



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.

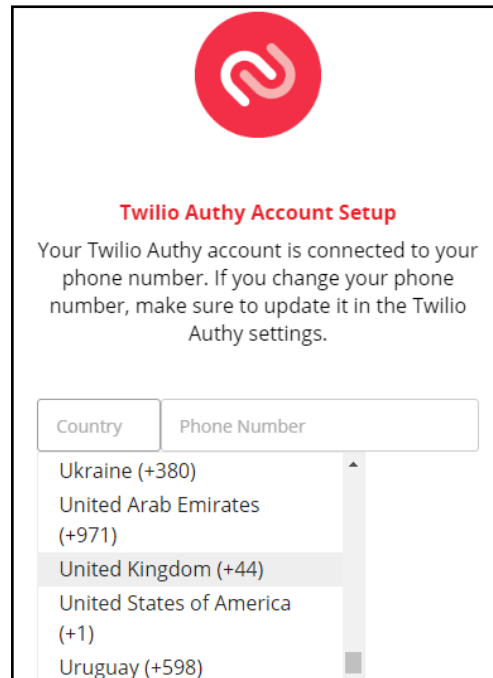
This guide will show you how to set up the Authy desktop app. (It can also be installed on your mobile device) Authy is a free application which provides a secure way to protect your online accounts. There is no requirement for an administrative password to authorise the installation and it will not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

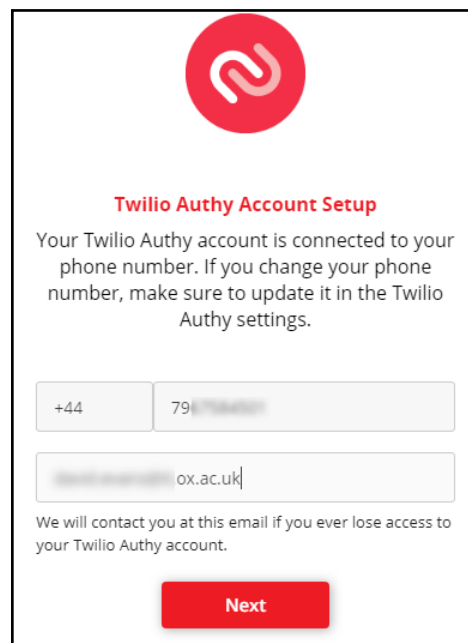
4. Click **Download**
5. Choose a place on your PC to save the download file. It may take a few minutes to download
6. Once the download is complete, open the application
7. Click **Run**
8. In the Twilio Authy Account Setup screen select the country that your phone is registered in or enter the plus code if you know it



The screenshot shows the Twilio Authy Account Setup screen. At the top is the Twilio logo (a red circle with a white 'S' shape). Below it is the heading "Twilio Authy Account Setup" in red. The text reads: "Your Twilio Authy account is connected to your phone number. If you change your phone number, make sure to update it in the Twilio Authy settings." Below this is a form with two input fields: "Country" and "Phone Number". The "Country" dropdown menu is open, showing a list of countries with their respective country codes: Ukraine (+380), United Arab Emirates (+971), United Kingdom (+44) (which is highlighted), United States of America (+1), and Uruguay (+598).

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.



The screenshot shows the Twilio Authy Account Setup screen. At the top is the Twilio logo (a red circle with a white 'S' shape). Below it is the heading "Twilio Authy Account Setup" in red. The text reads: "Your Twilio Authy account is connected to your phone number. If you change your phone number, make sure to update it in the Twilio Authy settings." Below this is a form with two input fields: "Country" and "Phone Number". The "Country" dropdown menu is open, showing a list of countries with their respective country codes: Ukraine (+380), United Arab Emirates (+971), United Kingdom (+44) (which is highlighted), United States of America (+1), and Uruguay (+598). Below the form is a text field for an email address, which contains "ox.ac.uk". Below the text field is a red button labeled "Next".

11. Click **Next**

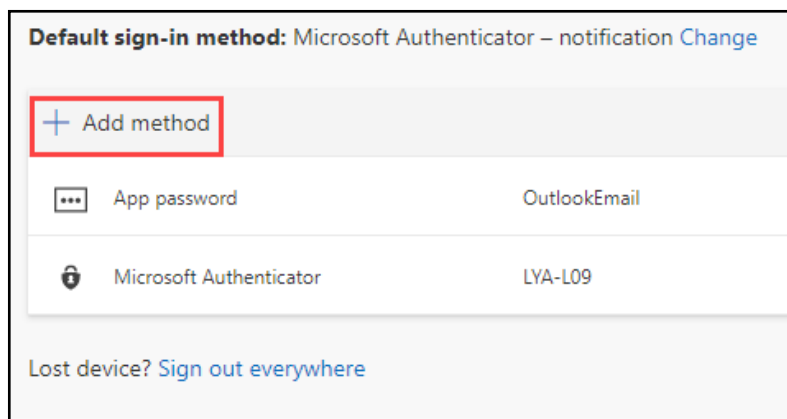
12. Choose whether to verify by SMS or Phone Call.

Multi-Factor Authentication Project

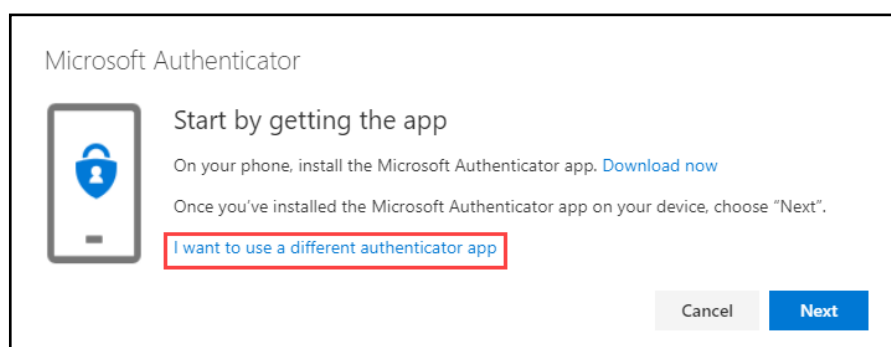
Downloading and configuring the Authy desktop app



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**



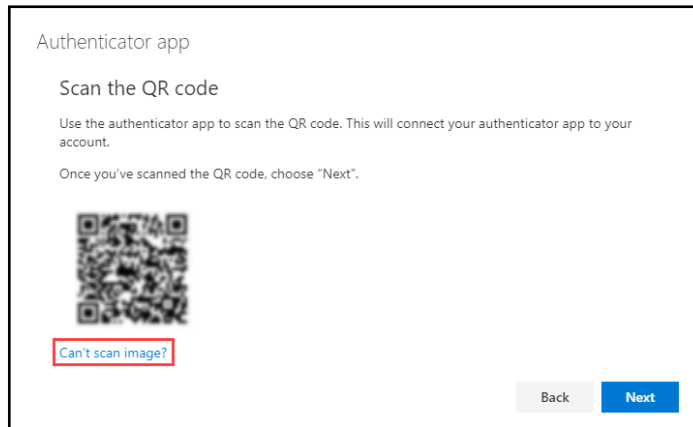
18. Choose Authenticator App in the drop-down menu
19. Click **Add**
20. The Microsoft Authenticator dialogue box appears. Click **I want to use a different authenticator app**



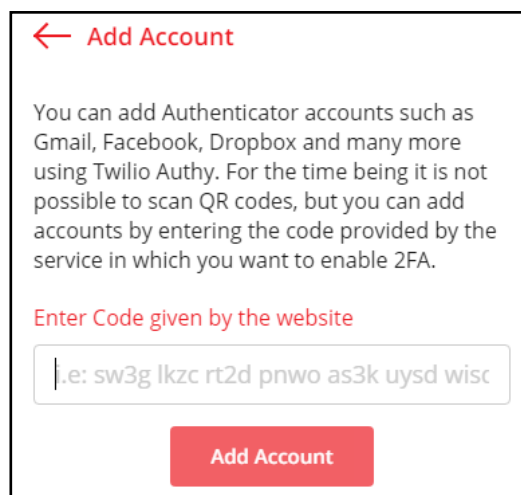
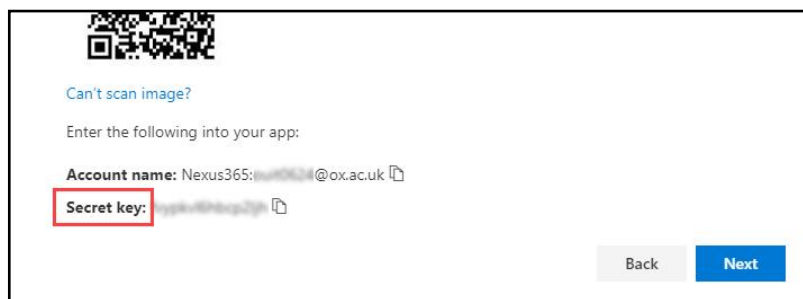
21. Click **Next**
22. Because you are adding a desktop application you cannot scan the QR code. Click **Can't scan image**

Multi-Factor Authentication Project

Downloading and configuring the Authy desktop app



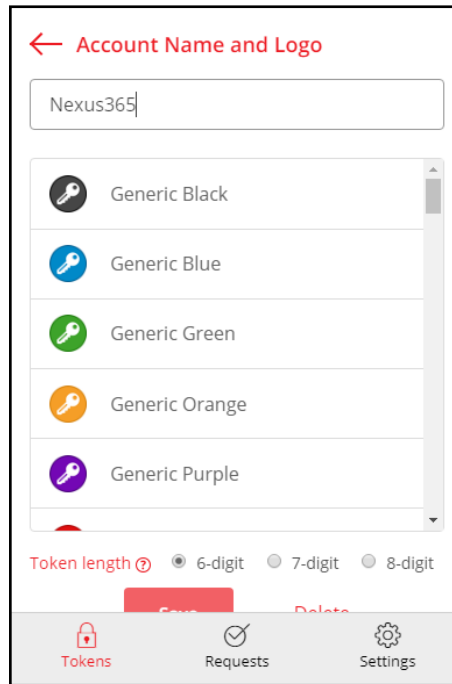
23. Enter the Secret key code into the Authy App Account page



24. Click **Add Account**

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

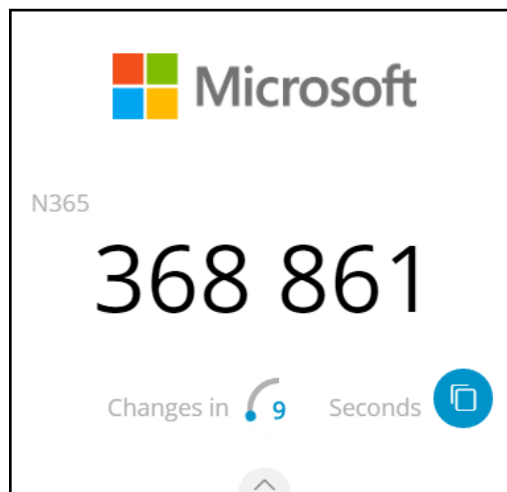
26. Select a logo to go with your account



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



Authenticator app

Enter code

Enter the 6-digit code shown in the Authenticator app.

368861

Back Next

A screenshot of a mobile application setup screen. On the left is a smartphone icon displaying 'XXX XXX'. To its right, the text 'Enter code' is followed by a sub-instruction: 'Enter the 6-digit code shown in the Authenticator app.' Below this, a text input field contains the number '368861'. At the bottom right, there are two buttons: a grey 'Back' button and a blue 'Next' button.

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

Default sign-in method: Microsoft Authenticator – notification [Change](#)

+ Add method

App password	OutlookEmail	Delete
Authenticator app		Delete
Microsoft Authenticator	LVA-L09	Delete

A screenshot of the Microsoft Security Info page. At the top, it shows 'Default sign-in method: Microsoft Authenticator – notification' with a 'Change' link. Below this is an 'Add method' button. A list of methods is shown in a table-like format with icons, names, and 'Delete' links. The methods listed are 'App password' (OutlookEmail), 'Authenticator app', and 'Microsoft Authenticator' (LVA-L09).

37. Click **Change**

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

Change default method

Which method would you like to use to sign in?

Microsoft Authenticator – notification

Microsoft Authenticator – notification

Authenticator app or hardware token - code

A screenshot of the 'Change default method' screen. It asks 'Which method would you like to use to sign in?'. A dropdown menu is open, showing 'Microsoft Authenticator – notification' as the current selection. Below it, 'Authenticator app or hardware token - code' is highlighted with a red box.

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.