

Multi-factor authentication (MFA)

Signing in to Office 365 for the first time and setting up MFA.....	1
Before you begin	2
Are you at home or on campus?	2
Section A. On campus	2
Section B. At home.....	2
Section C. Common steps to complete	4
Installing and configuring the Microsoft Authenticator App on iPhone	6
How to update your preferred MFA verification option at any time	9
How to reset your MFA configuration to start again.....	9

Signing in to Office 365 for the first time and setting up MFA

When you first access Office 365, you sign in using your University of Otago email address and need to set up multi-factor authentication (MFA). If your access is from:

- on-campus, you set it up manually
- off-campus, you will be prompted to do it when you log in

Multi-factor authentication (MFA) is a security mechanism that requires you to provide two or more known pieces of information in order to authenticate your identity. For example, logging in to your bank account via a web browser may require you to enter a code sent to your mobile phone or use the bank's mobile app to confirm your access. Using Office 365 at home requires you to approve the access using the "Microsoft Authenticator" app on your mobile phone or to enter a code sent to it.

After setting up MFA, keep your mobile phone handy whenever you sign in to Office 365 so you can confirm your identity.

Please note that once MFA is set up on your mobile phone, your ongoing access to Office 365 will be linked to it. If you lose or need to replace your phone, please contact AskOtago for assistance:

Tel +64 3 479 7000 or 0800 80 80 98

Email askotago.it@otago.ac.nz

Before you begin

During the MFA setup process Microsoft will ask “How should we contact you” [to perform MFA checks as you log in]. The options are:

- **Mobile App:** At Otago this refers to the “Microsoft Authenticator” app that you install on your mobile phone, and means that when you log in to Office 365, Microsoft will either request a one-time code from the app or send the app a “please approve this login” message that you respond to.
- **Authentication Phone:** this also refers to your mobile phone, but in this case when you log in, Microsoft sends an SMS (TXT) code to your phone that you will enter on the Office 365 login page. Alternately, they will call your phone to confirm your identity.

The University's Cyber Security Team strongly recommends that you use the “Microsoft Authenticator” app on your mobile phone as your primary additional verification option, as it provides the highest level of security for your account and data.

If you are unable to install the “Microsoft Authenticator” app onto your mobile phone, you can receive a text code as an alternative identity verification method.

Are you at home or on campus?

Depending on your location, follow the steps in either section A. or B. below, then follow the common steps in section C.

Section A. On campus

If you are logging in for the first time while on campus, you will need to go directly to MFA here: <https://aka.ms/mfasetup>

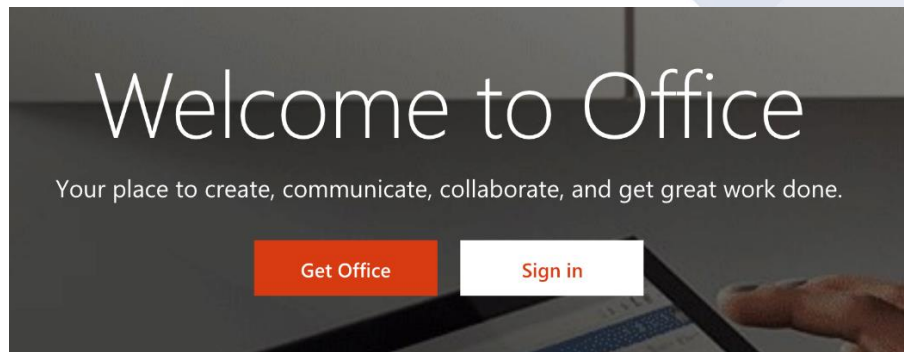
[This video from Microsoft will guide you through the steps](#)

Section B. At home

You will be prompted to set up multi-factor authentication when you first log in to Office 365.

Open a new web browser session with no other tabs running. There is no need to use the University's VPN Service to access Office 365 online when you are off campus.

1. [Go to the Office 365 sign in page](#) and click **Sign in**.



2. Enter your University email address, then press the **Next** button.



Sign in

_____@otago.ac.nz

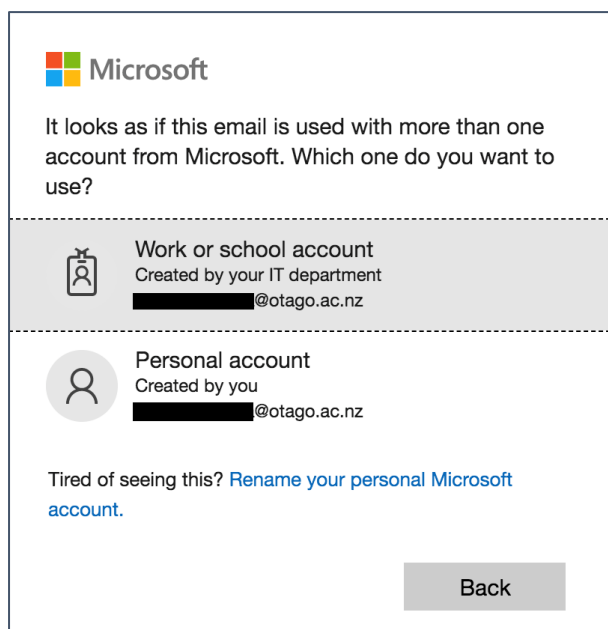
No account? [Create one!](#)

[Can't access your account?](#)

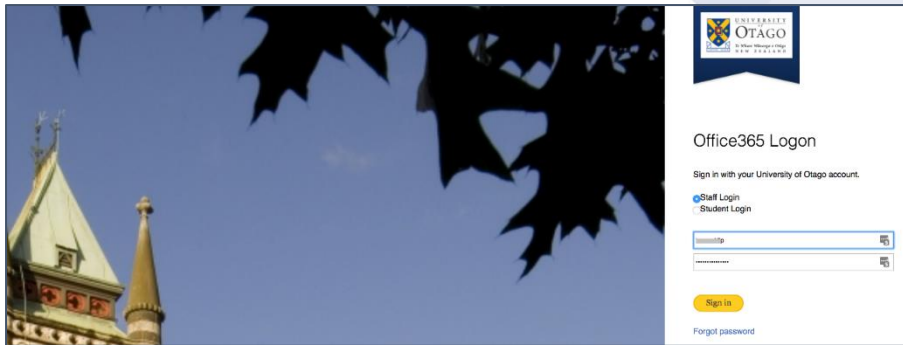
[Sign-in options](#)

Next

3. If you are presented with a choice of accounts to sign in to (as shown below), select **Work or School account**.



4. When Microsoft detects your Otago email address, it will redirect you to the University's secure web-based login service. Select the **Staff Login** radio button and enter your University username and password. You may see either of the two following login screens.



Sign in

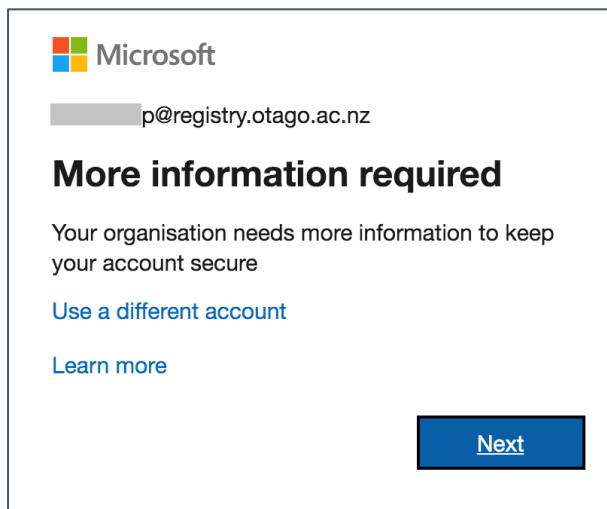
https://adfs.otago.ac.nz

Username

Password

Section C. Common steps to complete

1. In the *More Information required* window, press **Next**.



2. In *Step 1: How should we contact you*, use the drop-down option to change it to Mobile App

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone
 Mobile app
 New Zealand (+64)

Phone number can contain only the digits 0-9, dashes, spaces, full stops and parentheses.

Method

Send me a code by text message

[Next](#)

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

3. Select the **Use verification code** radio button and click **Set up**.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

Receive notifications for verification
 Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.


[Set up](#) Please configure the mobile app.

4. This will bring up the *Configure mobile app* window displaying a QR code. Leave this window open, and go to your mobile phone.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



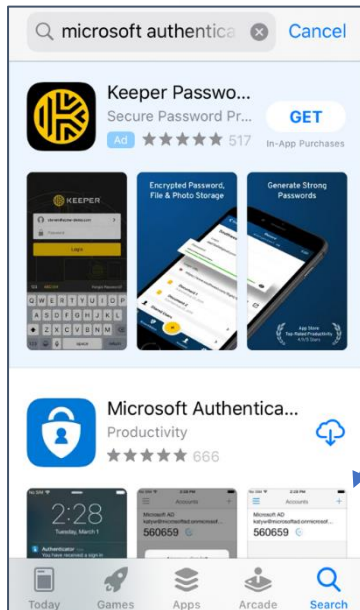
If you are unable to scan the image, enter the following information in your app.
 Code: 345 197 120
 URL: <https://co1eupad05.eu.phonefactor.net/pad/951085251>

If the app displays a six-digit code, choose "Next".

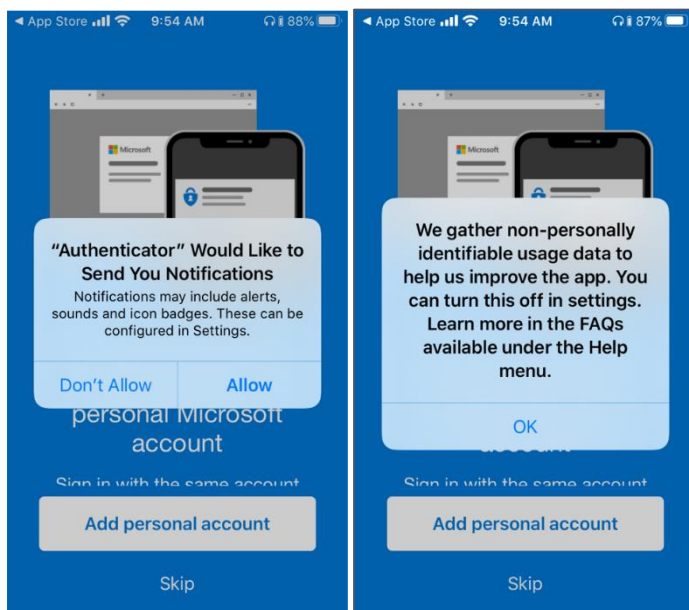
[Next](#) [Cancel](#)

Installing and configuring the Microsoft Authenticator App on iPhone

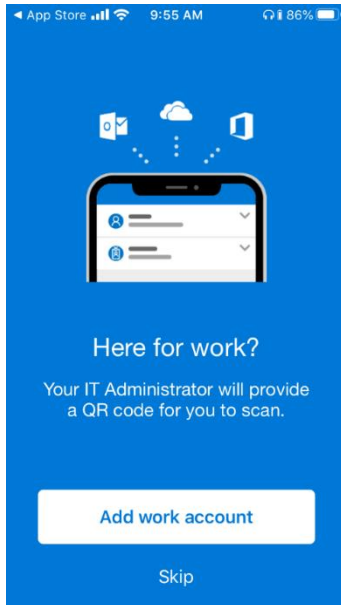
5. Open your App Store, search for **Microsoft Authenticator**, download it, and open it.



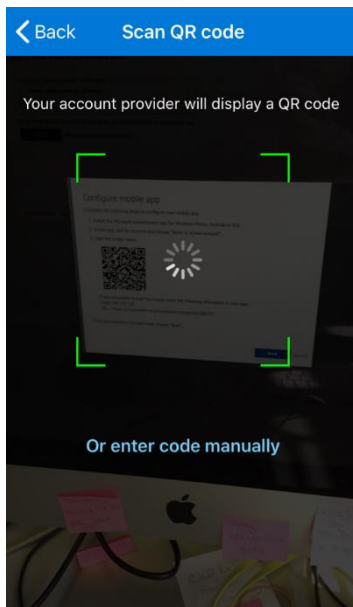
6. When prompted, choose to **Allow** notifications and tap **OK** on the screen that mentions data gathering.



7. Tap the **Skip** link at the bottom until you get to the screen asking if you are *Here for work?* On that screen, tap **Add work account**,



8. Hold your phone camera over the QR code displayed on your computer:



9. The mobile app setup is now complete, so click the **Next** button.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Mobile app has been configured for notifications and verification codes.

10. Add your mobile phone number as a back-up, and press **Finished**.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

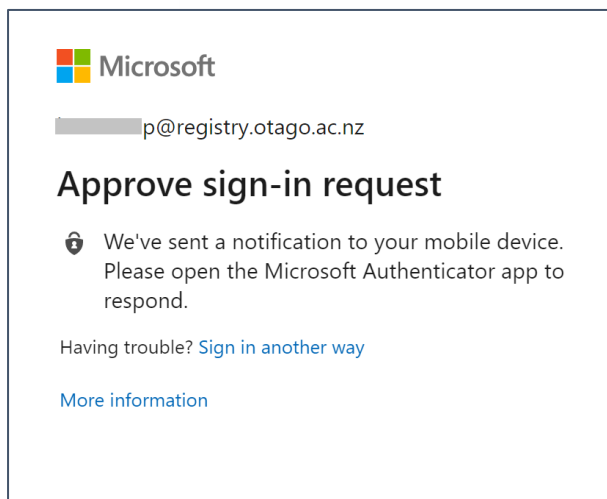
Step 3: In case you lose access to the mobile app

New Zealand (+64)

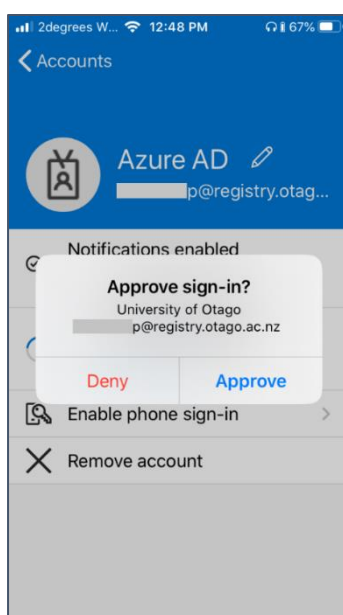
Finished

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

11. You will be prompted to sign into Office 365 again. (Note the link allowing you to sign in another way. This can be used if you have any difficulty with the authenticator.)



12. Signing in will send a notification to your phone. **Approve** this on your phone.



13. You can also tick the box on the prompt to stay signed in while your computer is on.



14. You will see a page showing that you have set up all the security features. You can close this tab and return to Office 365.

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
[View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Notify me through app

how would you like to respond?

Set up one or more of these options. [Learn more](#)

Authentication phone

Authenticator app or Token

Authenticator app - iPhone

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

How to update your preferred MFA verification option at any time

If you have previously set up MFA, and now want to change your preferred verification method (e.g. to use the Microsoft Authenticator app) go to the MFA setup page:

<https://aka.ms/mfasetup>

[This Microsoft video](#) shows you how to set your preferred verification method to use the Microsoft Authenticator app.

How to reset your MFA configuration to start again

If you have problems with your installed MFA and need to start again, please contact AskOtago for assistance:

Tel +64 3 479 7000 or 0800 80 80 98

Email askotago.it@otago.ac.nz