



Multi-factor authentication (MFA)

Frequently asked questions

Common problems with MFA and your Cranfield account

This document should be read in conjunction with our help sheet [IT25_MFA setup guide](#).

As there are some common problems happening more frequently than any of us would like, we have put together this guide to address the most common problems and some possible fixes.

1. I lost my mobile device or it was stolen

If you have lost or had your mobile device stolen, you can sign in using a different method but you must also contact the IT Service Desk to clear the device from your MFA settings. After your settings are cleared, you will be prompted to register for two-factor verification when you next sign in.

2. I don't have my mobile device with me

We don't all always have a mobile device to hand. If you previously added another method to sign into your account, such as your office phone, you should be able to use that method. If you didn't previously set up an additional verification method, you will have to contact the IT Service Desk who will help you get back into your account.

To sign into your Cranfield account using alternative verification method:

1. Sign into your account, selecting the link **Sign in another way**.
2. Choose your alternative verification method and continue with the two-factor verification process.

Note: If you don't see the 'Sign in another way' link, it means that you haven't set up any other verification methods. Contact the IT Service Desk for help.

A screenshot of a Microsoft authentication page. At the top is the Microsoft logo and the email address 'kelly@contoso.com'. Below that is the heading 'Enter code'. A message says 'We texted your phone +X XXXXXXXX21. Please enter the code to sign in.' There is a text input field labeled 'Code'. Below the input field is a checkbox labeled 'Don't ask again for 60 days'. At the bottom left, there is a link 'Having trouble? Sign in another way' which is highlighted with a red box. Below that is a link 'More information'. At the bottom right is a blue button labeled 'Verify'.

3. I'm not getting prompted for my second verification information

You will only occasionally be prompted for your second verification information. One easy way to verify that MFA has been correctly set up is to access your University email (office.com) from a fresh In Private/Incognito browser session – this will always prompt for your verification.

If you have signed into your Cranfield account using your user name and password, but haven't been prompted about your additional security verification information, maybe you have yet to set up your device.

Your mobile device must be set up to work with your specific additional security verification method. To check which verification methods you have configured, see the [Manage your two-factor verification method settings](#) article.

If you know you haven't set up your device or your account, you can do it now by following the steps in help sheet [IT25 MFA setup guide](#).

4. I'm not getting the verification code sent to my mobile device

Not getting your verification prompt is a common problem typically related to your mobile device and its settings. Some possible things to try:

Try this	Guidance info
Restart your mobile device	Restarting your device ends any background processes or services that are currently running and could cause problems, along with refreshing your device's core components, restarting them in case they crashed at some point.
Verify your security information is correct	Make sure your security verification method information is accurate, especially your phone numbers. If you enter the wrong phone number, your alerts will go to that incorrect number. Fortunately, that user won't be able to do anything with the alerts. To make sure your information is correct, see the instructions in the Manage your two-factor verification method settings article.
Verify your notifications are turned on	Make sure your mobile device has notifications turned on and that you've selected a notification method that allows phone calls, your authentication app, and your messaging app (for text messages) to send visible alert notifications to your mobile device.
Make sure you have a device signal and Internet connection	Make sure your phone calls and text messages are getting through to your mobile device. Ask a friend or colleague to call and text you to make sure you receive both. If you don't, first make sure your mobile device is turned on. If your device is on, but you're not receiving calls or texts, it's most likely a problem with your network and you'll need to talk to your provider. If you often have signal-related problems, we recommend you install and use the 'Microsoft Authenticator app' on your mobile device. The authenticator app can generate random security codes for sign-in, without requiring any network connection.
Turn off 'Do not disturb'	If you have turned on 'Do not disturb' for your mobile device, notifications won't appear. Refer to the device manual for instructions about how to turn off this feature.

Try this	Guidance info
Check your battery-related settings	If you've set up battery optimization to stop lesser-used apps from remaining active in the background, your notification system has most-likely been affected. To try to fix this problem, turn off battery optimization for your authentication app and your messaging app, and then try signing in to your account again.
Disable third-party security apps	If you have an app that protects text messages or phone calls to minimize unknown callers, it may prevent the verification code being received. Try disabling any third-party security apps on your phone, then request another verification code.

5. I want to add a new phone number

If you have a new phone number, you'll need to update your security verification method details to receive notification. To do update your verification method, follow the steps in the **Add or change your phone number** section of the [Manage your two-factor verification method settings](#) article.

6. I want to add a new mobile device

If you have a new mobile device, you'll need to set it up to work with two-factor verification.

1. Set up your device following the steps in help sheet [IT25 MFA setup guide](#).
2. Update your account and device information in the **Additional security verification** page, deleting your old device and adding your new one. For more information, see the [Manage your two-factor verification method settings](#) article.

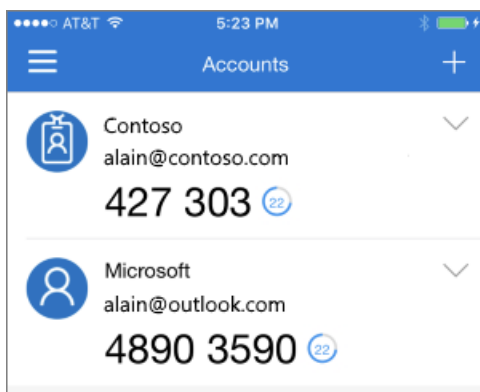
Optional steps:

- Download, install, and set up the Microsoft Authenticator app on your mobile device by following the steps in the [Download and install the Microsoft Authenticator app](#) article.
- Turn on two-factor verification for your trusted devices by following the steps in the **Turn on two-factor verification prompts on a trusted device** section of the [Manage your two-factor verification method settings](#) article.

7. I'm having problems signing in on my mobile device while travelling

In an international location, you might find it more difficult to use a mobile device verification method such as text messaging. Using a mobile device may also incur roaming charges. For this situation, we recommend you use the **Microsoft Authenticator app**, with the one-time passcode option.

When you open the Authenticator app, you will see your added account(s) as tiles. Clicking the account will show a one-time passcode you can use for your MFA login.



8. I can't turn two-factor verification off

Once you have correctly set up using two-factor verification with your Cranfield account, you must use this added security feature. You cannot remove this feature from your account.

Contacting us

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

IT Service Desk, Building 63

📞 +44 (0)1234 75 4199

✉ servicedesk@cranfield.ac.uk

👉 <http://servicedesk.cranfield.ac.uk>

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