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 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.

If you wish to register or update your MFA details, please visit https://www.staffs.ac.uk/mysecurityinfo. We would recommend that you register a phone number as one of your MFA options, even if you plan to use the app as your primary MFA method.

For some staff and students, 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.

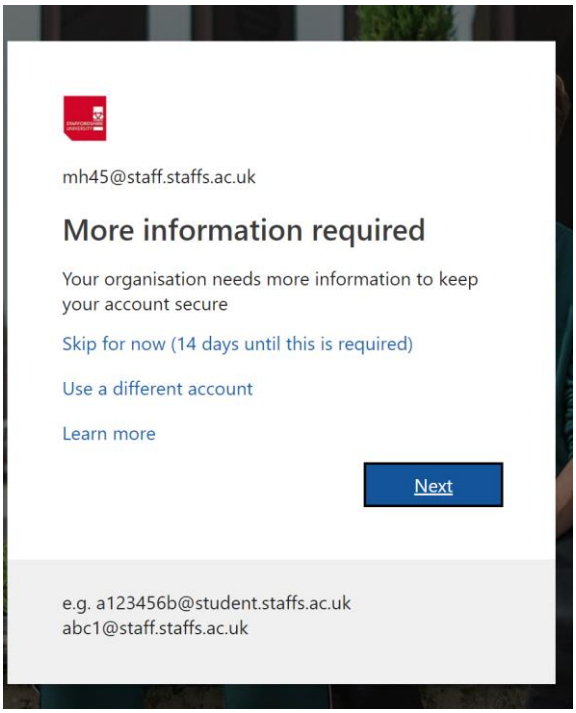
Frequently asked questions regarding Staffordshire University's MFA implementation can be found at the end of this document, but if you have any other questions, please contact Digital Services' support desk at 3800@staffs.ac.uk.

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

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, IRIS, etc.), you will be prompted to provide more information.



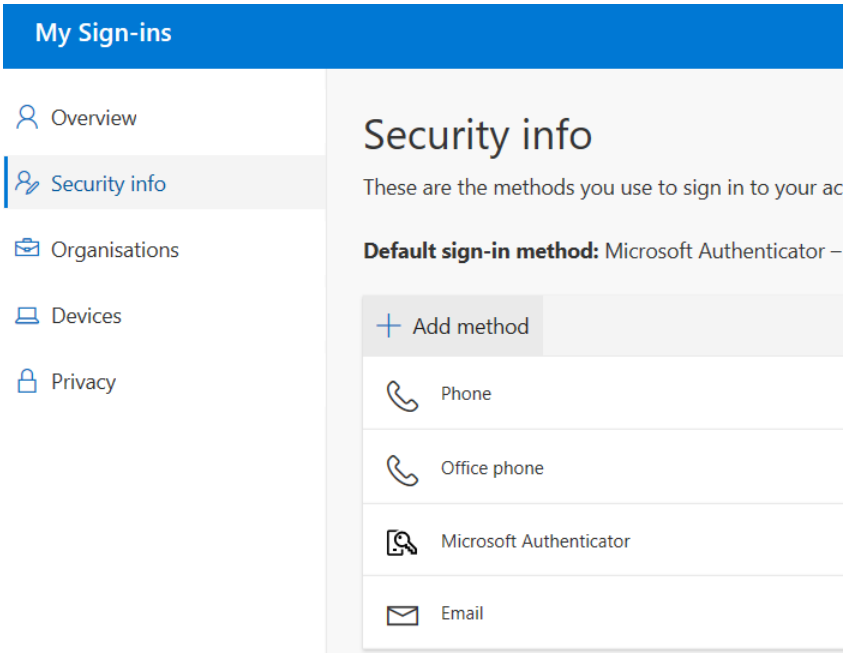
You can skip the registration process for up to 14 days, after which you must register to gain access to protected systems:

Clicking "Next" when prompted for more information uses the same MFA registration process as the manual registration detailed below.

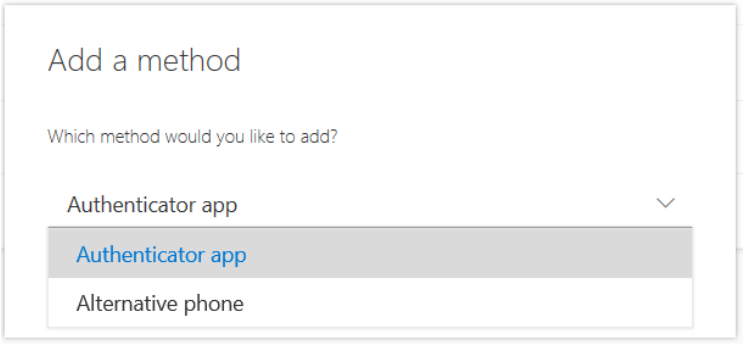
Manually Registering for Multi-factor Authentication

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)

In the "Security Info" page, click "+ Add Method" to start the registration process, the registration will default to set up the Microsoft Authenticator app on your tablet or smartphone:



Should you wish to use a phone call or SMS text message for verification instead, please click on the "Choose security info" link and select "Phone" as the authentication method:



As people tend to keep a phone number longer than an app, it is always recommended that you register your phone number. You can register multiple phone numbers as well as the Authenticator app from the multi-factor authentication site at https://www.staffs.ac.uk/mysecurityinfo.

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

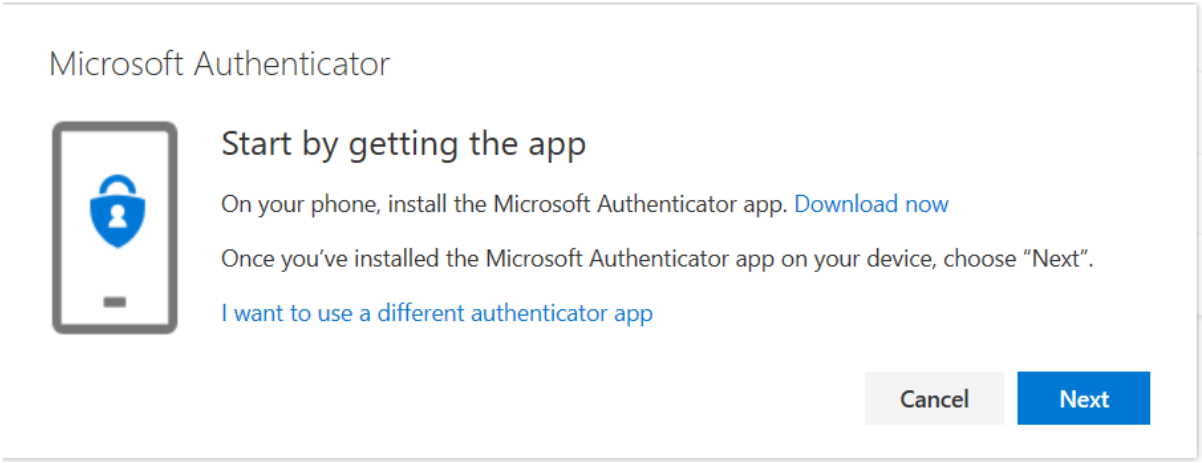
Details on setting up multi-factor authentication through a phone are available online at: https://docs.microsoft.com/en-gb/azure/active-directory/user-help/security-info-setup-phone-number

It is recommended that you review your MFA details periodically through the setup page https://www.staffs.ac.uk/mysecurityinfo

Registering the Authenticator App

1. Select the **Authenticator app** option

2. A "Start by getting the app" wizard will appear:

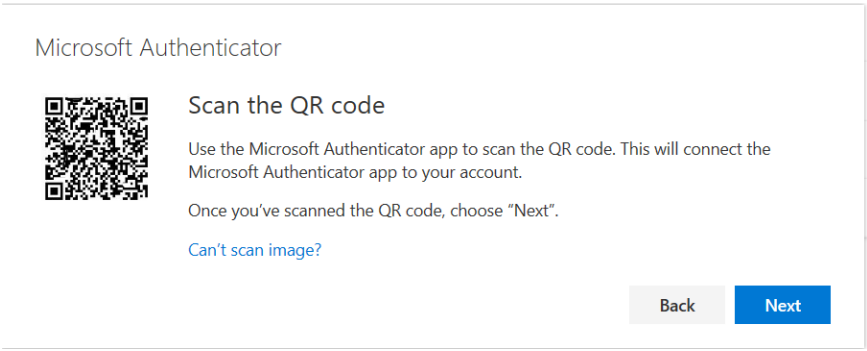


3. After you install the Microsoft Authenticator app, select "Next"

   If you're prompted, choose to allow notifications, add a new account and then select "Work or school account"

   If you already have your university account listed within Microsoft Authenticator, use the drop down menu on the right of the account to select "enable two step verification"

4. Select "Next"
5. A "Scan the QR code" screen will appear:



6. Open the Microsoft Authenticator app, select **Add account** from the "Customize and control" icon in the upper-right corner, and select "Work or school account"
7. If you have a QR code reader app, scan the provided code.

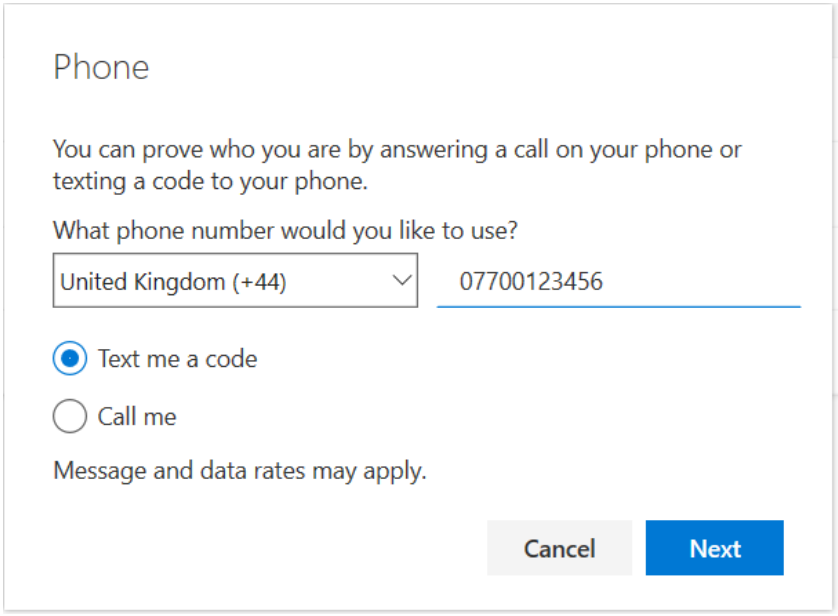
   If you don't have a QR code reader app, you can select the "Can't scan the QR code?" link and manually enter the code and URL into the Microsoft Authenticator app

8. 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 use "Choose security info" to add additional authentication methods.

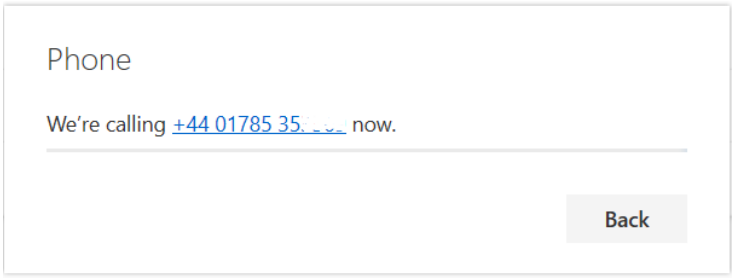
Registering a Phone

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 the **Call me** option, 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.



After registration, you can change your multi-factor authentication details at any time from this link: https://www.staffs.ac.uk/mysecurityinfo

Multi-factor Authentication FAQ

1. 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.

2. Why do we need multi-factor authentication?

3. Analysis of the 23 successful ransomware attacks on UK Colleges and Universities between August 2020 and June 2021 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. It is an essential defensive tool which helps to keep the university safe for all members of staff and students.

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

MFA does not require use of smart phone, you can use any phone, including your work number and/or home landline number to register for multi-factor authentication.

4. 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.

5. 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.

6. 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. You can register multiple phone numbers 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.

7. 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, however as people tend to keep a phone number longer than a

individual smart phone, it is always recommended that you always register a phone number 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.

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

Yes, the Microsoft Authenticator supports multiple devices.

9. 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.

10. 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.

11. 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 log on box;

For the Authenticator app, press "Approve".

12. 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.

13. 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.

14. 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.