Frequently Asked Questions: A new log in journey

Updated 2 June 2017

Our Cyber Security Programme is introducing new and improved practices to keep our information and data secure. This includes stronger security to protect access to certain University services, by introducing changes to the login process. It will involve logging into GlobalProtect Virtual Private Network and verifying your identity using 2-factor authentication.

Find answers to the most frequently asked questions below. If you need any further help or advice, you can contact our IT Support Centre 24 hours a day, seven days a week, by visiting: www.itservices.manchester.ac.uk/help or calling 0161 306 5544.

Questions are grouped by the following themes:

2-factor authentication (2FA)

- Getting to know Duo and 2-factor authentication
- Using your smartphone or a Duo key fob to verify your identity
- Securing University email with 2-factor authentication
- Using 2-factor authentication when travelling
- Using 2-factor authentication in teaching spaces
- Using 2-factor authentication in ‘wet labs’

Using GlobalProtect Virtual Private Network

Privacy and use of data

Account security
2-factor authentication

Getting to know Duo and 2-factor authentication

1. What is 2-factor authentication?

It’s an extra layer of IT security which requires you to enter two pieces of information to access certain systems.

Using something that you know (your password) along with something you use, like your phone or another device, to log in. Similar services are already being used by banks as well as Google, Twitter and Facebook. We are using a company called Duo to provide our 2-factor authentication service.

2. How does 2-factor authentication protect my account?

2-factor authentication protects your account by adding the extra security layer that will require you to verify your identity when you log in. As well as your username and password, 2-factor authentication requires that you have an authentication token in your possession allowing you to respond with a tap or a code as you login. If your username or password details are stolen, the person in possession of them won’t be able to login to your account without the token.

You can learn more about Duo, by visiting: https://guide.duo.com/

3. Why is the University introducing this extra layer of security?

We’re taking steps to protect both University services and our intellectual property from unauthorised access. It’s an extra step, we know, but 2-factor authentication is easy to use and you may have already come across similar services used by banks, Google, Twitter and Facebook.

4. Who will need to use 2-factor authentication?

2-factor authentication will be used by all University staff and Postgraduate Research students.

5. How do I set up 2-factor authentication?

All University staff and Postgraduate Research students will receive set up instructions which will involve visiting the IT Account Manager at: https://iam.manchester.ac.uk/. Click ‘Manage your IT account’ and select the ‘2FA(DUO)’ tab.

6. What do I need to install on my phone before I can use 2-factor authentication?
If you choose the smartphone option to verify your identity, you will need to install the Duo mobile app. The email you receive from IT Services will guide you through the set up process, including how to install the free Duo mobile app from your device app store. Instructions are available at: https://iam.manchester.ac.uk/. Click ‘Manage your IT account’ and select the ‘2FA(DUO)’ tab.

7. What happens if I don’t enrol onto Duo?

Duo is being used to protect certain University services with 2-factor authentication. You will not be able to access these services if you have not enrolled.

8. I deleted or didn’t receive my enrolment email. What should I do?

Go to the University IT Account Manager at: https://iam.manchester.ac.uk/. Click ‘Manage your IT account’ and select the ‘2FA(DUO)’ tab.

9. Will I have to authenticate with 2-factor authentication every time I lock my device?

No. When using a computer, you will only need to use 2-factor authentication once per day as long as you are on the University network. Each login session will last for 12 hours. During this period if you are using a laptop you will be able to move around the University Campus buildings using the same login session. Some services such as Outlook Web App however, will require you to use Duo each time you access them.

10. Will I have to use 2-factor authentication to access the University resources if I am on my own computer, or one that is not managed by the University and is not connected to the University network?

Yes, to access certain University services you will have to use 2-factor authentication, regardless of the type of device or network location. If you are using your own computer or one that is not managed by the University, you will also need to install our GlobalProtect VPN client. (see Using GlobalProtect Virtual Private Network)

Using your smartphone or a Duo key fob to verify your identity

11. What if I don’t have a mobile phone?

If a smartphone option is not suitable for you, there are the following alternatives: receiving a phone call, receiving a text message or using a Duo key fob to generate a code.
13. What do I do if I have no internet connection or mobile phone reception?

The Duo mobile app on your smart phone can generate a one-time passcode (OTP) without the need for any mobile or internet connection. Simply tap the Duo mobile app and use the code generated when prompted. The Duo key fob can also be used to generate codes or you can have a set of OTP codes sent in advance to your phone by text message.

You will need a mobile phone signal if you are using text message or phone prompt and an internet connection through Wi-Fi, 3G or 4G if you are using a Duo mobile push, which is the smartphone option.

14. Can I verify my identity if I select ‘phone call’ and then do not answer the phone?

No. You need to answer the phone and press a key when prompted.

15. What if I get a new mobile phone but keep the same number?

If you are using the Duo mobile app for authentication, you should backup your existing phone and transfer your apps and data to your new phone. If this is not possible you will need to enrol your new phone and remove the old one. You will not need to do anything if you are using a traditional mobile phone without the Duo mobile app.

16. What if I share a phone with someone else?

Just as we don’t share our passwords with anyone else, you should not share the device that you are using to verify your identity. If you normally share a phone, you should use a different method or a phone that is used only by you to verify your identity as part of the log-in.

17. What happens if I want to change from using a smartphone to a Duo key fob?

Contact our IT Support Centre, who will be able to issue you with a Duo key fob.

18. What if I forget or lose my phone?

Contact our IT Support Centre by visiting: www.itservices.manchester.ac.uk/help or by phone on 0161 306 5544. They will be able to issue an emergency passcode to a colleague nominated by you so that you can continue working. If you have lost your phone they will also help you register the phone as lost and enrol a new one.

19. What happens if I forget my Duo key fob? Can I use my colleague’s?
No. Your key fob is unique and will be registered to you. Contact our IT Support Centre by visiting: www.itservices.manchester.ac.uk/help or by phone on 0161 306 5544. They will be able to issue an emergency passcode to a colleague nominated by you so that you can continue working. If you have lost your Duo key fob they will also help you.

20. What do I do if I want to deactivate my Duo key fob?

If you no longer need your Duo key fob please request deactivation and return it to our IT Support Centre. Ensure that the token has been de-activated for your user account before it leaves your possession.

21. Can I register more than one authentication method?

Yes.

Securing University email with 2-factor authentication

22. Will I access my email any differently when it’s secured by 2-factor authentication?

You will access email the same way, but depending on the method you use to access email you may also need to authenticate with Duo when you log in each day or each time you access the web based Outlook Web App (OWA). If you use an existing mobile device (e.g. an iPhone or an iPad) to access email using ActiveSync then the day to day experience will be unchanged.

If you connect to the University mail servers from a Windows computer using a mail client, such as Outlook, you will go through an extra step after logging in to your computer. This will involve logging in with our GlobalProtect VPN client (see Using GlobalProtect Virtual Private Network) and using your smartphone or other chosen option to verify your identity. If you are using your own computer or one that is not managed by the University you will need to install our GlobalProtect VPN client before you can access a ‘full’ mail service using Outlook on that computer. You can do this by visiting: www.manchester.ac.uk/cyber/2step/gpvpn.

If you are using Outlook Web App (OWA) you will need to authenticate each time you open the application in your browser. You will provide your username and password as normal, then respond to a Duo authentication prompt using your 2-factor authentication token.

If you have an existing mobile device to access email using ActiveSync then the day to day experience will be unchanged. As you enrol new devices to ActiveSync you will be required to
respond to a 2-factor authentication prompt to complete enrolment. After enrolment new devices will connect to the mail systems without further prompts.

23. What if I have multiple mobile devices?

More than one mobile device can be used simultaneously to access University email. Only one of these devices (which will most likely be your smartphone) can be used as the 2-factor authentication device and this must have the Duo mobile app installed.

24. Will this stop my PA from having access to my email and calendar?

No. If your email has been delegated to someone else they will be able to continue to access your mailbox as before.

25. Will my personal email account on my mobile be affected by 2-factor authentication?

Your personal email accounts will not be affected. The University does encourage you to protect your personal email accounts with similar technology if available.

Using 2-factor authentication when travelling

26. What should I do if I am traveling outside of the UK or working overseas?

2-factor authentication should work the same way regardless of the country you are in. Modifying your phone’s date or time may prevent the Duo mobile app from working. You should alter the time zone on the device rather than the changing the time.

27. Can I use my smartphone to verify my identity if it has an international number?

Yes.

Using 2-factor authentication in teaching spaces

28. Will I have to use 2-factor authentication to log-in to teaching and learning computers?
No. You will be able to continue to log into teaching and learning computers in lecture theatres as you do now. However, when you subsequently try and access a protected service you will be prompted to use GlobalProtect VPN and 2-factor authentication.

29. Will I still be able to access email on a teaching PC?

Yes - Outlook Web App can be used to send and receive email from a public access or teaching PC; however you will need to authenticate with 2-factor authentication to access it.

**Using 2-factor authentication in ‘wet labs’**

30. What happens if I work in a ‘wet lab’ where use of mobile devices is not encouraged?

If you use a networked computer in a ‘wet-lab’ to access University services from that computer you will need to use a Duo key fob at that computer. You can use the same Duo key fob to access services at computers outside of the ‘wet lab’ or you can register your smartphone as an authentication method when outside the lab.

Individual ‘clean rooms’ will have special arrangements in place to support authentication.
Using GlobalProtect Virtual Private Network

31. When do I need to use the new GlobalProtect Virtual Private Network?

You will need to use the GlobalProtect Virtual Private Network client daily if you want to access mail from a personal computer using an application such as Outlook - in the future you will need it to access some resources in the new Restricted and Highly Restricted security zones.

32. What do I need to install on my computer or laptop before I can access University services?

If you are a member of staff or a Postgraduate Research student you will need to use GlobalProtect Virtual Network client installed on your device. GlobalProtect VPN client will be installed automatically on all managed devices. Find out if your computer is managed or unmanaged. If you are using your own computer or one that is not managed by the University, you will need to install our GlobalProtect Virtual Private Network. You can do this by visiting: www.manchester.ac.uk/cyber/2step/gpvpn

33. Can I install GlobalProtect VPN client on more than one device, for example at home and at work?

Yes, GlobalProtect VPN client can be installed on as many devices as you need. Note that the GlobalProtect VPN client is only needed if you wish to access email from a personal computer such as a Windows PC or Mac, or in the future if you wish to access University resources that reside in the new ‘Restricted’ or ‘Highly Restricted’ security zones.

34. What are the ‘Restricted’ and ‘Highly Restricted’ security zones, and how can I find out if my resources are hosted there?

The new network security zones have been created to host some University services to provide additional protection against unauthorised access. All applications will be moved to either an Unrestricted a Restricted or Highly Restricted zone. Many systems and applications that contain sensitive data and are intended for use only by staff and postgraduate research students will be hosted in, or migrated to the Restricted zone. The Highly Restricted zone will host more sensitive University resources. At the time when applications are migrated into the zones users will be informed about any changes to the login process.

35. Is it possible to run another VPN client when GlobalProtect VPN is enabled?

No, GlobalProtect must be temporarily disabled if you need to use another VPN client.
36. What do I do if GlobalProtect VPN keeps prompting me to login when I don’t need to use it?

GlobalProtect has been configured temporarily to connect automatically when your device is used away from the University campus. We expect this to change so that you will benefit from automatic connection when on-campus, but be able to connect manually when off-campus. In the meantime, you can disable the GlobalProtect VPN client if you do not wish to use it and prevent on screen prompts for connection.

Don’t forget to re-enable it when you return to the University network.

For Windows users – Right click the GlobalProtect system tray icon ( ) and select Disable. If you do not see the icon, click a chevron or arrowhead symbol to see hidden icons in the notification area.

For Mac users – Click the GlobalProtect menu bar icon ( ) and select Disable.

Privacy and use of data

37. What information is being stored by Duo and how do I know it’s secure?

The only two pieces of information that the University shares with Duo are your user ID and your University email address. If you choose to use a mobile phone or landline, then your phone number will also be held. Our contract with Duo is fully compliant with UK data protection legislation which means neither the University nor Duo will use your Duo registered mobile number for any other purpose other than 2-factor authentication without your explicit consent.

38. How much mobile data does Duo use when I use my smartphone to verify my identity?

Each time you receive a Duo notification on your smartphone you will use a very small amount of data. We expect this to be approximately 40KB (0.00004GB) per month which may come out of your mobile data plan if you are not connected to Wi-Fi. It should not cost you anything to receive authentication text messages in most locations. Use of one-time password (OTP) codes generated by the Duo mobile app will not incur any data costs.

39. What happens when I leave the University? Will the service keep my phone details forever?

No your details will be deleted from the service after your University ID is disabled a few weeks after you have left.
Account security

40. What should I do if I am locked out of my account?

Go to: https://iam.manchester.ac.uk/ to unlock your account. If however you are experiencing problems with your Duo key fob contact our IT Support Centre.

41. What should I do if I receive an unexpected Duo notification on my phone when I am not logging in myself?

If your computer has recently been connected to a network it may be that GlobalProtect is attempting to connect resulting in the Duo prompt to your phone and may be safely ignored if this is the case and you do not wish to complete the connection. If you have not connected your device to a network, it may mean that your password has been compromised and Duo is protecting your account. You should deny the login attempt then report it to our IT Support Centre if you are suspicious. Consider changing your password if you suspect somebody has accessed to your account by logging into the IT Account Manager at: https://iam.manchester.ac.uk/.

42. Do I have to use PIN protect on my phone?

If your phone or mobile device is set up for University email access, the device is already required to have a PIN or fingerprint enabled.

If you are purely using your phone for 2-factor authentication we strongly recommend that you protect access to your phone with a PIN to protect your information and access to the Duo mobile app.