Multi-Factor Authentication

Setting up verification via the mobile app

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.

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. Go to My Sign-Ins
2. Select your account
   ![Select account](image)
3. Enter your Single Sign-On (SSO) password
4. Click Next on the ‘More information is required’ screen
   ![More information required](image)

Before you can add your account, you must download and install the MS Authenticator app on your device.

5. Click Next
   ![Keep your account secure](image)

15.03.21/v2.0
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.

6. Open the MS Authenticator app on your phone. If prompted, allow notifications in the app
7. Click Add account
8. Select Work or school Account

9. Select the option to ‘Scan a QR code’. A QR code scanner will appear on your phone screen.
10. Click Next on the Set up your account screen

11. Scan the QR code displayed using your phone. If the QR code cannot be scanned, select Or enter the code manually and go to step 12, otherwise go to step 14.
12. Go back to ‘Scan the QR Code’ screen and click Can’t scan image?
13. Enter the Code and the URL displayed into the MS Authenticator app and click Finish
14. Click **Next**

![QR code scan](image)

Scan the QR code
Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.
After you scan the QR code, choose "Next".

Can't scan image?
Back  Next

15. The MS Authenticator app will send a notification to Approve or Deny the sign-in request. Click **Approve**.

![Notification](image)

**Approve sign-in?**
Nexus365
mailto:test@ox.ac.uk
Deny  Approve

16. The notification has been approved. If the notification doesn’t work and you get an error message go to step 20.

![Authentication](image)

**Microsoft Authenticator**

- Notification approved

Back  Next

17. Click **Next**

18. Your Microsoft Authenticator app is now set up, click **Done**

![Success](image)

**Success!**
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

**Default sign-in method:** Microsoft Authenticator - notification

Microsoft Authenticator

Done

15.03.21/v2.0

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

21. Click Resend notification to receive a new notification. If you clicked Enter a code, skip to step 25.

22. The MS Authenticator app will send a new notification
23. Click Approve

24. Click Next on your computer. At this point your Multi-factor authentication method has been set-up.

25. If you clicked Enter a code, you will be asked to add an account.
26. In the MS Authenticator app, click the symbol in the top right corner.

27. Click Add Account
28. Choose Other Account (Google, Facebook etc.)

29. On your computer, click Next

30. Scan the QR Code
31. On your computer, click Next
32. In the App, open the account which has been set up for code (logo is a black circle with a person inside it)

33. On your computer, enter the six-digit code from the app and click **Next**.

Your MFA method is now set-up.

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).

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 Authenticator app, the following process will describe how to set up multi-factor authentication using 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**

2. Select the option to add a new account from the authenticator app and select **Scan a QR code**

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

4. A QR code will be displayed on the screen
5. Scan the QR code
6. Click **Next** on your computer

7. A six-digit code will be requested for the account being set up. Open the Authenticator app and type the code for that account.

8. Click **Next**
9. 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**.