Multi-factor authentication (MFA)

Helpsheet IT25

Multi-factor authentication (MFA) provides an additional layer of security for your Cranfield user account, ensuring secure access to online resources such Office 365 (email, OneDrive, etc.) and Agresso. Even if an attacker manages to find out your password (e.g. via a successful phishing attack) it is useless to them without also knowing the additional authentication method that you have configured.

Cranfield uses the 'Microsoft Multi-Factor Authentication' system.

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

- Applications such as Outlook, Teams or OneDrive on your Cranfield PC will require you to authenticate the first time after setup, but not every time.
- Access to services via a web browser, such as Agresso, Webmail or SharePoint Online will prompt you regularly on your work computer 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 the normal login to your computer.

Once configured, if you receive an authentication prompt for a log-in attempt that you did not initiate, this is a sign that someone else is trying to access to 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 MFA questions and answers document.

To avoid issues during the setup process:

- Disable any VPN connections you have running;
- Configure your web browser to allow pop-up windows and enable cookies.

You are required to configure two methods of authentication. Microsoft Authenticator is the supported app for MFA at Cranfield and is recommended as the verification method, it provides 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.

The overhead on your data plan is very low and, in most cases, where you are trying to access your university account you will have access to Wi-Fi with no data impact. The app can also be used to provide authentication in locations where you do not have a phone signal as it continuously generates secure passcodes.

- If you already have another authenticator app on your smartphone, from the MFA setup screen on your computer, click '**I want to use a different authenticator app**', open the preferred app on your smartphone and scan the QR code displayed.
- If you wish to use SMS text messages or voice calls, or you have a device that cannot run the Microsoft authenticator app, click '**I want to set up a different method**' (see below for details).

Whichever methods you choose, you will have the option to select any of your other pre-configured authentication methods when you sign into your Cranfield account.

Authenticating using the MS Authenticator app

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

If you have previously set up a device for MFA, and are attempting to configure a new one, you will need to contact the Service Desk to remove your old device before continuing with this process.

Within 24 hours of completing the process:

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

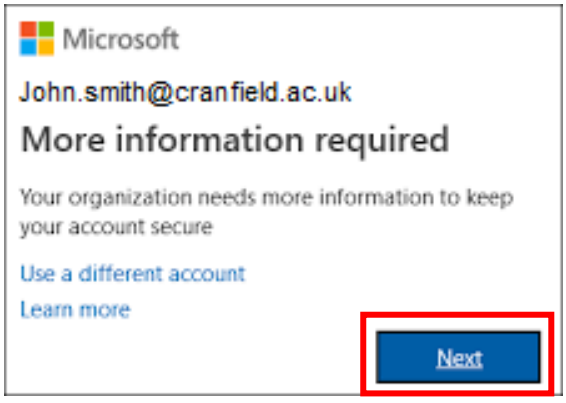
If you already have the Microsoft Authenticator app on your smartphone, skip step 1 below.

1. On your smartphone

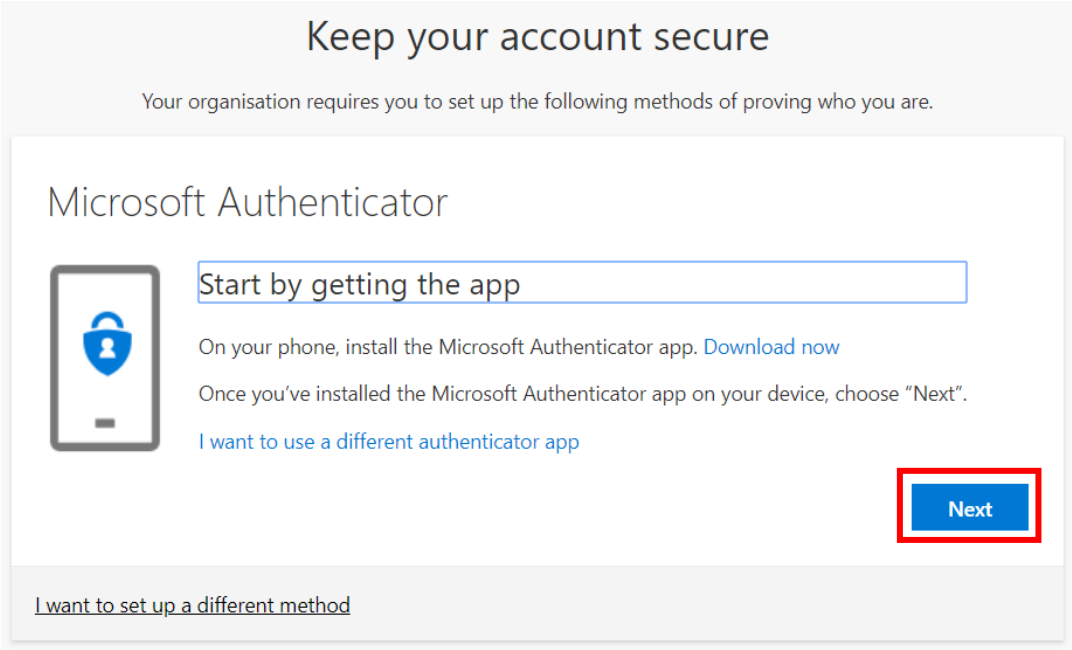
Download and install the **Microsoft Authenticator** app from your device's app store.

2. On your computer

When signing into various university online resources, you will see '**More information required'**, click **Next** to view the multi-factor authentication setup screen.



You will see the Microsoft Authenticator setup screen.



Continue to click **Next** 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 referenced above).

If you have previously configured the Microsoft Authenticator app for another account:

- 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

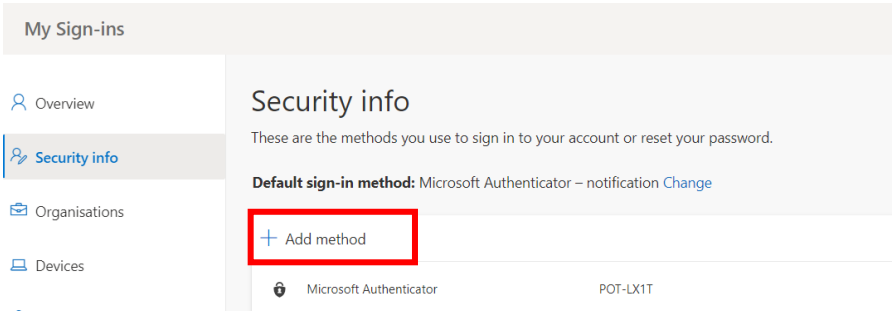
If, you do not see a QR code on your computer screen, click **Next** until one appears and follow these steps:

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** – you will be re-directed to the Cranfield account **Security info** page.

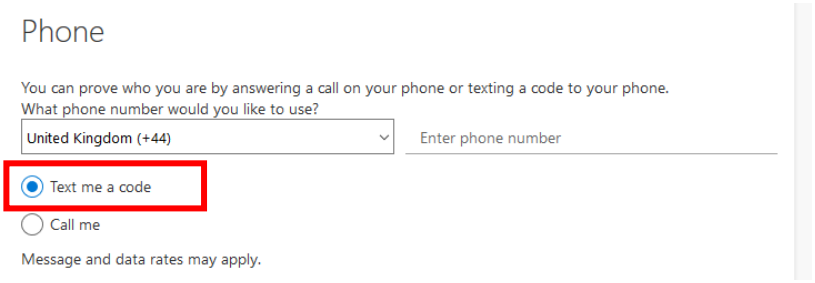
5. Set up a secondary authentication method

Still on your computer, from the Cranfield account **Security info** page follow these steps:

1. Click **Add method**.



2. Select **Phone** from the drop-down list and click **Add**.
3. Select an 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. Type the code into the **Enter Code** box on your computer screen, then click **Next**, and click **Done**.

Voice calls

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

Do NOT enter a Teams voice call number for this step.

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

Troubleshooting

- If you are unable to scan the QR code on your device, click '**Can't scan image?**' 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 smartphone.

- If you receive an error scanning the QR code, record the error message and set up SMS verification instead. Notify the Service Desk detailing 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 in that instead.

- To change an authentication method, log in to www.office.com/ click your profile picture or initials in the top right corner and select **My account** > **Security & privacy** > **Additional security verification** > **Update your phone numbers used for account security**.

Contacting us

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

IT Service Desk, Building 63
Self-service: http://servicedesk.cranfield.ac.uk
Email: servicedesk@cranfield.ac.uk
Call: +44 (0)1234 75 4199

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