

Multi-factor Authentication Guide

Introduction

Multi-factor authentication (MFA) is a technology to secure systems and data with more than just a password; using phone calls, SMS text messages or mobile authenticator apps to provide an additional layer of security.

Staffordshire University's implementation of security uses a risk-based approach, where most logons do not require any additional authentication steps; however, if accessing your account from an unusual device or location, then MFA may be required, and users who have not registered for MFA may find that their access is blocked.

Analysis of dozens of ransomware attacks that have resulted in the complete loss of IT at UK universities and colleges has identified deployment of MFA for all users as a key safeguard. MFA is an excellent preventative measure estimated to block around 99.9% of cyber-attacks, and it's a quick and easy process for users to install. It helps to create a safe, secure learning and working environment for everyone at the University.

To protect your account, the University now require that you register additional multi-factor authentication details for your account. Where registration is required a setup wizard will be included as part of the web logon process.

To register or update your MFA details, please visit <https://www.staffs.ac.uk/mysecurityinfo>. We recommend that you register the Authenticator app as your primary authentication method as this is more secure, however it is advisable to also register a phone number as one of your additional MFA options.

[Frequently asked questions](#) regarding Staffordshire University's MFA implementation can be found at the end of this document, but if you have any other questions, please contact Digital Services' support desk at 3800@staffs.ac.uk.

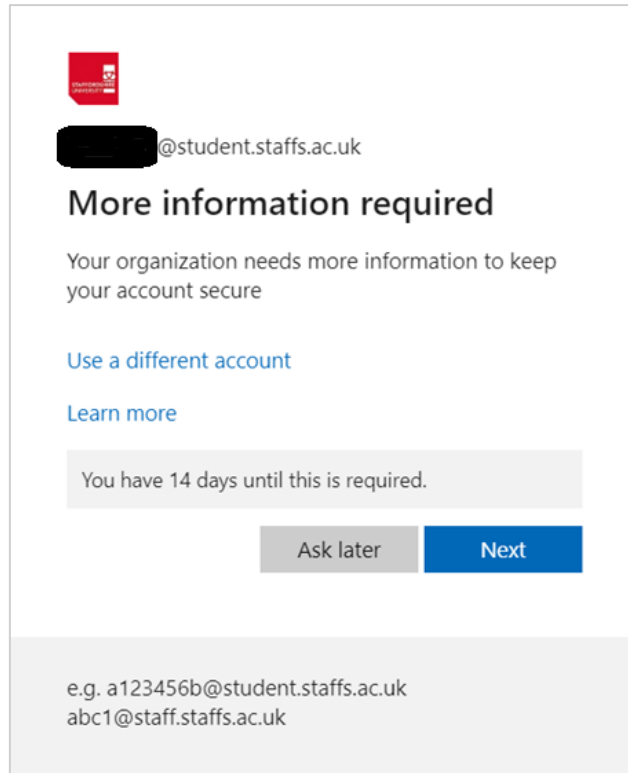
Many external systems, such as Facebook, Google, Snapchat, Instagram and Microsoft, have their own implementation of MFA (sometimes called 2FA) to protect their users' data. It is recommended you enable MFA for any of these services you use for additional protection.

Contents

Introduction	1
1. Multi-factor Authentication Registration Wizard	2
2. Registering the Authenticator App.....	3
3. Registering a Phone.....	4
4. Manually Registering for Multi-factor Authentication and Reviewing Settings.....	5
5. Further Information	6
6. Multi-factor Authentication FAQ	7

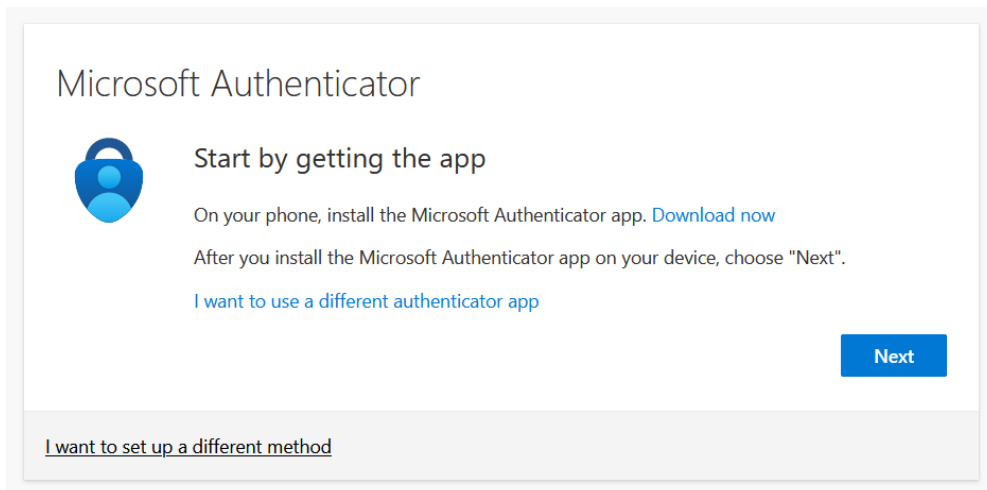
1. Multi-factor Authentication Registration Wizard

For users who are required to register for multi-factor authentication, but have not previously opted into this protection, the next time you access one of the protected University systems (Outlook, OneDrive, Office 365, etc.), you will be prompted to provide more information.



You can skip the registration process for up to 14 days, after which you must register to gain access to protected systems:

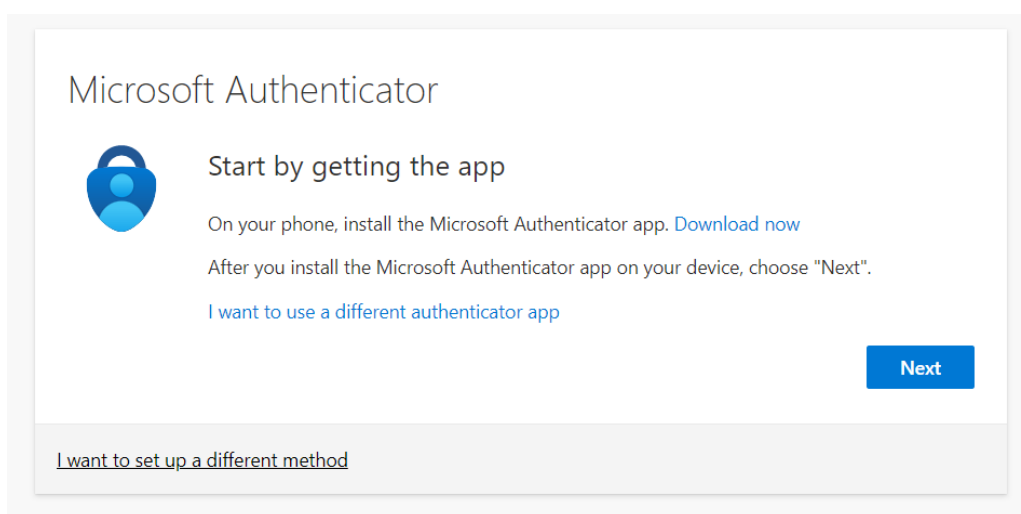
If you click "next" you will be prompted to register the Authenticator application - see section 2 for instructions. If you click 'I want to set up a different method' you will be given the option to register your phone – see section 3 for instructions regarding that.



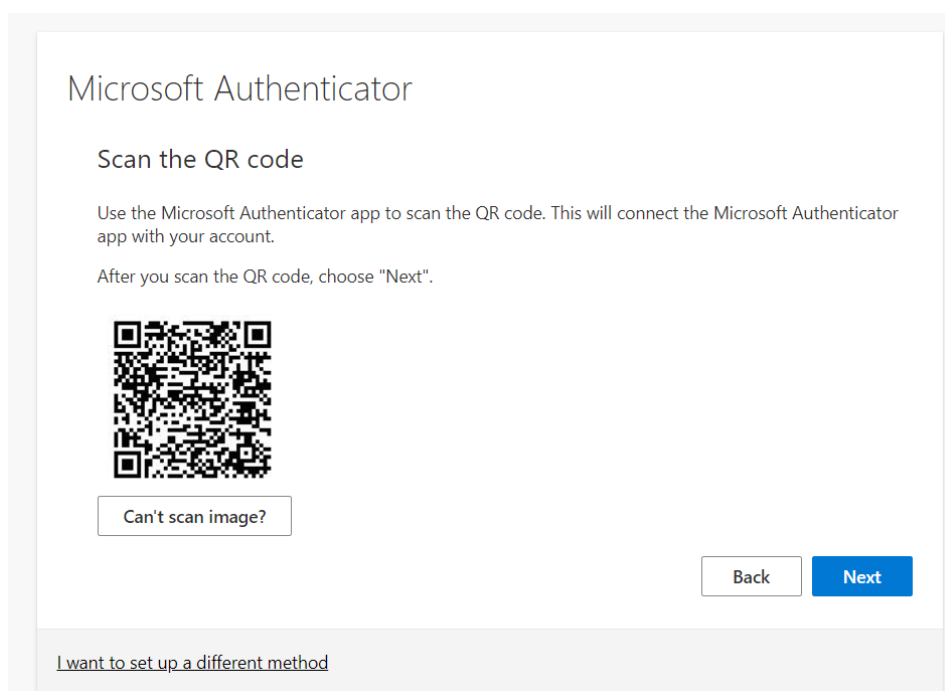
2. Registering the Authenticator App

1. Select the **Authenticator app** option
2. A "Start by getting the app" wizard will appear. Install the Microsoft Authenticator app on your device. If you wish to use an alternative authenticator you can do this** by clicking "I want to use a different authenticator app" and following the instructions provided by that application. The following guide will focus on the Microsoft Authenticator process:

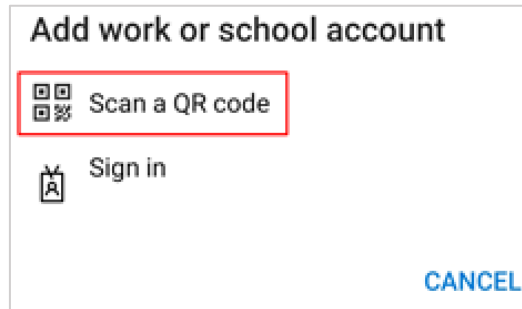
** *this option is currently available to students only, not staff members*



3. After you install the Microsoft Authenticator app you may be asked if you wish to allow notifications – please consent to this.
4. Select "Next" on screen until you arrive on a page with a QR code which will appear on screen as shown below:



5. In the Authenticator app, add a new account by pressing the '+' icon at the top and then select "Work or school account", then select the option which states 'Scan a QR code'

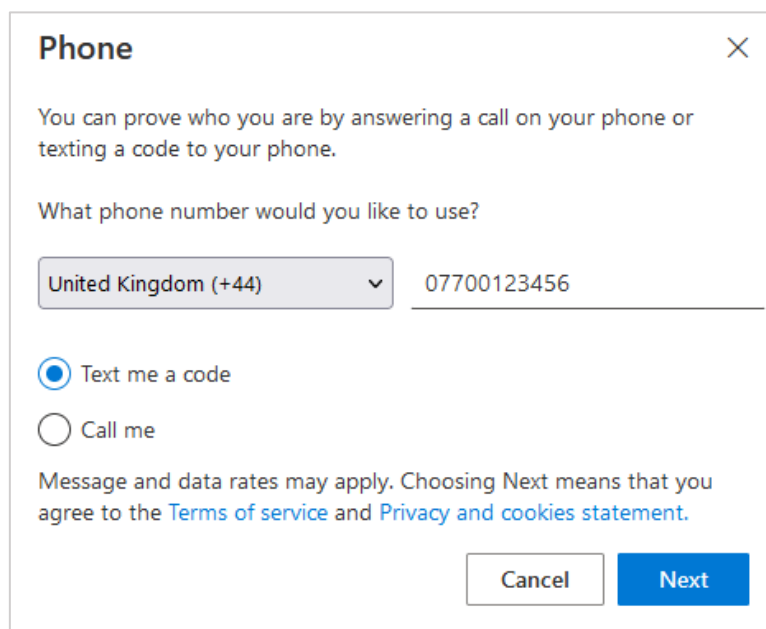


6. Hold your phone up and scan the QR code on screen. If you are unable to do this, you can select the "Can't scan image?" link and manually enter the code and URL into the Microsoft Authenticator app
7. Use the Microsoft Authenticator app to approve the notification to activate the app.

After registration, you can change your multi-factor authentication details at any time from this link: <https://www.staffs.ac.uk/mysecurityinfo> - see Section 4 for more information.

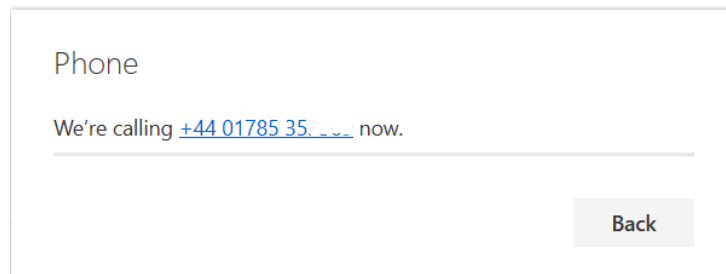
3. Registering a Phone

1. Select the **Phone** option
2. A "Set up your phone" wizard will appear:



3. Pick your **Country or Region** from the drop-down box, type your phone number (including area code, if applicable) into the **Phone Number** box, select either the **Call me or Text me a code** option (dependent on your preference), then select **Next**.

You will receive an automated phone call to make sure you typed in the correct phone number. At that time, you'll be asked to push the hash (#) key to confirm and to complete your set up. If you selected the 'Text me a code' option, you will be asked to confirm the code which was sent.

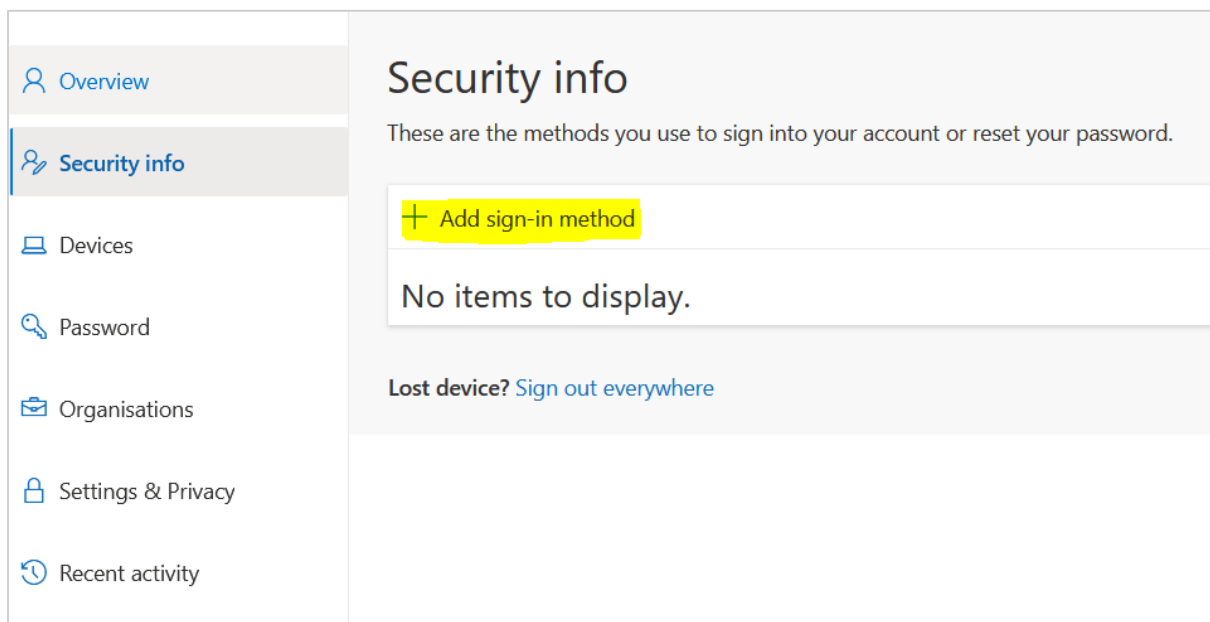


After registration, you can change your multi-factor authentication details at any time from this link: <https://www.staffs.ac.uk/mysecurityinfo> - see section 4 for more information.

4. Manually Registering for Multi-factor Authentication and Reviewing Settings

Users can visit the Multi-factor authentication pages at <https://www.staffs.ac.uk/mysecurityinfo> (or <https://aka.ms/MFASetup>) to register their account for multi-factor authentication (MFA), and change the authentication methods.

In the "Security Info" page, click "+ Add sign-in method" to start the registration process, and choose 'Authenticator app' or 'Phone' in order to proceed. If you choose "Phone", it will allow you to use a phone call or SMS text message for verification. You can also choose 'Alternative Phone' and register a second device. See Section 2 for Authenticator app registration, and section 3 for phone registration. If you need to remove obsolete authentication methods you can do so in this portal.



As people tend to keep a phone number longer than an app, it is always recommended that you also register your phone number, but use the Authenticator app as your primary method.

5. Further Information

Details on setting up the Authenticator app are available online at:

<https://docs.microsoft.com/en-gb/azure/active-directory/user-help/security-info-setup-auth-app>

Details on setting up multi-factor authentication through a phone are available online at:

<https://docs.microsoft.com/en-gb/azure/active-directory/user-help/security-info-setup-phone-number>

It is recommended that you review your MFA details periodically through the setup page:

<https://www.staffs.ac.uk/mysecurityinfo>

6. Multi-factor Authentication FAQ

What is multi-factor authentication (MFA)?

Multi-factor authentication (MFA) is the use of additional verification steps beyond a standard password to prove your identity as part of the log on process. MFA may include a phone call to a registered number, an SMS text message or a code generated by a mobile app as an additional verification step.

The University MFA implementation uses a risk-based approach, so that there will only be an additional verification challenge when accessing your account from an unusual location or unusual device, and University managed devices are always deemed secure regardless of their location.

Why do we need multi-factor authentication?

MFA is an essential defensive tool which helps to keep the university safe for all members of staff and students. It offers an additional level of protection to safeguard your account and data.

Analysis of ransom-ware attacks on UK Colleges and Universities has identified that deployment of MFA is one of the most beneficial actions that an organisation can take to protect itself similar attacks in the future.

I don't have a smart phone, how can I register for MFA

MFA does not require use of a smart phone, you can use any phone, including a landline number to register for multi-factor authentication. Students also have the option to use a FIDO security key, however this option is not currently available for staff members.

How does MFA protect me?

MFA provides an additional line of defence for our protected systems and data. Should your password be compromised by a malicious third party, they will be prevented from accessing protected resources without access to your phone.

How do I get MFA for my University account?

You can register at any time for Multi-factor authentication by signing up at <https://www.staffs.ac.uk/mysecurityinfo>. Once you have successfully registered a phone number or authenticator app, the University systems will enable protection for your account within 15 minutes and send you a welcome email.

How can I change my MFA details?

To add or update your multi-factor authentication details, please visit <https://www.staffs.ac.uk/mysecurityinfo>.

As people tend to keep a phone number longer than an app, it is always recommended that you register your phone number as your secondary authentication method. You can register more than one phone number as well as an app from the multi-factor authentication site at <https://www.staffs.ac.uk/mysecurityinfo>. If you only register an authenticator app, then you will receive email reminders to add a phone number to your Multi-factor authentication settings.

Which is the preferred MFA method?

If you have a smartphone, then use of the authenticator app is the simplest and most secure method for MFA, so this is our recommendation. However, as people tend to keep a phone number longer than an individual smart phone, it is always recommended that you

register a phone number also to ensure that you can maintain access when you come to replace your smartphone.

You can register multiple numbers as well as an app from the multi-factor authentication site at <https://www.staffs.ac.uk/mysecurityinfo>.

Can I use the Microsoft Authenticator app for MFA on multiple devices?

Yes, the Microsoft Authenticator supports multiple devices.

When will I get prompted for MFA?

The University MFA implementation uses a risk-based approach, so that there will only be an additional challenge when accessing from an unusual location or unusual device. All University managed devices are always deemed secure regardless of their location.

I have never been prompted for MFA; is it working?

To simplify the experience for end users, the University MFA implementation is designed to only prompt when there is a high security risk. The University's cybersecurity team have tested the solution to prove that MFA does challenge in these high-risk scenarios. If you wish to test that your MFA information is set up, and that you know what an MFA challenge looks like, please visit the MFA set up page at <https://www.staffs.ac.uk/mysecurityinfo>.

What do I do when I get prompted for MFA?

If the MFA challenge is in response to a log on that you are undertaking then:

For a phone call, press # when prompted;

For an SMS text message, enter the provided code in the logon box;

For the Authenticator app, enter the provided code in the logon box;

I got prompted for MFA authentication, but was not logging on at the time; what should I do?

This may mean that some else has access to your username and password. Please change your password immediately and report this to Digital Services for investigation.

I no longer have access to my MFA device; what do I do?

If you have alternate phone number or device registered, you can use this and go to <https://www.staffs.ac.uk/mysecurityinfo>, to remove old numbers and devices, or to add in new devices. If you no longer have access to any registered devices, please contact Digital Services who are able to reset your MFA details to allow you to register your new device.

I get prompted for MFA every time I log on; how do I stop this?

If you are using a TOR browser or VPN to mask your location then this is expected, otherwise please report this to Digital Services for investigation.