Multi-Factor Authentication Project

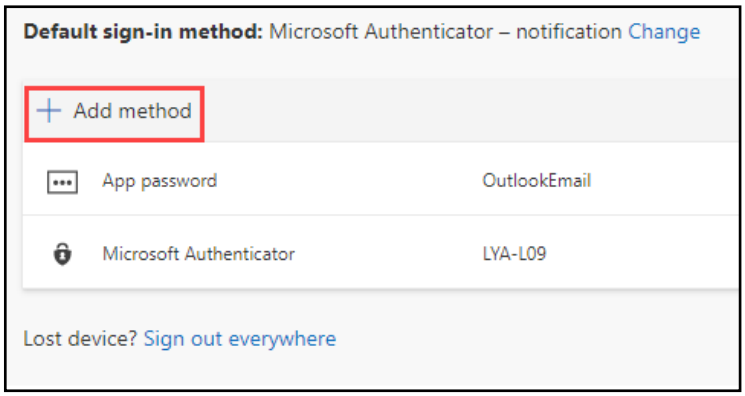
Downloading and configuring the Authy mobile app

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.

This guide will show you how to set up the Authy mobile app (It can also be installed on your desktop or laptop). Authy is a free application which provides a secure way to protect your online accounts.

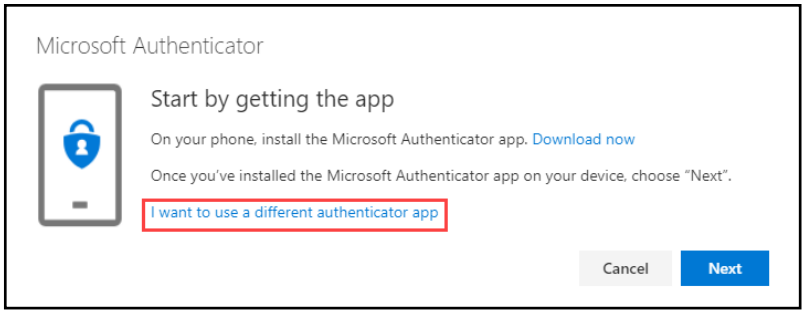
1. Go to the App Store/Play Store on your mobile device.
2. Search for Authy
3. Install the application.
4. Open Authy on your device
5. You need to enter a telephone number for verification purposes. Tap the Code area and search for the Country to which the phone number you want to enter is registered (+44 for United Kingdom).
6. When you have found the Country, tap it to select it.
7. Tap the Cellphone number area and enter the telephone number
8. In the email field, enter a contact email address which can be used to contact you should you ever lose access to your Twilio Authy Account. This does not have to be your Oxford email address
9. Click **OK**
10. The Account Verification screen will display. Choose whether to verify by SMS or Phone Call.
11. If you choose SMS, you will receive a text message with a 6-digit pin which you need to enter in the box on the screen
    If you choose Phone Call, you will receive an automated phone call. The automated voice will read out a 4-digit code, up to three times. End the phone call and enter the pin on the screen.
12. The Authy account screen will populate.
13. Go to the Microsoft Security Info page
14. You may be required to enter your SSO information and complete your MFA process
15. Click **Add Method**



16. Choose Authenticator App in the drop-down menu

17. Click **Add**

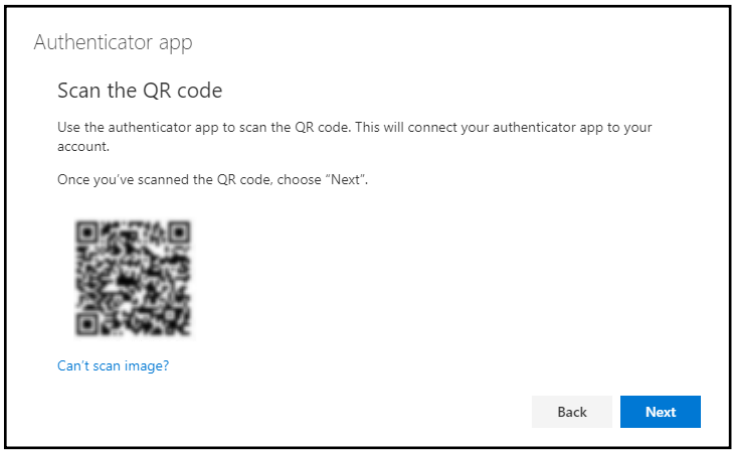
18. The Microsoft Authenticator dialogue box appears. Click **I want to use a different authenticator app**



19. Click **Next**

20. On your mobile device click **Scan QR Code**

21. Use your mobile device to scan the QR code. You may have to give permission for the app to access your camera



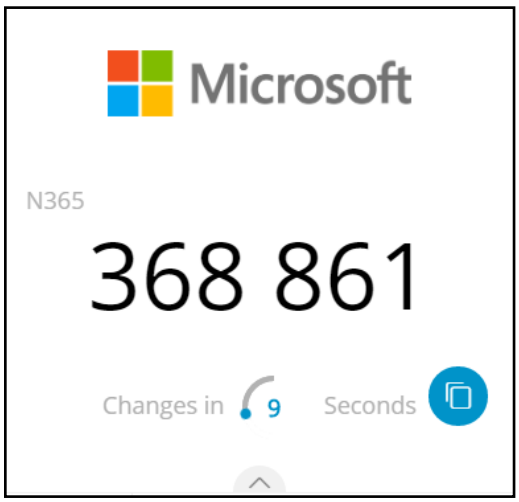
22. In the Authy app, the Secure Backups page will display in the app. Enter a password so that Authy can back up your account

23. Tap **Edit logo** if you want to change the logo for the account

24. Enter an Account Name (e.g. Nexus365)

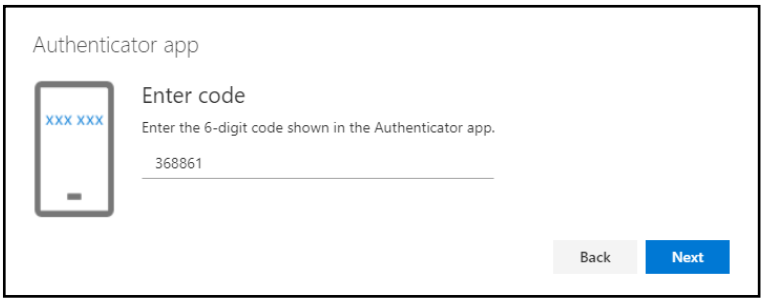
25. Click **Save**

26. The Authy app screen will show your chosen logo, account name and a 6-digit code which changes every 30 seconds.



27. Go back to the Microsoft Sign-Ins screen and click **Next**

28. Enter the 6-digit code



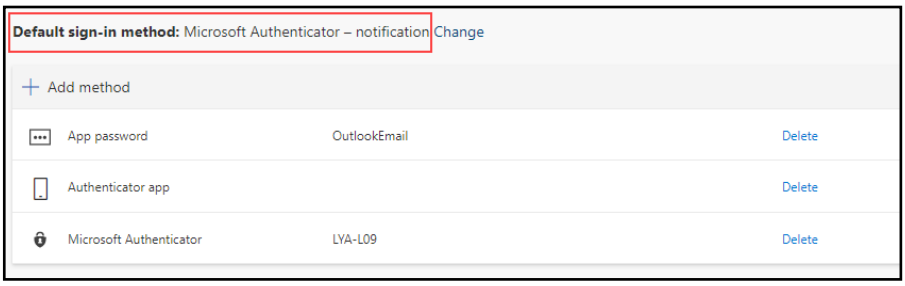
29. Click **Next**

30. Authenticator App will now appear in the list of registered methods.

31. If you have more than one multi-factor authentication method and you want to use the Authy app, you must select it as your default sign-in method.

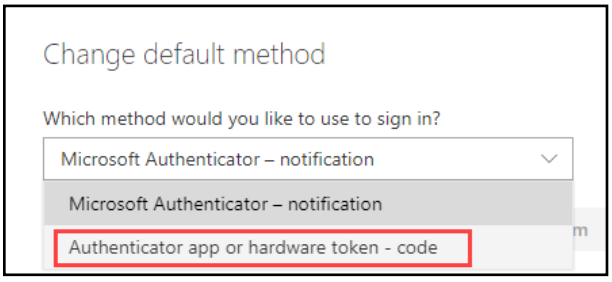
32. Go to the Microsoft Security Info page

33. At the top of the screen is the default sign-in method



34. Click **Change**

35. In the Change default method screen, use the drop-down menu to select Authenticator App or hardware token – code



36. Click **Confirm**

37. A green confirmation message will appear on the screen informing you that your default sign-in method has been changed.

    Note: Every installation of Authy on a desktop, laptop or mobile device will need to be set up as a separate authenticator in the Microsoft Security Info page.