Jesus College Oxford

SSO Accounts – Introduction of Multi-Factor Authentication

Overview

Multi-factor Authentication (MFA) on your SSO account means that when you log in you will need, in addition to your password (which is often known as the first factor) a second factor. This second factor can be implemented with a variety of different methods (outlined further on) but for most people the simplest is to use an Authenticator app on your phone. When you want to log in with your SSO and you've entered your password correctly, the Authenticator app will ask you to confirm that it's you by pressing the app's "Approve" button. MFA makes it much more difficult for attackers to gain unauthorized access to your SSO account and it is expected that the adoption of MFA has massively reduced the number of Oxford accounts which are compromised each year.

A very small number of users may not be able to use multi-factor authentication due to exceptional circumstances, such as accessibility issues. In these cases, individuals can request an exemption by completing a service desk exemption request. This request must be authorised by a manager, supervisor, tutor or administrator – the request form will be sent to them automatically for confirmation.

Choosing your means of MFA

The University has provided a number of different methods for MFA – the main ones are:

- Using the Microsoft Authenticator app on your mobile phone
- Receiving an SMS message on your mobile phone
- Receiving a phone call on a landline or mobile phone
- Using the Authy desktop/mobile authenticator app
- Using a hardware token

The main advantages and disadvantages of these methods are outlined below, and there is a link to the instructions on how to implement each method in the "Setting Up MFA in Advance" section further on.

If you have a suitable smartphone (almost any Android or Apple phone from the last five years is fine) then the Microsoft Authenticator app is usually the most simple and flexible way to achieve MFA. When you login with your SSO the Authenticator will ask you to press its "Approve" button, and that's all you need to do to complete the operation. This method does of course rely on you having your phone with you at the time, and the phone must also have a data connection to the Internet as well, either through wifi or its own mobile network data.

If your mobile phone can't connect to the Internet, or isn't able to at the location where you want to log in, you can instead use an SMS message as an MFA method. With this, you register your mobile phone number against your SSO account and when you log in the system will send you a 6-digit code as a text message. You then enter this code on the computer you want to log in on, and this completes the MFA operation. This is obviously a little more fiddly than simply hitting the Approve button on the Authenticator but it may be a useful method for anyone with an older mobile phone or one which cannot receive data in the location from where they want to log in.

Phone calls are another simple way to complete MFA – the system will call you on a pre-defined number and all you need do is press the hash key on the phone to authenticate. Obviously this relies on the phone line being free, and for landlines (if you have one) you have to be physically present to answer it. We would recommend using the phone-call method as a possible alternative solution in the event that your usual means of MFA is not working .

The Authy app is another alternative – this is software which can be installed on your computer (Mac or Windows) or even your phone, and which generates a 6-digit token that changes every 30 seconds and which can be used as the MFA login. Like the tokens delivered by text message, it's a bit more fiddly than the Microsoft Authenticator as you have to enter the 6 digit token code each time but again, this would be fine as a backup method in the event that your smartphone is out of action. You do need a phone to set up Authy initially (it can be mobile or landline which it will call or text in order to identify you) but once configured on a desktop computer it won't generally need to use the phone again.

Finally, for anyone for whom the above methods are not practicable, you could use a hardware token. These are small USB devices which have a push-button on them – when you are prompted for MFA you simply push the button and this confirms that it's you that's logging in. It's again a very simple and easy-to-use method of achieving MFA and the only major downside is that you have to carry the device around with you if you want to log in from different locations. The cost of the devices is generally £20 - £30.

In most circumstances you will choose one of these methods of MFA to be your default method, and you will also configure as many other methods as you wish as alternatives in the event that your default method is unavailable. The alternatives should be chosen so that they will cover the range of likely situations you might find yourself in – for example, a staff member might choose the Authenticator as their default MFA login, but then also configure alternative methods using their home and work landlines. In the event that their phone is not available, they will still be able to log in regardless of whether they are at home or work. For a student, again the Authenticator is likely to be the best default method but for alternatives they could use a phone call to the mobile and also installing Authy onto their computer, meaning that they would again still be able to log in should the mobile be unavailable for any reason.

There are other methods of MFA outlined on the IT Services link below but we believe that for most people, the Microsoft Authenticator plus a variety of different phone numbers, and/or Authy, should provide the simplest and most effective means of logging in.

Setting up MFA in advance

We would strongly advise setting up your MFA methods in advance of arriving at the College. You will need your SSO to sign into a number of College services such as meal-booking and wifi system, so configuring it in advance will mean a much smoother experience when you get here. It will mean that when you are prompted for MFA the first time, you simply need to use your pre-configured method to complete the login process and this should take a matter of seconds. If you haven't set up MFA in advance then you may find, when you're prompted, that you're not in an ideal location to do it, and you won't be able to connect to email or Microsoft Teams until you have.

To set up MFA in advance, please use the IT Services guidance here:

https://projects.it.ox.ac.uk/prepare-mfa

This is a comprehensive guide to what you need to do to configure the different means of MFA. Obviously you can ignore any of the methods which you are not planning to use. If you're not sure which methods to use or need assistance with setting them up then please contact the college IT department – it-help@jesus.ox.ac.uk

You can change your MFA methods or change your default method at any time by using this link:

https://mysignins.microsoft.com/security-info

but if MFA has already been enabled on your account, you will need to have at least one working MFA method in order to be able to log in to make changes. However, if necessary, IT Services or the college IT department are able to wipe all MFA methods from your SSO account so that you can set them up afresh. Proof of identity may be required for an MFA wipe to occur, though.

Watch out for…

When you log in with your SSO, it needs to be in the form

sso@OX.AC.UK e.g. jesu1234@OX.AC.UK

It's advisable to use lower-case prior to the @ sign and upper-case after it. **Note that when Teams asks you to log in with your email address you now need to enter sso@OX.AC.UK even though this is not in fact an email address.**