

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, however you can [edit your MFA preferences at any time](#).

Your MFA settings – [Set it up now](#)

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

Editing your MFA settings and options – [Edit 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

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

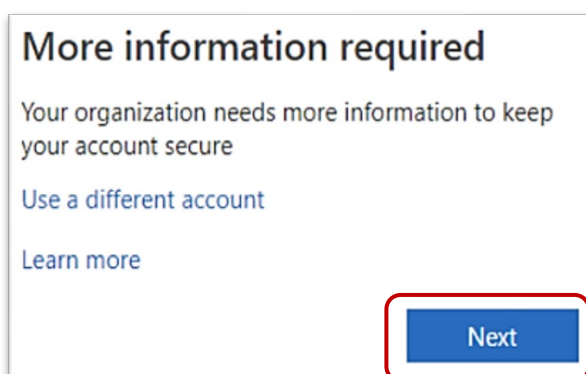
- Please watch [this video](#) for an overview.

The app should work on most Android and iOS handsets. Some older devices may not be able to use the app, if this is the case you set up: Authentication phone when registering.

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.

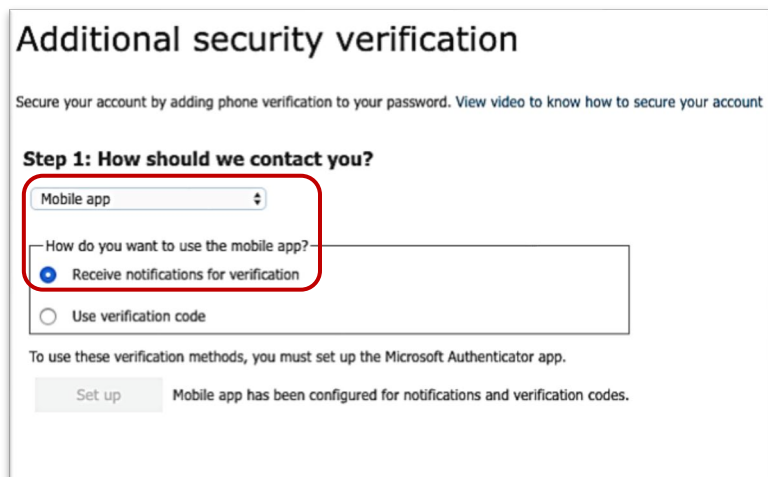
Setting up and using the Microsoft Authenticator App

1. When you sign in on your computer you will be prompted to provide more information or alternatively [click this link to start the process](#).



2. Click **Next**

3. On the next page, select **Mobile app** as the method of contact from the drop-down



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

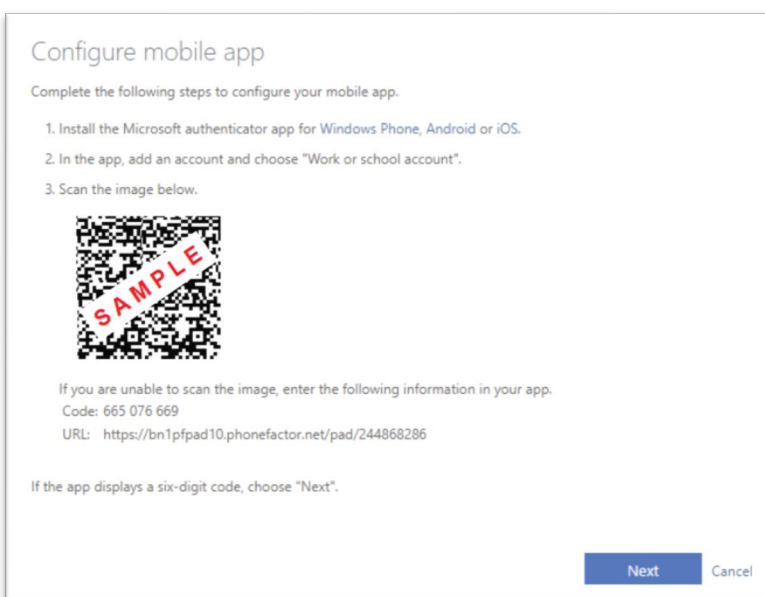
Mobile app has been configured for notifications and verification codes.

4. Select **Receive notifications for verification** to respond to a notification prompt on your device.

Or

Select **Use verification code** to enter a 6-digit code from the app for additional authentication at each logon ([this video](#) will show you how this works).


5. Click **Set up**
6. You will be presented with a screen which includes a QR code. Leave this window open whilst you do the next steps.



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.



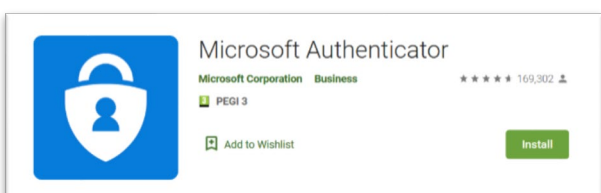
If you are unable to scan the image, enter the following information in your app.
Code: 665 076 669
URL: <https://bn1pfpad10.phonefactor.net/pad/244868286>

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

Next Cancel

7. On your mobile device, **install the Microsoft Authenticator app**.

Available from [Google Play](#), the [Apple App Store](#), or the [Microsoft App Store](#).



8. Once installed, **launch the app** and skip through the wizard if required.
9. Tap on **Add account (the + sign)**.
10. Select **Work or school account** and accept the app permissions.

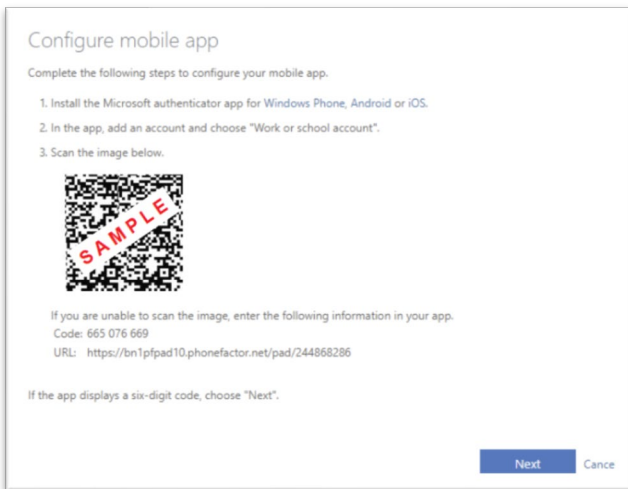
11. Use your device to **scan the QR code** displayed on your computer.

or

If you are doing the whole process on your phone switch to the configure mobile app page and **note down the 9-digit code and the URL** and enter it manually into the set up.

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.



12. Switch back to your computer and Select **Next**.

13. Wait for **Checking activation status** to complete.

Please Note: if configuration fails, delete the account and retry the previous steps again.

14. Select **Next** to continue.

15. On your mobile device, go to the Microsoft Authenticator app and tap **Approve** on the sign-in prompt.

16. Back on your computer, check the **Authentication phone** box and add a suitable number. If you have a second phone or an international number add it by checking the **Additional authentication phone** box and adding the number.

17. **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 **Receive notifications for verification** configuration, click on the notification on your mobile device and click **APPROVE**.

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**.

Editing your MFA options

Ok you have MFA set up and you want to change how you authenticate?

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 have got a new phone you will need to set up your new phone before you get rid of your old phone number or device.

If you are going to switch to the app or add a new phone/device, make sure you **install the Microsoft Authenticator app** first on your phone/device.

- Available from [Google Play](#), the [Apple App Store](#), or the [Microsoft App Store](#).

Changing your MFA options

Log in to [MFA - Additional security verification options page](#) with your university credentials on a computer or tablet

If you are unable to authenticate, please do the following:

- For students, please email: LTU@solent.ac.uk
- For staff, please log a ticket with [unity](#)

To start using the Microsoft Authenticator app rather than a phone call:

- Change the option under 'what's your preferred option' to **Notify me through app**.
- Then add your device as below if required.

To add a new or additional phone/device to the app:

- Click **Set up Authenticator app**.
- Follow the instructions on configure mobile app pop up.
(If you are doing the whole process on your phone you can switch to the configure mobile app page and **note down the 9-digit code and the URL** and enter it manually into the set up rather than scanning the QR code)
- Click **Next** and then on your phone tap **Approve** on the sign-in prompt.

To delete a device, click **Delete** next to the device you wish to remove.

To add an additional phone to your phone call authentication option

- Click on the Alternative authentication phone checkbox
- Select your country or region
- Enter your telephone number

When you have finished updating your options click **Save** at the bottom

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.

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 United Kingdom (+44) 0777777777 - Your phone number
 Office phone Select your country or region Extension

Alternative authentication phone Select your country or region

Authenticator app or Token Set up Authenticator app

Authenticator app - Moto G (5) Delete

Save Cancel

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

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.

Configure app without notifications

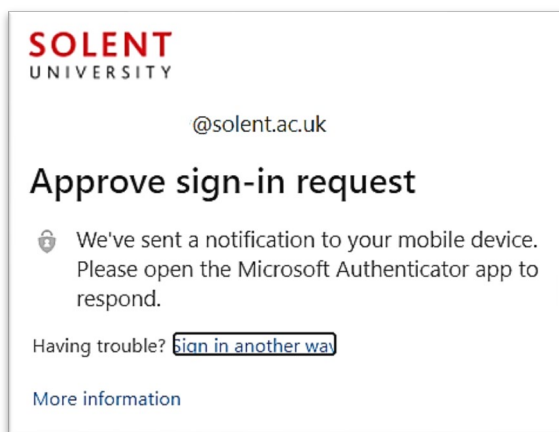
If you are unable to scan the image, enter the following information in your app.
Code: 595 473 500
URL: <https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/872467210>

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

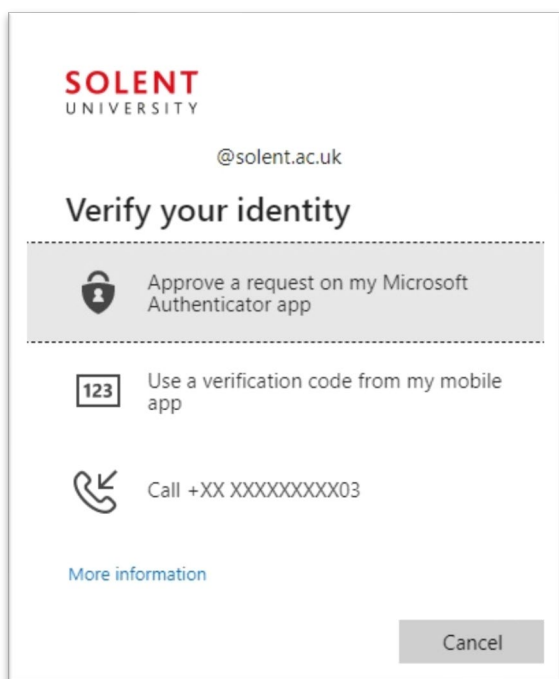
Next Cancel

Having trouble signing in?

If you try to log in but 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 **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
- Enter this into your computer when prompted to sign in.

Please note: the authenticator app generates a new code every 30 seconds.

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

- For students, please email: LTU@solent.ac.uk and supply your:
 - Username
 - Student ID
 - Date of Birth
 - Course name
 - Screenshot of the error
- For staff, please log a ticket with [unity](#)