Multi-Factor Authentication (MFA) Guide

To access the University's services or systems, you may need to verify your identity via Multi-Factor Authentication (MFA).

When you first try to log into one of the MFA-enabled systems or services you will be prompted to configure a secondary authentication method, you only need to do this set up once, unless you change your phone.

Your MFA settings – Set it up now

- **Need to set up MFA and have computer and/or a smart phone available?**

Update your MFA settings and options – Update it now

- **Already set up MFA phone call, but want to use the app instead?**
- **Got a new phone - add an additional phone to your MFA.**
- **Want to have multiple ways to MFA, including landline phone call, additional devices and apps?**

Having trouble signing in? – Sign in another way

MFA Microsoft Authenticator app set up

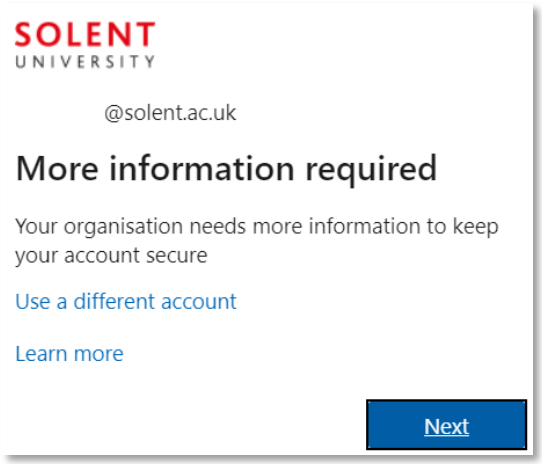
The Microsoft Authenticator mobile app is the simplest and most reliable to use.

The app should work on most Android and iOS handsets.

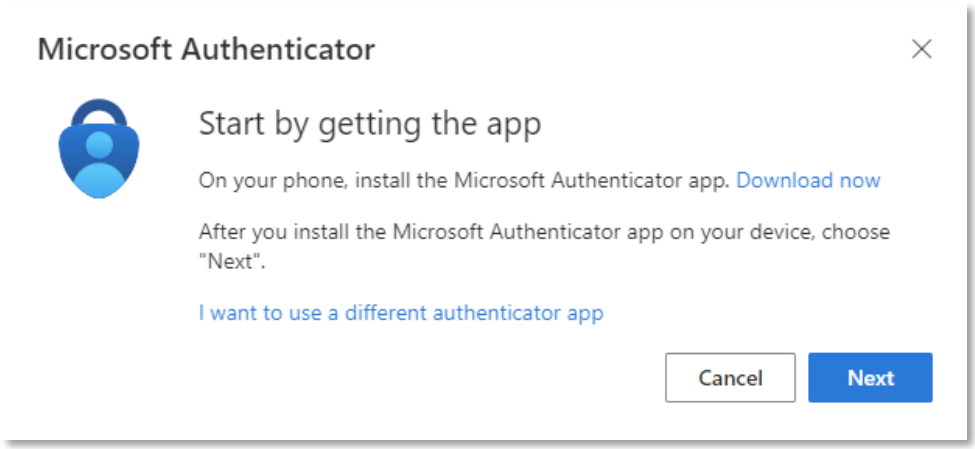
Please note: You will need signal and data on to set up the app, but once configured, the app can be used even if the handset has no mobile signal or internet connection.

Setting up and using the **Microsoft Authenticator App**

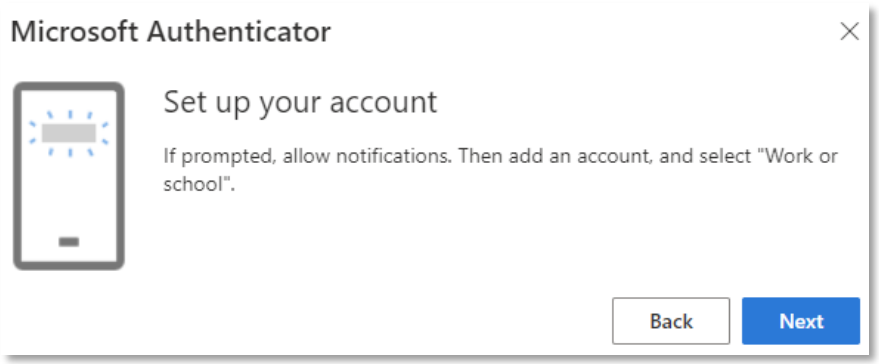
1. You will need a computer and your smart phone/tablet.
2. When you first sign into a university service you will be prompted to provide more information or alternatively click this link to start the process on your computer.



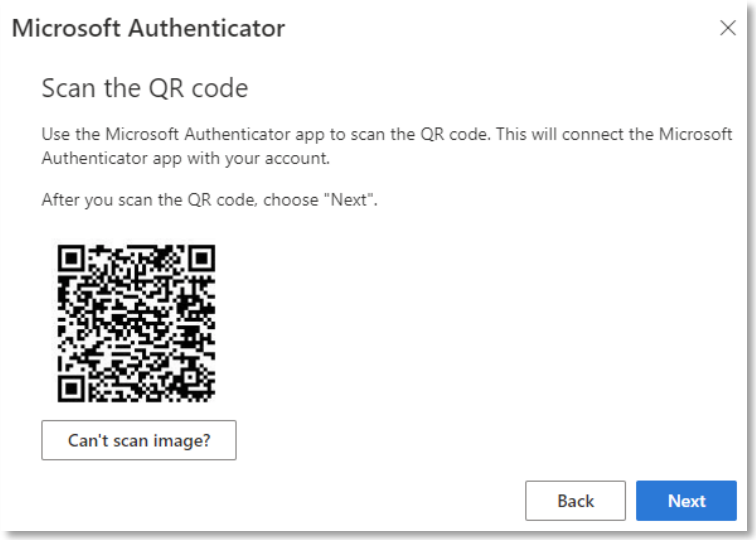
3. Click **Next**



4. On your phone, **install the Microsoft Authenticator app**.
   Available from Google Play, or the Apple App Store
5. Once installed click **Next on your computer/device**
6. Once installed, **launch the app** on your phone and skip through the wizard if required
7. Tap on **Add account (the + sign)** on your phone
8. Select **Work or school account**
9. Click **Next** on your computer



10. Use your phone to **scan the QR code** displayed on your computer
    or
    If you are doing the whole process on your phone, switch to the keeping your account secure page, click **Can't scan image?** and note down the 9-digit code and the URL and enter it manually into the authenticator phone app

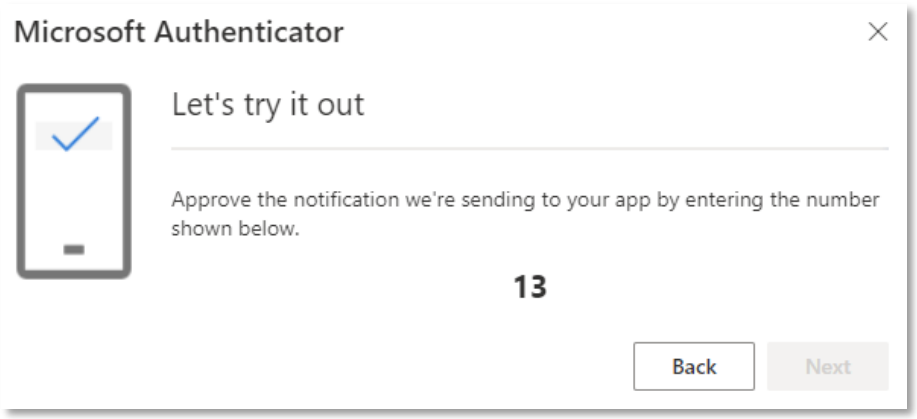


Please note:

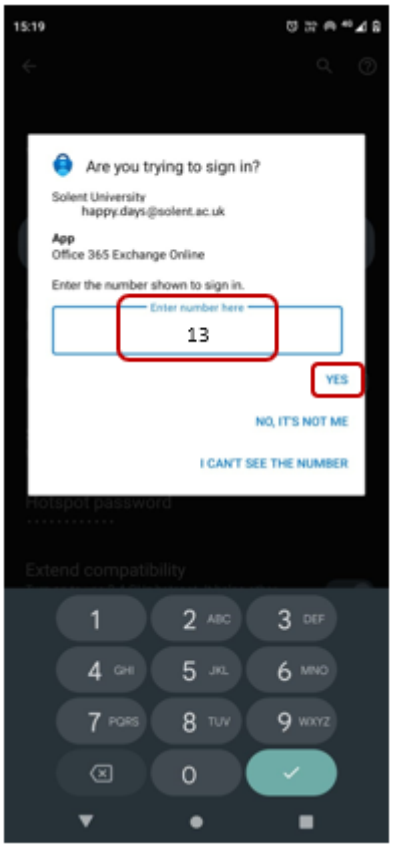
- iPhone users may have to enable the camera, in Settings in order to scan.
- If you can't use your phone camera, you'll have to manually enter the 9-digit code and the URL.
- Your account will be added automatically to the app and will display a six-digit code.

11. Click **Next** on your computer.

12. It will now test the app.

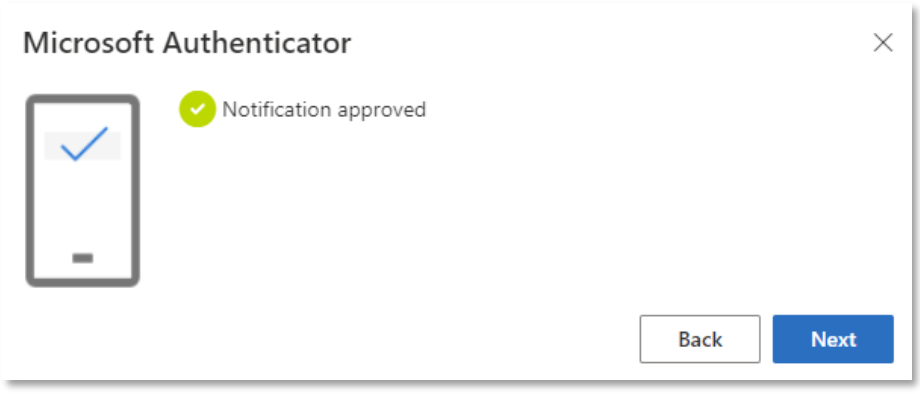


13. On your phone, go to the Microsoft Authenticator app and **enter the number shown on your computer**, then tap **YES**.

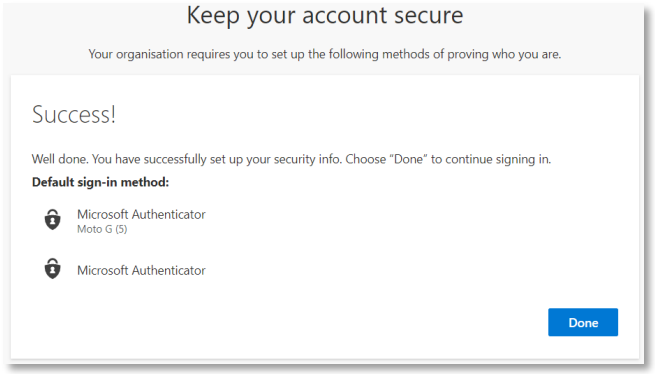


14. Your mobile device may ask you to confirm your devices pin or use your registered fingerprint or biometrics to continue.

15. Click **Next** on your computer.



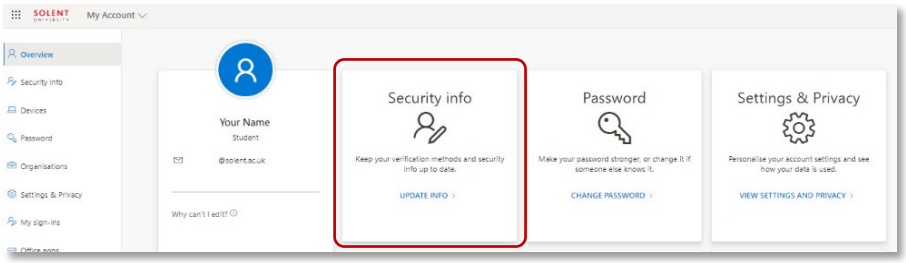
16. The MFA app is now set up. However, it is important to add alternative security information to help sign in and recover your accounts if required.



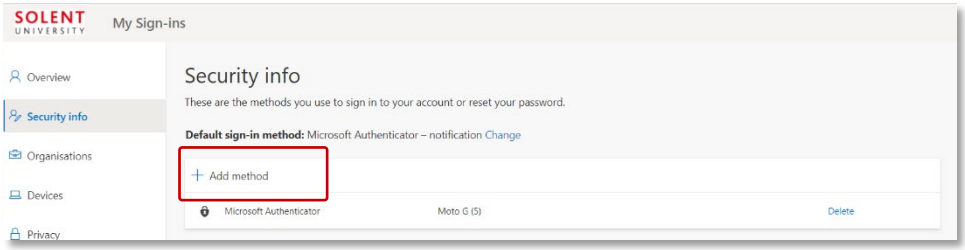
Adding your alternative security information.

This is an important step!
You can install the authenticator app on up to 5 devices and you can add a couple of telephone numbers and an email address, which can be used to authenticate who you are, in case the app stops working, or you forget your account password.

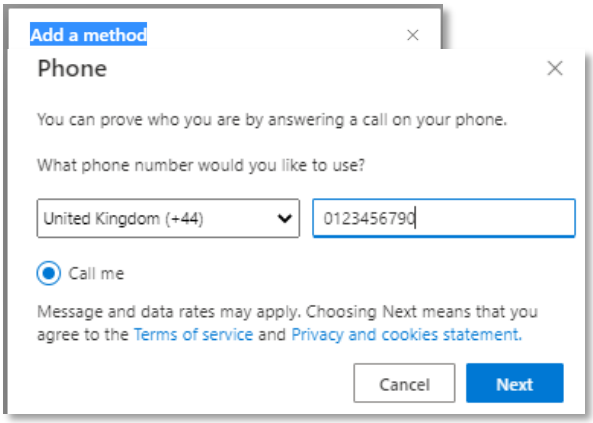
17. Either **click on Security info** or go to https://aka.ms/mysecurityinfo



18. Click + **Add method**



19. Select **Phone**

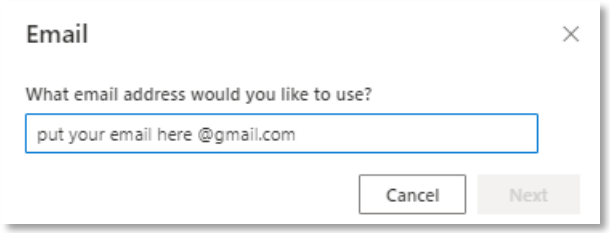


20. Add your mobile number and click **Next**

21. Your phone will ring to verify it, once your answer it **press the #** (hash/pound) to confirm.

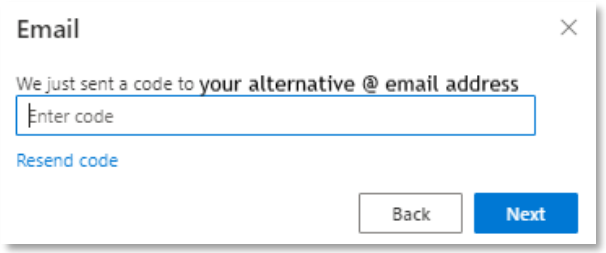
22. Click **Add method** to add an additional alternative phone, this can be a landline or alternative mobile and verify it again.

23. Click **Add method** and select email if you haven't already registered one for password resets.



24. Add an alternative email address (not your university one) and click **Next**

25. Go to that email address and find and copy the verification code, paste it into the box to confirm

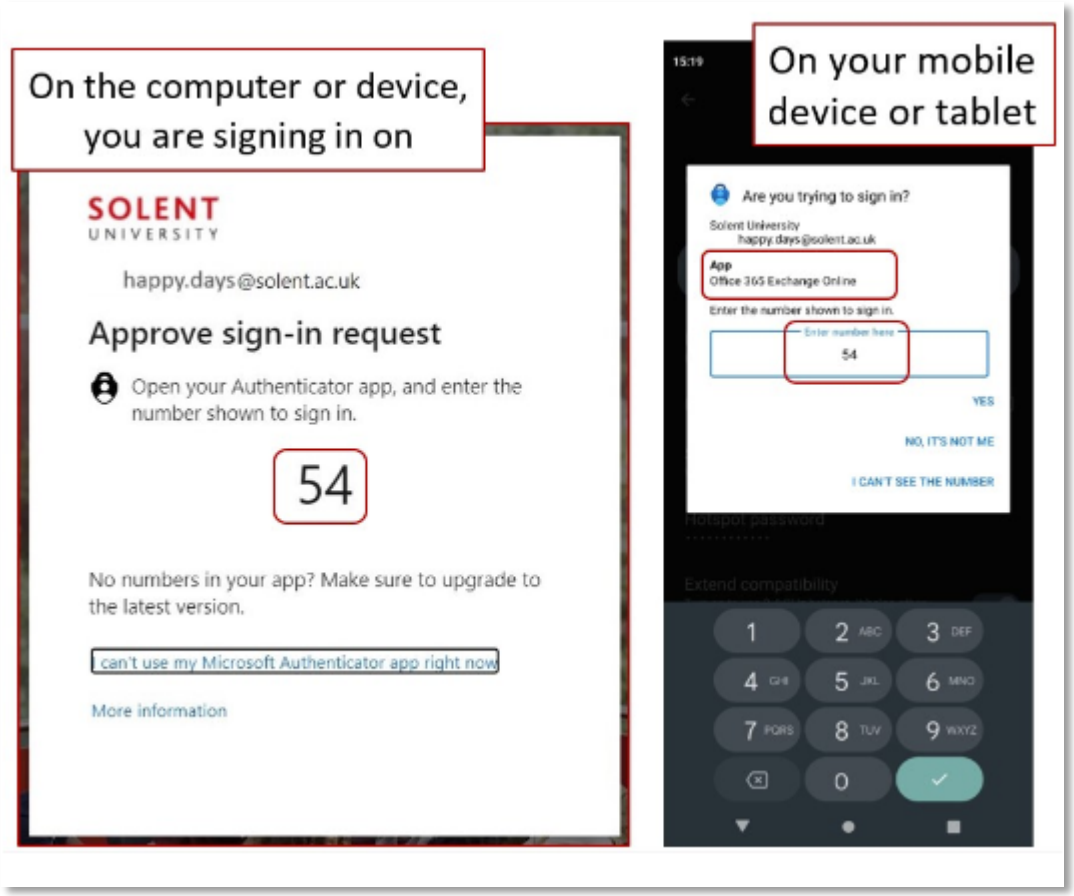


26. Click **Next**

27. **You are now set up**!

Signing in

In future, when trying to sign in, you will be prompted with a notification to approve your sign-in.



If you are using the **Use verification code** configuration, when prompted to **Please enter the verification code from your mobile app,** enter the 6-digit code from the Authenticator app on your mobile device.

Important - If you receive any sign-in approval request on your mobile device without seeing the first **Approve sign-in request** prompt on your computer, you should select **DENY**.

Update your MFA options

You can add multiple ways to MFA by installing the Microsoft Authentication app on multiple phones/devices or by setting up more authentication options.

You can also update your options, to use the recommended app rather than receiving a phone call.

Please note: If you are getting a new phone, set up MFA on your new phone before you get rid of your old phone number or device.

Changing your MFA options

Log in to https://aka.ms/mysecurityinfo with your university credentials on a computer or tablet.

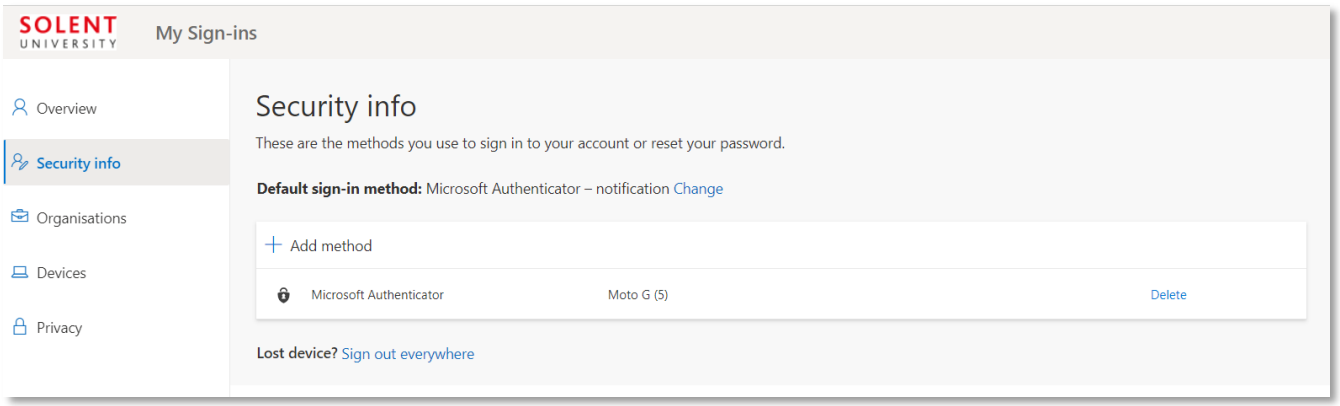
If you are unable to authenticate at all, please contact us for assistance

- For students, please complete our Help form
- For staff, please log a ticket with Unity

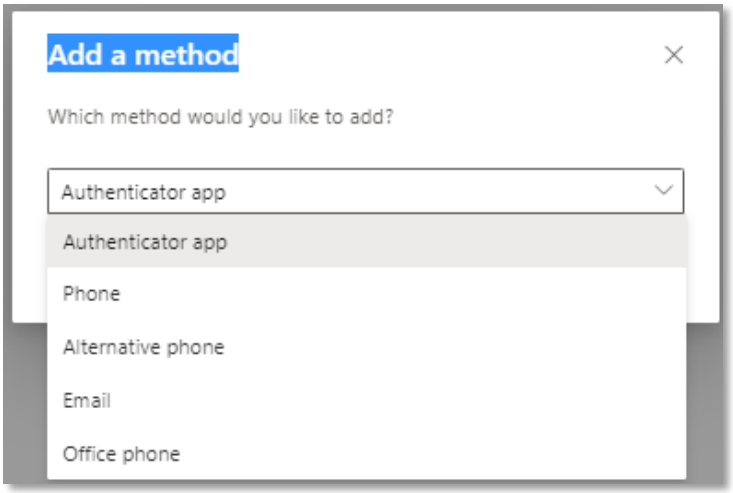
To add a new mobile phone, or additional devices to use the Microsoft Authenticator app.

Watch this video on how to add a new phone (please note: we do not have text method verification).

1. Click + **Add method.**



2. Select **Authenticator app**



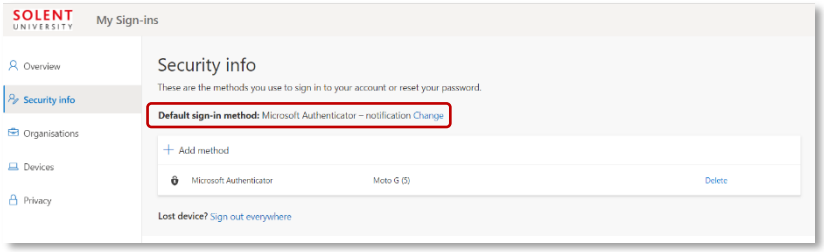
3. Complete steps 3-14 in the **MFA Microsoft Authenticator app set up** above

To add an additional phone call option

1. Click **+ Add method.**

2. Select **Phone** or **Alternative phone** and enter your telephone details
   Following steps 16-20 in the MFA Microsoft Authenticator app set up above

To change the Default sign-in method



1. By **Default sign-in method**: Click **Change**
2. Set to **Microsoft Authenticator – notification**
3. Click **Confirm**

Remember to click **Delete** alongside your existing old telephone numbers, or authentication apps.

If you are on a shared computer, remember to sign out (click on your email address at the top right and click **Sign out**) before leaving.

Having trouble signing in?

If you try to log in but and you don't have your preferred device available, or you don't have signal or internet connection, depending on your MFA preferences, you can select:

- **I can't use my Microsoft Authenticator app right now**
- or **Having trouble sign in another way**

Then choose another method to authenticate depending on what you have set up.

No signal or internet connection?

If your phone lacks a signal, internet connection or you are abroad, and you have the app installed select **Use a verification code from my mobile app.**

- Open the **Microsoft Authenticator app** on your phone select the account you are trying to access
- Make a note of the One-time password code
  Please note: the authenticator app generates a new code every 30 seconds.
- Enter this into your computer when prompted to sign in.

If you are unable to authenticate at all, please contact us for assistance:

- For students, please complete our Help form
- For staff, please log a ticket with Unity