phone (or another device) and expire within a specific timeframe.

What should I do if I receive a verification request but I am not trying to sign in?

This may be an unauthorised access attempt, and we recommend that you decline the request and contact the service desk.

What if I travel frequently or am regularly on field trips? What should I do if I don't have mobile data or good cellular service?

We recommend setting up the Microsoft Authenticator app and using the push notification or verification code / one-time passcode.

While the "approve/, deny" option is the most convenient method within the Authenticator app, the one-time verification codes will continue to generate on your phone even if it has no service. We also recommend setting up multiple options, such as the one-time password as a backup.

Please remember to access your UC Microsoft 365 applications online; you will also need access to Wi-Fi/data.

How do I change my MFA settings?

You can always return to aka.ms/mfasetup and change your MFA verification methods at any time.

We encourage you to use the Microsoft Authenticator App as your first option because it offers you convenience, reliability and security. We also recommend setting up more than one verification method where possible.

What if I don't want to install an app on my phone or my phone doesn't have the capability?

If you don't want to install the Microsoft Authenticator app on your phone, you can use the Passkey option through a YubiKey.

How do I know if I have already registered or not?

You can check your MFA registration settings by using this link: aka.ms/mfasetup, to see the verification options you have set up.

If you can't see any of your chosen options displayed, the registration process is incomplete. Please try again.

What happens if I get a new mobile phone? I have a new phone number. How do I register for MFA?

You can change your MFA details at any time via the link: aka.ms/mfasetup.

You can update your MFA options, including setting up the Authenticator app to receive notifications.

How do I restore my Authenticator App to a new phone?

Microsoft Authenticator provides a backup and restores capability for accounts.

To move your Microsoft MFA account to a new phone, follow these steps:

- Open the app on your old phone
- Tap the three dots at the top right
- Tap "Settings"

- Enable “Cloud backup”/”iCloud Backup”
- On your new phone, install the Microsoft Authenticator app and log in to your account
- Select “Begin Recovery”.

Your account and its settings will be added to your new phone.

Are there any costs?

The Microsoft Authenticator app uses a tiny amount of data to perform the “Approve/Deny” notification. However, if you use the code generated within the Microsoft Authenticator app, this has no charge.

Version: 0.17E, Last updated: 03/10/2025