Multi-factor authentication (MFA)

Helpsheet IT25a

Multi-factor authentication (MFA) provides an additional layer of security for your university account, ensuring secure access to online resources such as Canvas VLE and Office 365 (email, OneDrive, Teams). Even if an attacker manages to access your password (e.g. via a successful phishing attack) it is useless to them without also knowing the additional authentication method you have set up.

The University recommends and supports the 'Microsoft Multi-Factor Authentication' system.

Once the signup process is complete, you will start to see prompts when you are logging into university applications.

- Applications such as Outlook, Teams or OneDrive on your university PC will require you to authenticate the first time after setup, but not every time.
- Access to services via a web browser, such as Webmail or SharePoint Online will prompt you regularly and you will always be prompted on a computer you are using for the first time.
- You will never be prompted for multi-factor authentication during normal login to your computer.

Once configured, if you receive an authentication prompt when you have not attempted to access or log-in to a service, this indicates that someone else is trying to access your account. **Do not** accept the request and contact the IT Service Desk immediately.

Before you begin

Download this document before attempting the steps. While unlikely, in case you lose connection during the setup process, troubleshooting guidance is provided on the last page. You will also find answers to common problems in our Q&A document on the MFA webpage.

To avoid issues during the setup process:

- Disable any VPN connections you have running; and
- Configure your web browser to allow pop-up windows and enable cookies. You will find information for specific browsers online.

We recommend and support the Microsoft Authenticator app for MFA as the verification method it provides offers the best flexibility. The app is completely self-contained and does NOT have access to other information on your mobile phone, including any of your personal apps, photos, or other personal details.

If you wish to use SMS text messages or voice calls instead or have a device that cannot run the Microsoft Authenticator app, see Alternate method to authenticate.

Authenticating using the Microsoft Authenticator app

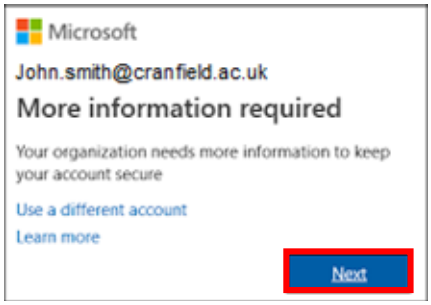
To setup the authenticator app, ensure you have a computer and a smartphone with you, you will need both to complete the setup process.

1. On your smartphone

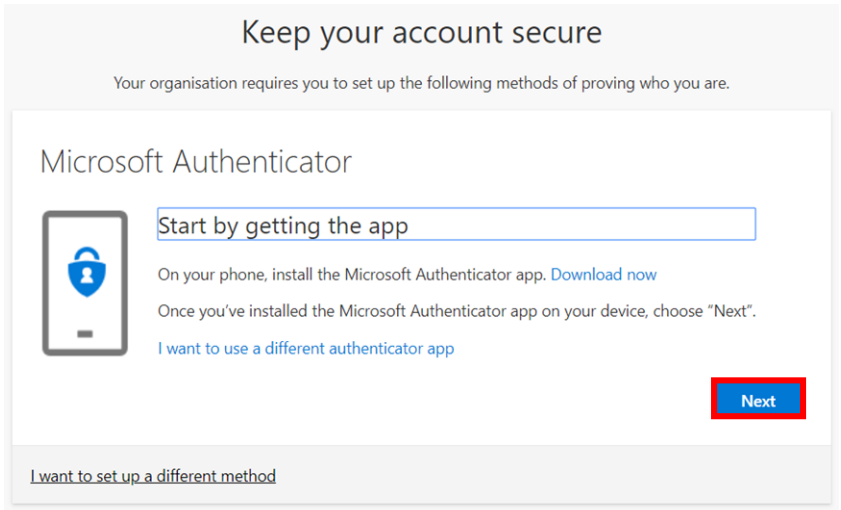
Download and install the **Microsoft Authenticator** app from your device's app store.

2. On your computer

After signing into various university online resources, you will see '**More information required**', click **Next** to view the multi-factor authentication setup screen – alternatively, from your PC, laptop or tablet, open a browser and go to https://aka.ms/MFAsetup.



Click **Next** on the Microsoft Authenticator setup page until you see a QR code displayed on your computer screen.



3. On your smartphone

Open the Microsoft Authenticator app on your smartphone and follow these steps:

1. Ensure you **allow notifications** and **skip** any offers to add home/other accounts until you are prompted to add a '**Work/School Account**';
2. If prompted, **allow the app to use your camera/take pictures and record video** (this enables the app to capture the QR code on your computer screen).

If you already use the Microsoft Authenticator app for your other online accounts:

- Open the MS Authenticator app;
- Tap the **3-dots menu** icon in the app and select **Add account**;
- Tap **Work or school account** and then tap **Scan a QR code**;
- Continue to follow the steps below.

4. On your computer

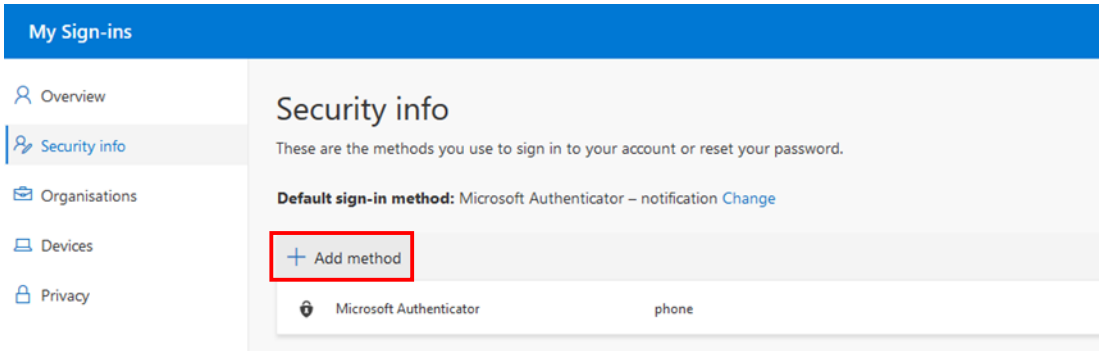
If you do not see a QR code on your computer screen, continue to click **Next** until displayed, then follow these steps:

1. Scan the QR code using your smartphone;
2. On your computer, click **Next**;
3. Approve the authentication request when it appears on your smartphone screen;
4. Once complete, click **Next**;
5. You have now registered your primary MFA method, click **Done** and you will be returned to the **Security info** page (continue below).

Create a secondary MFA method

To protect against issues with your authenticator app, we **strongly recommend** setting up a secondary method of authentication. You can do so from the **Security Info** page which will now be displayed on your computer screen (https://mysignins.microsoft.com/security-info).

1. Click **Add method**;



2. Select **Phone** from the drop-down list and click **Add**;
3. Select the appropriate country code and enter your mobile phone number;
4. Select **Text me a code**, then click **Next**;
5. A text message will be sent to your mobile phone with a six-digit code; input the code into the **Enter Code** box on your computer screen, then click **Next**;
6. Click **Done**.

Within 24 hours of completing the process:

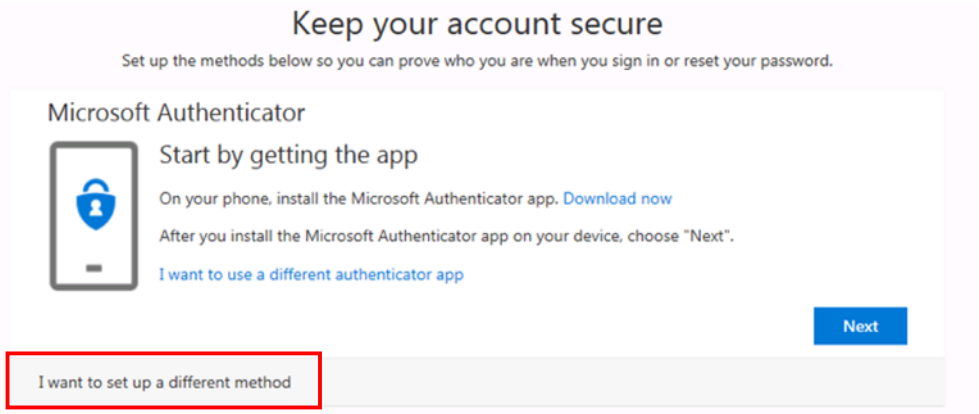
- you will start to see authentication prompts when logging into Microsoft web applications (e.g. Office 365);
- you will be prompted once for each installed Office application such as Outlook, Teams, etc.

Alternate method to authenticate

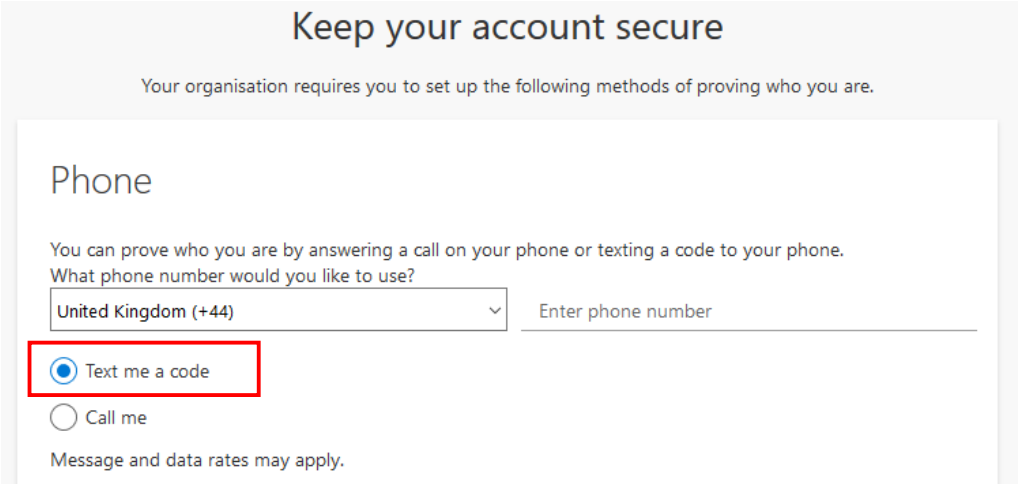
SMS text messages

Follow this guidance only if you wish to use SMS text messages instead of using the authenticator app.

1. Go to the MFA setup website: https://aka.ms/MFAsetup and sign in with your university email address and password;
2. When prompted for more information, click **Next**;
3. In the Microsoft Authenticator setup screen, click **I want to set up a different method**;



4. Select **Phone** from the '**Choose a different method**' drop-down list;
5. Click **Add**, then select your country and enter your mobile phone number;
6. Select **Text me a code**, then click **Next**;



7. A text message will be sent to your mobile phone with a six-digit code. Type the code into the **Enter Code** box on your computer screen and click **Next**;
8. Click **Done**.

Authenticate by voice call

You can also select 'Call me' in the Phone option above and then enter a landline such as your office number and home number. Using this method, you will receive an automated voice call asking you to confirm your log in.

Only use the landline method if you do not have a mobile phone.

Amending authentication information

To make changes to your authentication methods, log in to office.com, click your profile picture or initials in the top right corner and select **View account** > **Security info**.

Troubleshooting

- If you can't scan the QR code on your device, click **Can't scan image?** located below the QR code on your computer screen. This will display a numeric code and URL for you to enter manually into the authenticator app on your smart device.

- If you receive an error scanning the QR code, record the error message and then use the method detailed in Alternate method to authenticate to set up SMS verification instead. Contact the Service Desk with details of the error message and your device type.

- If you experience a problem setting up the authenticator app, uninstall it from your smart device and re-install from your app store.

- If your internet browser gets caught in an authentication loop, either:
    - close all browsers on your computer and start a fresh session by going to https://aka.ms/MFAsetup; or
    - open a private browser window and visit https://aka.ms/MFAsetup.

Contacting us

For further information or assistance using Multi-factor Authentication please contact us.

IT Service Desk
http://servicedesk.cranfield.ac.uk
servicedesk@cranfield.ac.uk
+44 (0)1234 75 4199

Our skilled support staff are available to help Monday - Friday: 8 AM – 6 PM

Updated Aug-2021