Multi-Factor Authentication Project

The Multi-Factor Authentication Project is responsible for providing all Oxford Single Sign-On users with additional verification methods when accessing materials which are currently protected by Single Sign-On. This guide will assist you in setting up an additional authentication factor for your Single Sign-On.

The project is adopting a phased approach to the second factor being switched on. You will receive communications in set intervals informing you of when you are due to go-live with your second factor.

When this is switched on, your access to existing applications will be suspended.

This guide will show you how to set up the mobile app to send notifications or a code which will act as your multi-factor authentication method.

1. You may receive a notification advising that your details need updating. Clicking on the notification will take you to the settings page for your PC.

2. Click Fix now

3. If you are not taken to your PC settings a message will appear asking for more information. It will also appear after you click Fix Now

4. Click Next

5. The Nexus365 security verification screen will display
This is the area where you set up how the system will contact you when you need to provide a second authentication method.

You can set up an authenticator app to send a notification or a code to your mobile device as your security verification method. The first part of this guide describes the processes involved to set up the Microsoft Authenticator App.

Please navigate to the next section (Setting up multi-factor authentication on a different authenticator app) for the process on how to set-up a different authenticator app.

Before you can add your account you must download and install an Authenticator App on your device.

6. On the Nexus365 security verification page, click **Next**

7. Open the mobile app

8. If prompted, allow notifications in the app

9. In the App, click **Add account**, then click **Work or school Account**

10. A QR code scanner will appear on the screen

11. In the Nexus365 security verification screen, click **Next**
12. Scan the QR code.

13. Click Next

14. The app set-up will be completed (Skip to step 20)

15. If you can’t scan the QR code, click Can’t scan image?

16. On the Nexus365 security verification page a nine digit code and a URL will be populated

17. In the app, click Or enter code manually

18. Enter the code and the URL

19. Click Finish in the app

20. The system will send a notification to the app

21. Click Approve in the mobile app
22. The Nexus365 security verification page will show that the notification has been approved. (If the notification doesn’t work or you want to set up a code, skip to step 25)

23. Click Next

24. A green confirmation message will appear in the top corner of the screen confirming that the app has been set up. Microsoft Authenticator will appear in the list as a registered method

25. If the notification doesn’t work (or you press Deny instead of approve) an error message will appear in the system

26. Click Resend notification to receive a new notification (if you clicked Enter a code instead, skip to step 29).

27. If you clicked Resend notification approve the new notification.

28. Click Next

At this point your Multi-factor authentication method has been set-up.

29. If you clicked Enter a code, you will be asked to add an account
30. In the App, click the symbol in the top right corner.

31. Click Add Account

32. Choose Other Account (Google, Facebook etc.)

33. On your computer, click Next

34. Scan the QR Code

35. Click Next

36. In the App, open the account which has been set up for code (logo is a black circle with a person inside it)

37. On your computer, enter the six digit code from the app.

In some instances, the system will ask if you want to set-up an App Password. These are only required if you are accessing older applications or non-Microsoft clients (Outlook prior to 2016, Gmail, native email applications on smart devices).

If you do not need to set up an App password you can close the page.

For assistance on how to set up an App password please use the guidance on the project webpage.

*Note - first you must have requested App password enablement using the appropriate service request.
Setting up multi-factor authentication on a different authenticator app

If you would prefer to use a different authenticator app, or your device restricts you from installing the Microsoft App, the following process will describe how to set up multi-factor authentication on a different authenticator app. First you must have downloaded your chosen authenticator app.

1. On the Microsoft Authenticator screen click **I want to use a different authenticator app**

   ![Microsoft Authenticator](image)

2. From within the app select the option to add a new account

3. Click **Next** in the set-up window on your device

   ![Authenticator app](image)

4. A QR code will populate on the screen

5. Scan the QR code

6. Click **Next**

7. The authenticator app is now set-up.

8. In the app, complete any set up processes that appear.
9. On your computer, a window to enter a 6-digit code will appear. Enter the code to test the set up.

![Authenticator app](image)

10. Click **Next**

11. Following successful entry of the code the set-up will be complete. Authenticator App will now show as a method of multi-factor authentication in your Microsoft Account.