Multi-Factor Authentication Project

Downloading and configuring the Authy desktop app

Multi-Factor Authentication Project

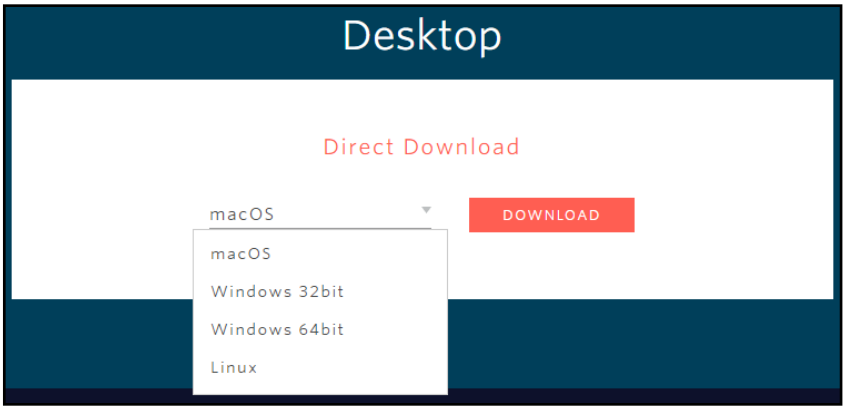
The Multi-Factor Authentication Project is responsible for providing all Oxford Single Sign-On users with additional verification methods when accessing materials which are currently protected by Single Sign-On. This guide will assist you in setting up an additional authentication factor for your Single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

This guide will show you how to set up the Authy desktop app. (It can also be installed on your mobile device) Authy is a free application which provides a secure way to protect your online accounts. There is no requirement for an administrative password to authorise the installation and it will not be found in the Oxford Applications installer either.

1. Use the link to download Authy

2. Scroll to the bottom to you can see the desktop box

3. Use the drop-down menu to pick the type of computer you have.



   If you are on a Windows machine and are unsure if it is 32bit or 64bit, search your computer for the control panel. When in the control panel click **System and Security,** then click **System.** The system type will be detailed on that page.

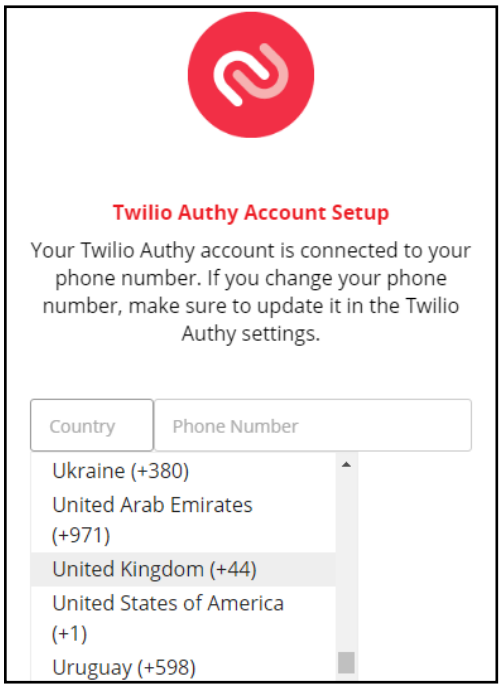
4. Click **Download**

5. Choose a place on your PC to save the download file. It may take a few minutes to download

6. Once the download is complete, open the application

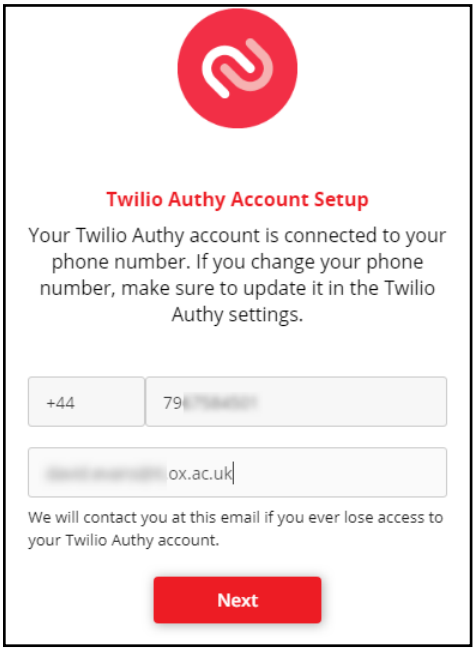
7. Click **Run**

8. In the Twilio Authy Account Setup screen select the country that your phone is registered in or enter the plus code if you know it



9. Enter your telephone number

10. 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.



11. Click **Next**

12. Choose whether to verify by SMS or Phone Call.

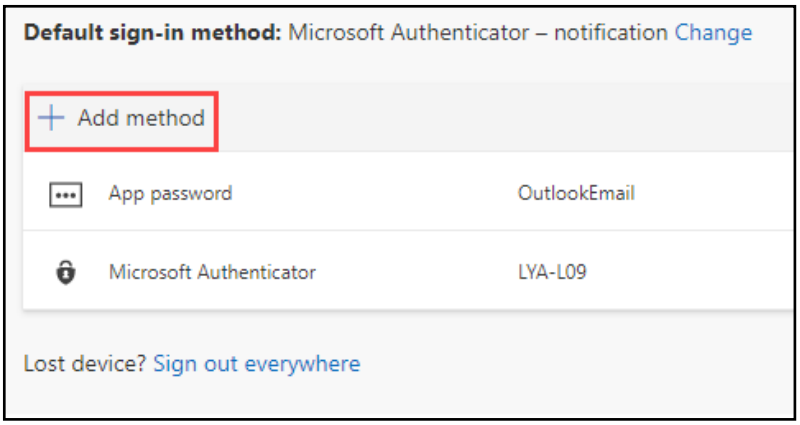
13. If you choose SMS, you will receive a text message with a 6-digit pin which you need to enter in the box on the screen
    If you choose Phone Call, you will receive an automated phone call. At the same time, a 2-digit pin will appear on the screen. Enter the pin on the phone's keypad.

14. The Authy account screen will populate.

15. Go to the Microsoft Security Info page

16. You may be required to enter your SSO information and complete your MFA process

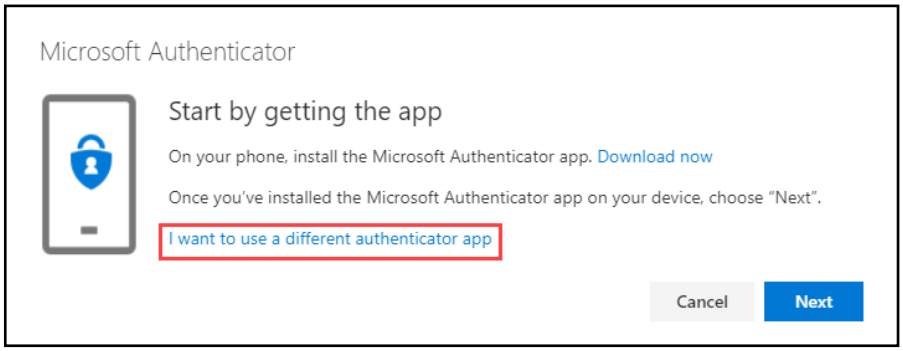
17. Click **Add Method**



18. Choose Authenticator App in the drop-down menu

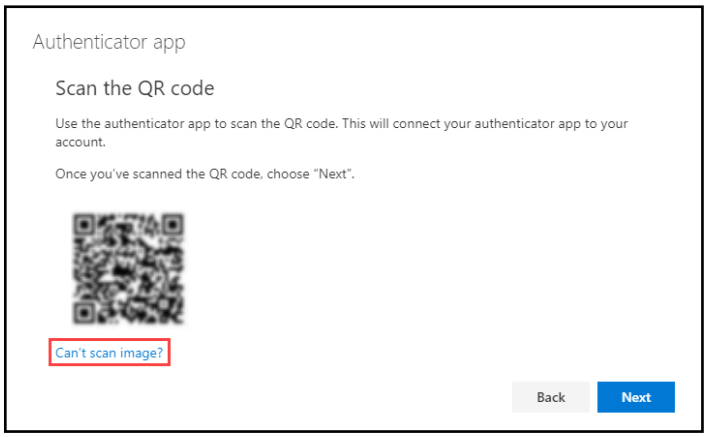
19. Click **Add**

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

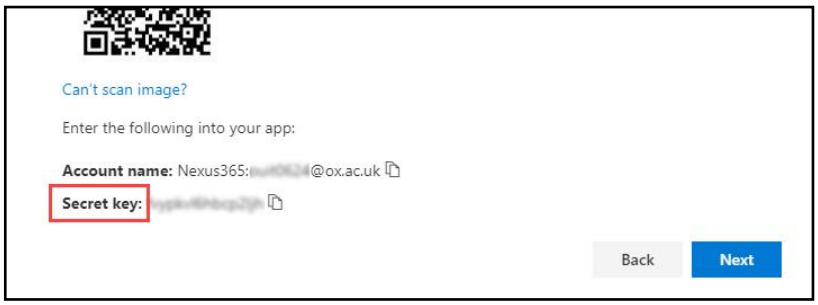


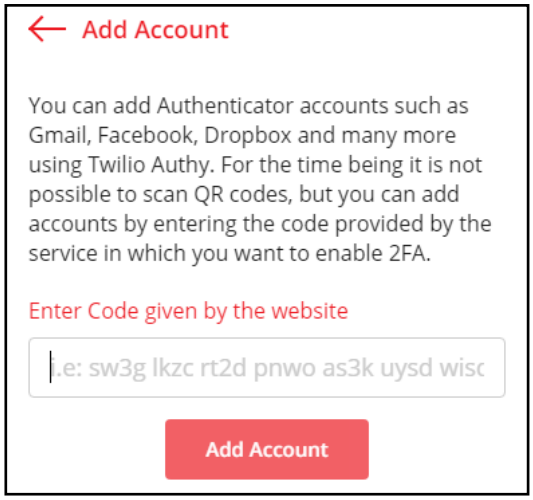
21. Click **Next**

22. Because you are adding a desktop application you cannot scan the QR code. Click **Can't scan image**



23. Enter the Secret key code into the Authy App Account page

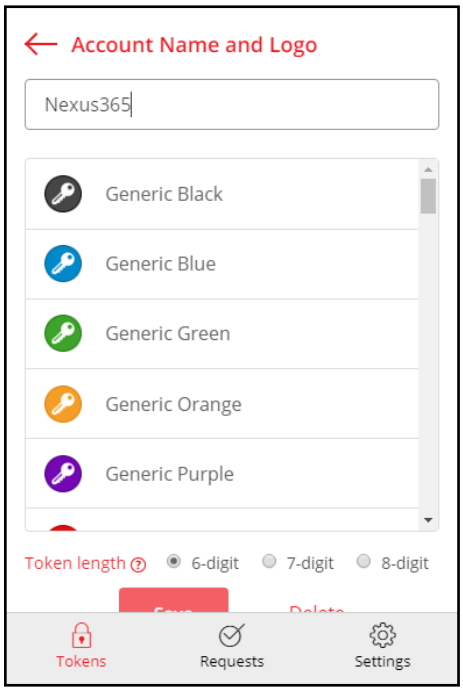




24. Click **Add Account**

25. In the Authy App, enter an Account Name (e.g. Nexus365)

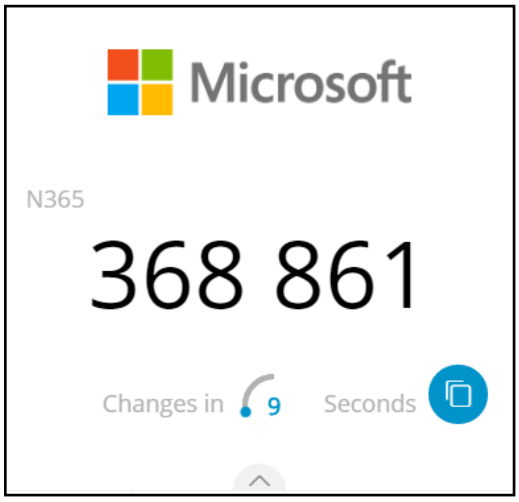
26. Select a logo to go with your account



27. Leave the Token length as 6-digit

28. Click **Save**

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

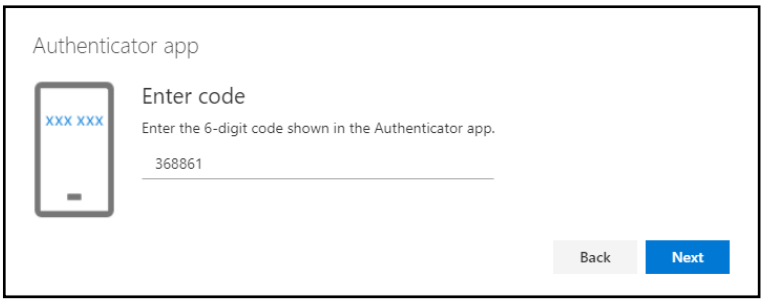


30. Go back to the Microsoft Sign-Ins screen and click **Next**

31. Enter the 6-digit code

Multi-Factor Authentication Project

Downloading and configuring the Authy desktop app



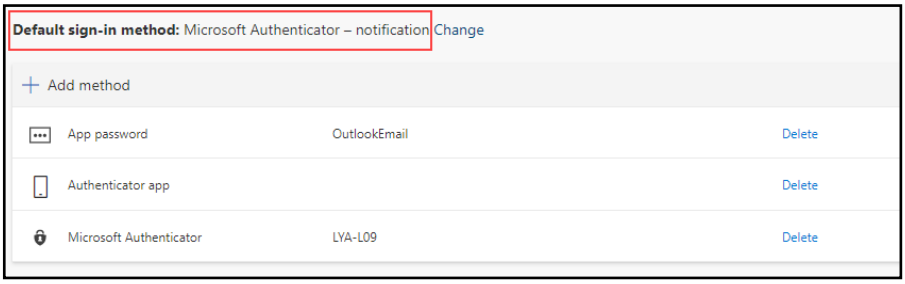
32. Click **Next**

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

34. 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.

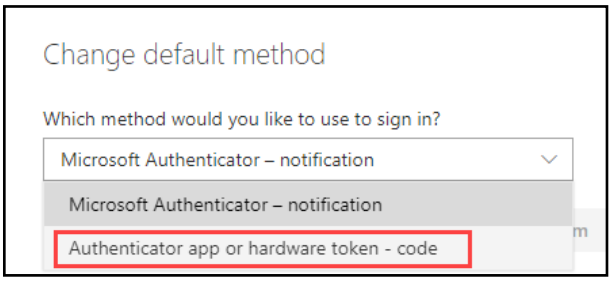
35. Go to the Microsoft Security Info page

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



37. Click **Change**

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



39. Click **Confirm**

40. 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.