Multi-factor authentication (MFA)

Find this information online in the AskOtago Knowledgebase

About multi-factor authentication (MFA)

Multi-factor authentication (MFA) is a security mechanism that requires you to provide two or more pieces of evidence to authenticate your identity. For example, logging in to a website at home may also require you to approve the access via an app on your mobile phone or to enter a code sent to it. This provides an additional layer of security to ensure your account is not compromised.

MFA and Microsoft 365

Access to Microsoft 365 outside of the University of Otago network requires a second form of identification using a mobile device. An authenticator app should be downloaded to your mobile phone, or if this is not possible, an authentication code can be sent to you via SMS.

You will need to set up MFA when you first log in to Microsoft 365. After setting it up, make sure your mobile phone is available nearby when you sign into Microsoft 365 in case you need to reconfirm your identity.

Once MFA is set up on your mobile phone, your ongoing access to Microsoft 365 will be linked to it.

If you lose or replace your phone, you will need to contact AskOtago for assistance:

Freephone 0800 80 80 98 (within New Zealand)
Tel +64 3 479 7000
Email askotago.it@otago.ac.nz

Multi-factor authentication (MFA) methods

During the MFA setup process, Microsoft will ask "How should we contact you?" [to perform MFA checks as you log in]. The two methods used by the University of Otago are:

Mobile app (preferred)

Download the "Microsoft Authenticator" app to your mobile phone. When you sign in to Microsoft 365, Microsoft will request a one-time code from the app or will send the app a “please approve this login” message for you to approve.

Authentication via mobile phone

If you are unable to use the authenticator app, Microsoft can send an SMS (text message) code to your mobile phone for you to enter on the Microsoft 365 login page.

The University's Cyber Security Team strongly recommends that you use the "Microsoft Authenticator" app on your mobile phone as your MFA method, as it provides the highest level of security for your account and University of Otago data.

The University of Otago recommends the following MFA options in order of preference:

For staff

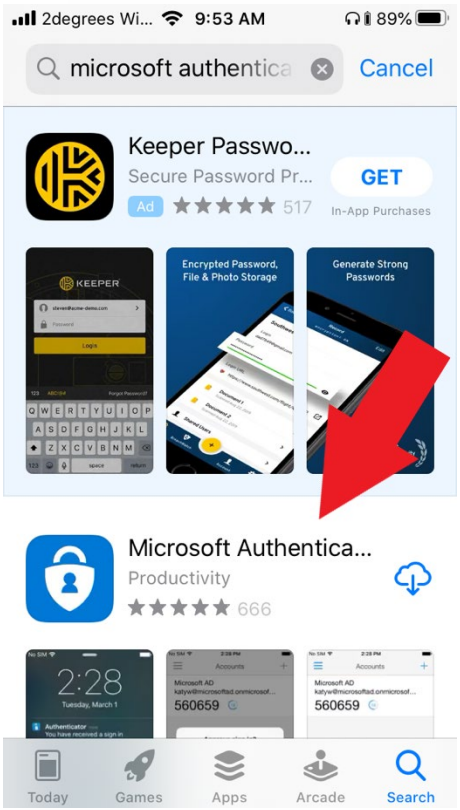
1. Microsoft Authenticator on University-owned/personal mobile device.
2. SMS/phone call to University-owned/personal mobile device.
3. Authy application installed on your own laptop (i.e. not a shared device).
4. Token2 Physical Key if none of the above are suitable.

For students

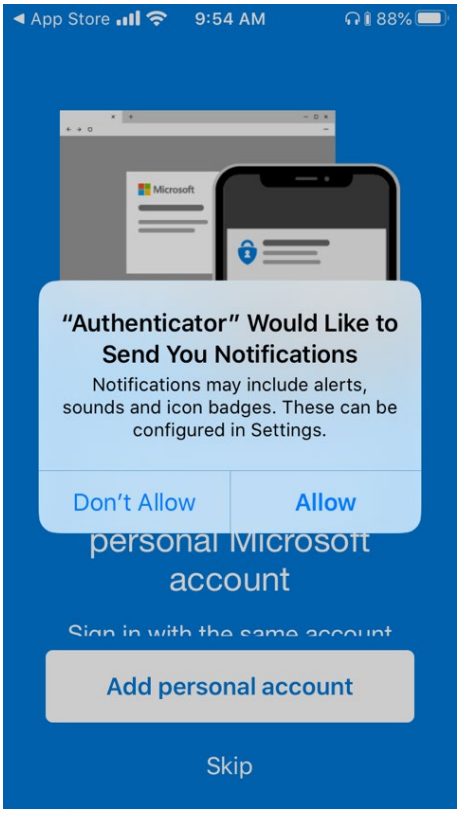
1. Microsoft Authenticator on University-owned/personal mobile device.
2. SMS/phone call to University-owned/personal mobile device.
3. Authy application installed on your own laptop (i.e. not a shared device).

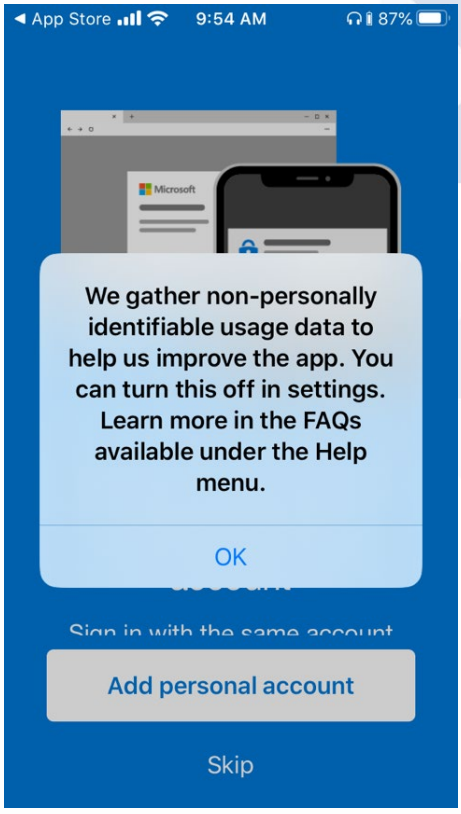
Downloading the Microsoft Authenticator App on an iPhone

1. Open your App Store, search for **Microsoft Authenticator**, download it, and open it. Note: ensure that this is the one offered by the Microsoft Corporation and does not contain in-app purchases.

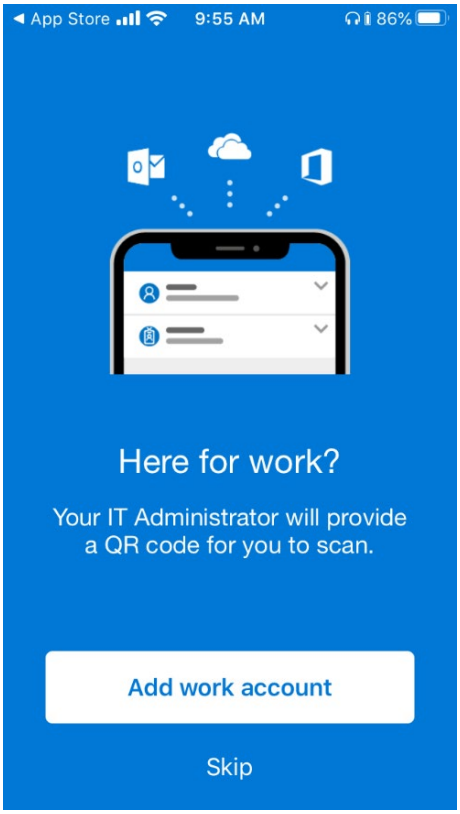


2. When prompted, choose to *Allow notifications* and tap *OK* on the screen that mentions data gathering.



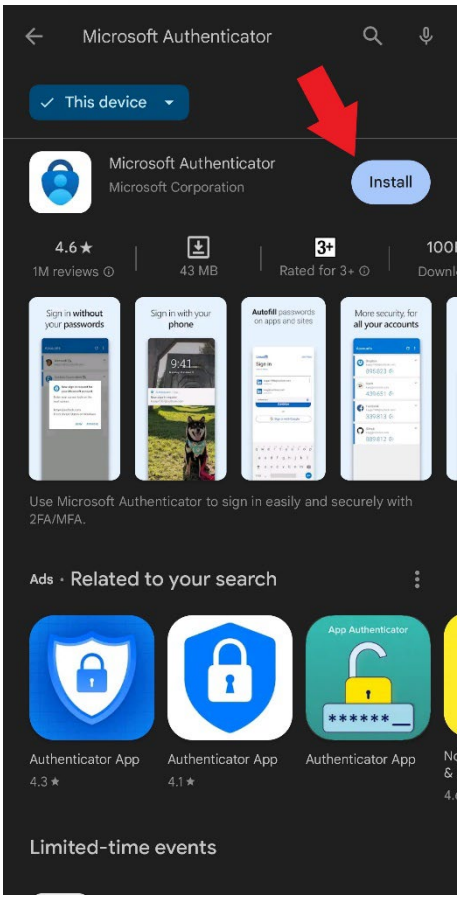


3. Tap the *Skip* link at the bottom until you get to the screen asking if you are **Here for work?** On that screen, tap *Add work account*.



Downloading the Microsoft Authenticator app on an Android phone

1. Open the Google Play App.
2. Search for "Microsoft Authenticator". Note: ensure that this is the one offered by the Microsoft Corporation and does not contain in-app purchases.



3. *Install*, then *Open* the app.

Setting up MFA on campus

Sign into Microsoft 365 for the first time using your University of Otago email address and password. Then go to the MFA set-up page and follow the instructions:

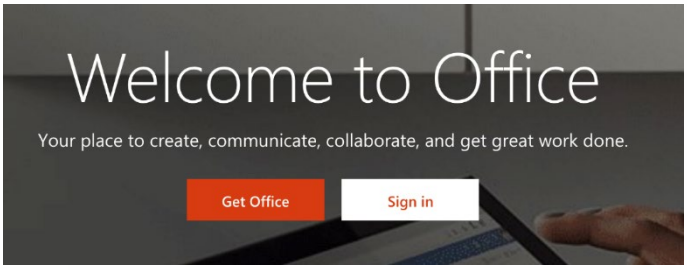
https://aka.ms/mfasetup

You can also see these instructions from step 9 in the off-campus section below.

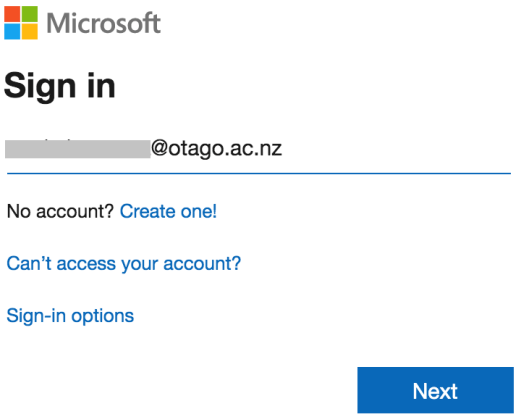
The following Microsoft video will guide you through the steps:

How to register for Azure Multi-Factor Authentication

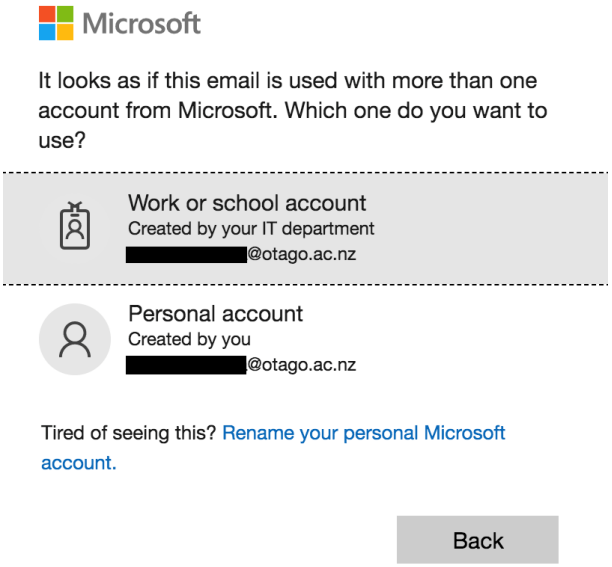
1. Open a new web browser session with no other tabs running. You don't need to use the University's VPN Service to access Microsoft 365 online when you are off-campus. Go to the Microsoft 365 sign in page and click the *Sign in* button.



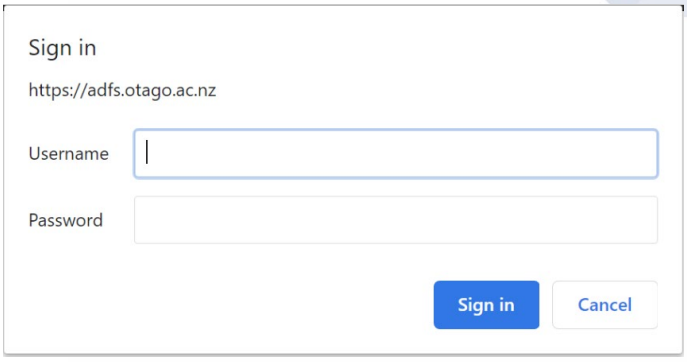
2. Enter your University of Otago email address, then press the *Next* button.



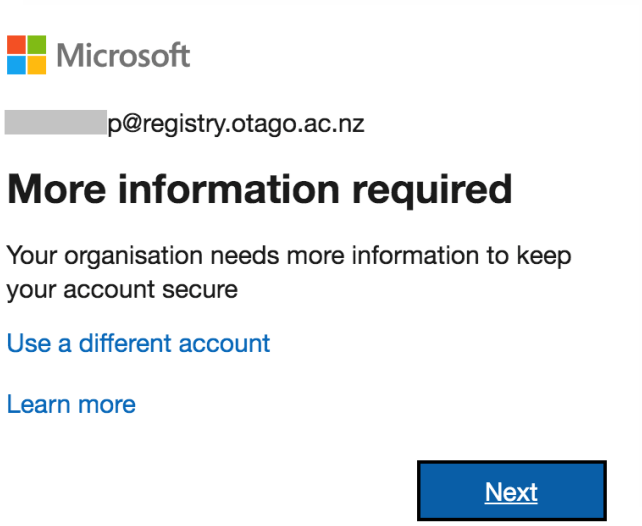
3. If you are presented with a choice of accounts to sign in to (as shown in the screenshot below), select *Work or School* account.



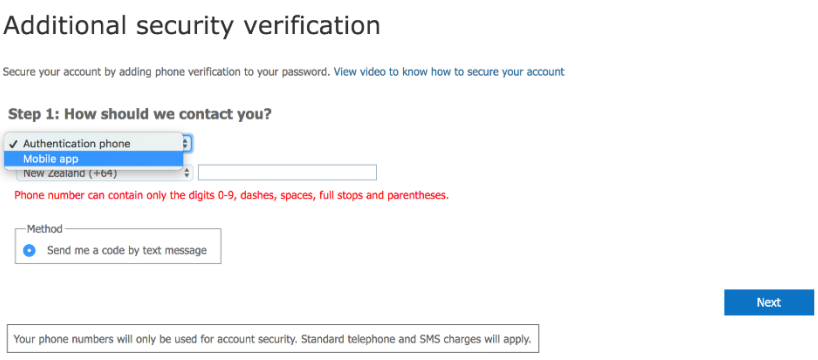
4. Enter your University of Otago username and password, then click *Sign in*.



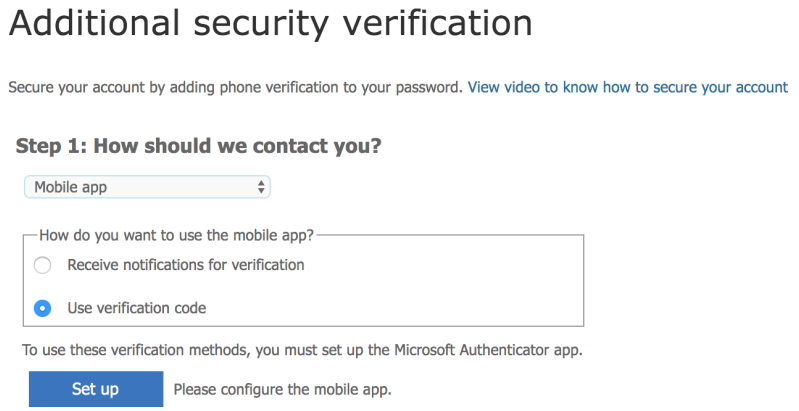
5. In the **More Information required** window, press *Next*.



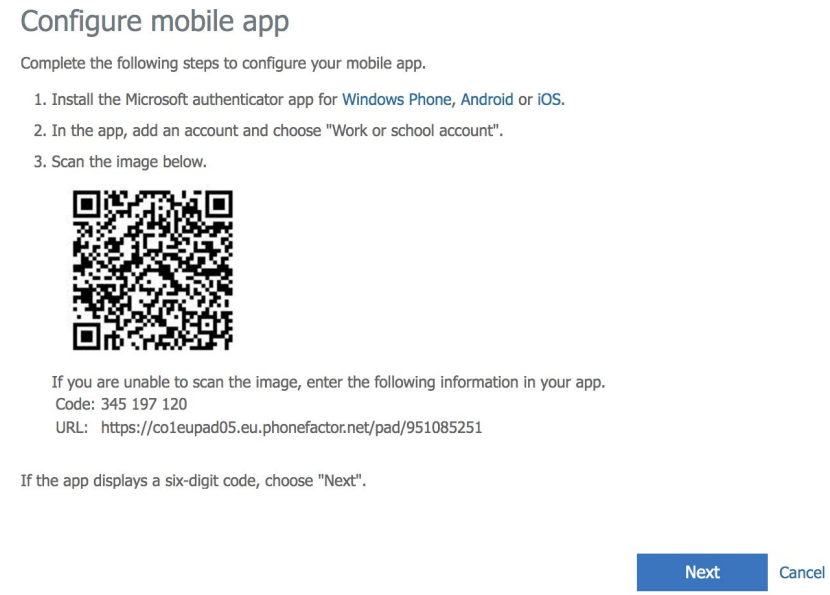
6. In **Step 1: How should we contact you?** use the drop-down option to change it to *Mobile App*.



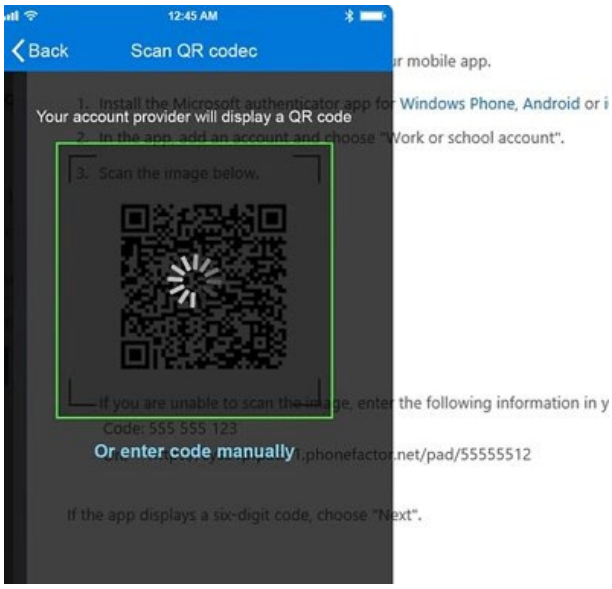
7. Select the *Use verification code* radio button and click *Set up*.



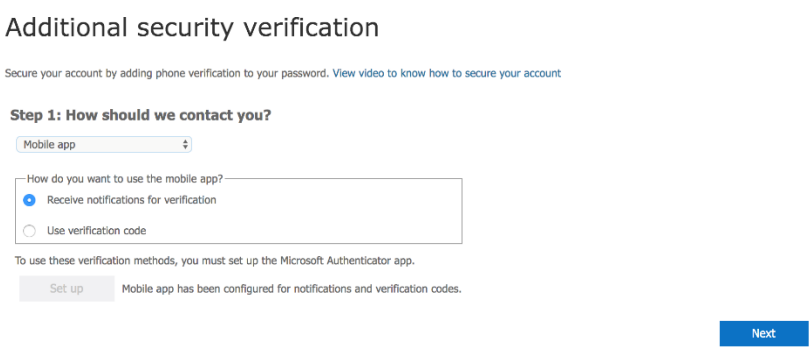
8. This will bring up the *Configure mobile app* window displaying a QR code. Leave this window open and go to your mobile phone.



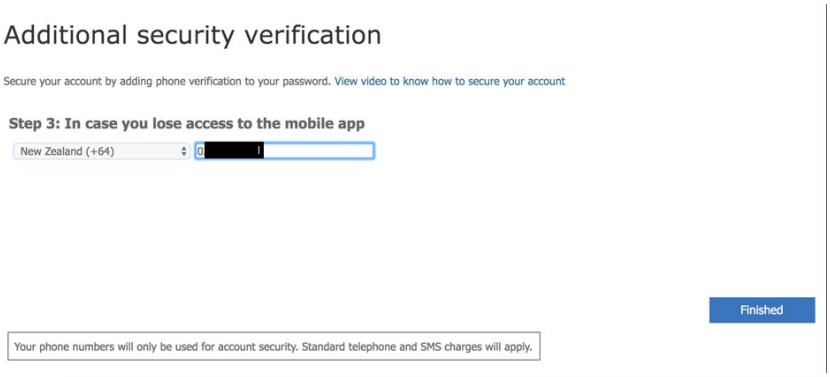
9. Hold your phone camera over the QR code displayed on your computer to scan it.



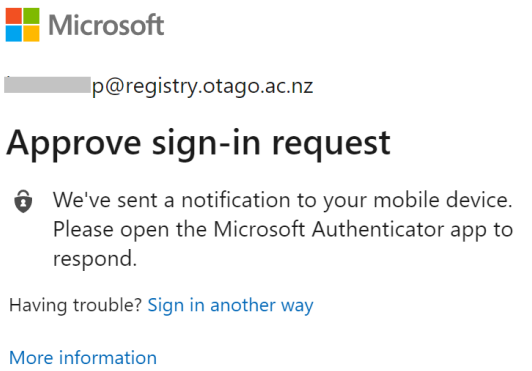
10. The mobile app setup is now complete, so click the *Next* button on your computer.



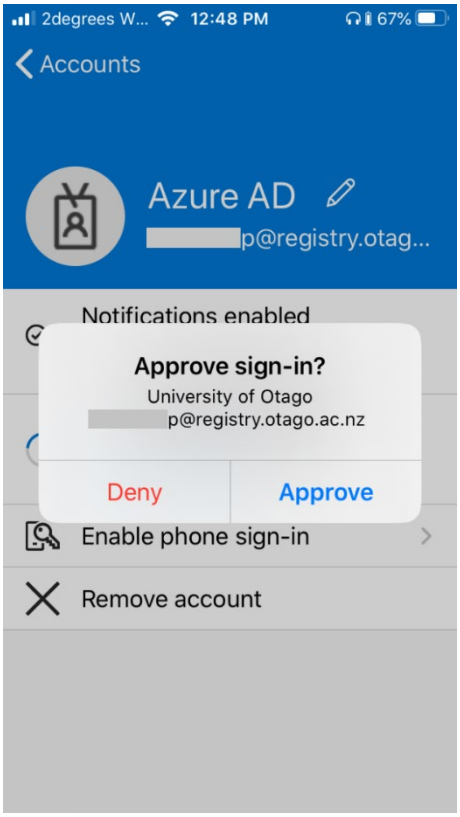
11. Add your mobile phone number as a back-up and click *Finished*.



12. You will be prompted to sign into Microsoft 365 again. (Note: there is a link allowing you to *Sign in another way*. This can be used to send you an SMS if you have difficulty with the authenticator.)

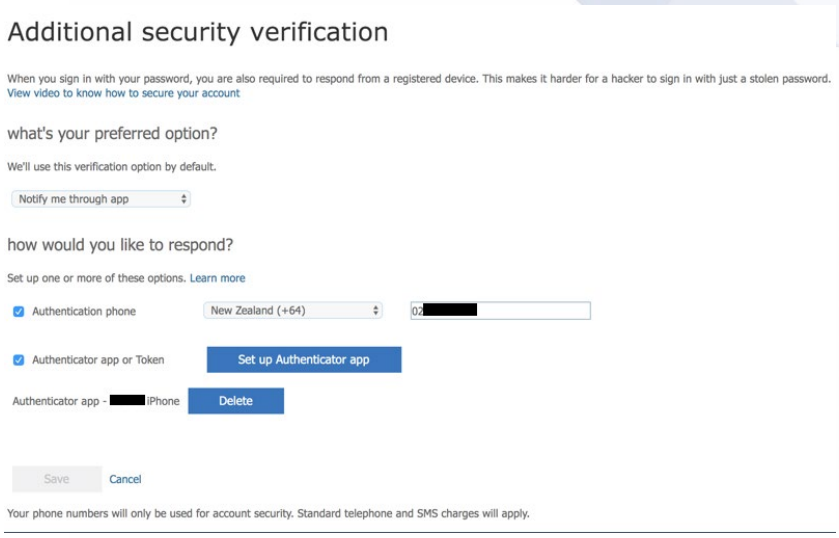


13. Signing in will send a notification to your phone. *Approve* this on your phone. (Remember that your phone needs mobile data or Wi-Fi switched on and notifications enabled for the Microsoft Authenticator app so that it can receive the notification).



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

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



Updating your preferred MFA verification method

If you have previously set up MFA to send an SMS for verification, and now want to change your preferred verification method to use the Microsoft Authenticator app, go to the MFA setup page: https://aka.ms/mfasetup

Click on the *Sign in another way* link and follow the instructions above to set up the Microsoft Authenticator app as your preferred verification method.

Resetting your MFA configuration

If you experience any issues with your installed MFA and need to start again, please contact AskOtago for assistance:

Freephone 0800 80 80 98 (within New Zealand)
Tel +64 3 479 7000
Email askotago.it@otago.ac.nz