Multi Factor Authentication (MFA) FAQs

Why is the University implementing MFA?

Cybercrime continues to rise and as a result it is increasingly important that your personal information and data is protected. MFA is being implemented in order to do exactly this, using a widely utilised security tool, to keep personal and university data secure.

The University's MFA service adds an extra validation step after a username and password has been entered, making it significantly more difficult for hackers to access that service or system. This extra protection is needed because of the increasingly sophisticated levels of attacks used by hackers to gain access to online services.

The extra validation step used by the University's MFA service helps to prove who you are by adding 'something you have' to 'something you know'.

Something you know - your password.
Something you have - a security token generated by an app on your phone or a phone call to your phone.

Can I opt-out of setting up MFA?

No, all staff and students are required to have their accounts protected when accessing MFA enabled services.

Which services use MFA?

Below is a full list of university services related to Microsoft 365 and other online systems that will require you to provide MFA when off campus.

If you have previously set up MFA for university system access, this will continue to work and will just extend to cover the additional systems and services. If you have a university Windows 10 laptop then some of these services may not require MFA authentication.

Everyone signing in to:

- University Portal
  - Ethics
- Microsoft 365 including:
  - Microsoft Office 365 apps, including such as Word, Excel, PowerPoint and Outlook
  - OneDrive
  - Teams
- Solent Online Learning – SOL (Moodle)
  - LinkedIn
  - Marks Upload
- Adobe Creative Cloud
- Avid_Newsroom
- Bentley IMS
- Boomerang
- edutrack
- EdX.org
- myday
- ReadAndWrite
- Rhino 3D
- SEAtS Solent Site
- SISO SmartHub

Staff signing in to:

- Via the University Portal:
  - Data Preferences
  - Gifts and Hospitality
  - Phonebook
- Contensis
- Planera (non-VPN access only)
- Quercus (non-VPN access only)
- Tableau (non-VPN access only)
- GeckoEngage
- Smartsheet
- Worktribe (Curriculum Management)

Students signing in to:

- Via the University Portal:
  - Edit Student Details
  - Graduation Booking
  - Student Course Options
  - Student Placements
  - Student Registration
  - Student Results
  - Therapy and Mental Health
- My Study Life

I've received an unexpected text message or an App notification to verify my authentication.

Please decline the app notification and contact the ICT Service Desk who can investigate further.

What do I do if I cannot get into my account?

Please contact the ICT Service Desk.

Will I need MFA on campus?

No. Just an initial one-off sign up is needed, then authentication while off-campus.

Can I use my existing MFA app?

If you have previously set up MFA using Microsoft Authenticator, for university system access, this will continue to work and will just extend to cover the additional systems and services.

If you have another MFA app installed the University's MFA service uses the Time-based One Time Password (TOTP) standard for generating unique, time-limited, authentication codes. Any MFA app that follows the TOTP standard could also be used. Please note: we are not able to provide any support for the use of such apps.

Can I use the Microsoft Authenticator App to authenticate other non-university services, e.g. my personal Amazon account?

Yes you can.

Open Microsoft Authenticator app on your mobile phone and go to 'add account'. You can then use it to protect your personal accounts for example: Amazon, PayPal and Facebook. Please note: we are not able to provide any support for this use of MFA.

I am concerned about using my personal mobile phone for work or as part of my university study?

Keeping your university account secure will protect both the organisation and your own personal data.

Your personal mobile device details are not used for any other purpose than protecting your account. By adding the Microsoft Authenticator App to your personal device this is just providing a method to confirm who you are. The app is not used to manage or control your device or provide any personal data and can be used for other organisations and systems requiring MFA.

When you finish your course, or if you leave the University, you can remove the Universities account from the Microsoft Authenticator app but continue to use it to protect your other services.

When I provide my MFA sign up details/methods, will the University have access to this information?

No, the Microsoft Authenticator mobile app (iOS and Android) does not request any personal information, it simply holds an electronic token unique to your university account.

You can manage your MFA settings later in the MFA - Additional security verification options page.

Is there another way to be secure without using my personal mobile device?

You must select at least one additional security method to your university password, however, if you cannot, or do not wish to use your personal mobile device, there are some other options available.

You can use any landline number as an additional method. For example, you can use your home phone number.

If it is not possible to use either of these options then a third-party MFA app that runs on Windows, MacOS or Linux could be used, provided that the app is compliant with the Time-based One Time Password (TOTP) standard. Please note: we are not able to provide any support for the use of such apps.

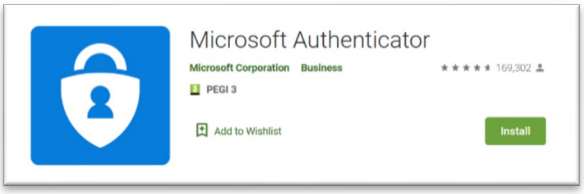
What should I do if I lose my phone?

If you are on campus, log into MFA - Additional security verification options page and delete your **'Authenticator app – Phone name'** option at the bottom and set up a new method or device.

If you are off-campus, contact the ICT Service Desk for further assistance.

What if I change my phone?

If you get a new phone then you will need to install the Microsoft Authenticator app on your new phone and change the setup of your MFA.



What can I do if I don't have a smartphone or phone?

We recommend that you use, where possible, either the Microsoft Authenticator app on your smartphone or the option to call to your personal mobile or landline phone.

If it is not possible to use either of these options then a third-party MFA app that runs on Windows, MacOS or Linux could be used, provided that the app is compliant with the Time-based One Time Password (TOTP) standard. Please note: we are not able to provide any support for the use of such apps.

What is the difference between Microsoft Authenticator app (notification) and Microsoft Authenticator app (code)?

The Microsoft Authenticator App can function in two modes; one which provides an easy one click notification pop up, you click approve and your sign in is authorised.

The other mode is app code which provides a rolling six-digit code that changes every 30 seconds, you need to enter the code before it changes.

Both methods are secure. The notification method is the quickest, but you have to approve/deny every MFA request related to your account, including approval requests that may be generated by account access attempts by hackers.

The app code method takes longer but protects you from having to decide whether an access request is valid or not, as hackers would need to have access to an MFA app registered to your account in order to gain access.

If your device only gives you the code option, ensure your default method is set correctly. Visit the MFA - Additional security verification options page and change the default option to Microsoft Authenticator – notification.

Please note: some smart phones do not support the notification method.

How to I contact the ICT Service Desk?

- Log an issue via: unity.solent.ac.uk
- Call us on: 023 8201 2345
- Or pop into RMG14