Multi-Factor Authentication user guide
Contents
1. Introduction .................................................................................................................................... 3
    1.1. Further Information ................................................................................................................ 3
2. Implementation steps .................................................................................................................... 4
    Step one: Microsoft Outlook sign in .......................................................................................... 4
    Step two: More information required ........................................................................................ 5
    Step three: MFA enrolment ........................................................................................................ 5
    Step four: Download mobile app ............................................................................................... 6
    Step five: Setup mobile account ............................................................................................... 6
    Step six: Link Royal Holloway account and mobile app ........................................................... 7
    Step seven: Verify authentication is working ............................................................................. 8
    Step eight: Set-up a telephone number ....................................................................................... 9
    Step nine: Receive a code by telephone ...................................................................................... 9
3. Setting up MFA if you do not have a mobile device ................................................................. 11
4. Confirming security details after 60 days .................................................................................. 14
1. Introduction

Multi-Factor Authentication (MFA) is becoming ever-present in the modern world and for you as an end user, it is critical because it provides an added layer of security, helping prevent your data being stolen or your College account being hijacked.

So what is MFA?

If you’ve been prompted with a push notification on your phone after you’ve tried logging into a different application, for example online banking, you’ve experienced it. MFA requires you to provide an additional factor to verify your identity aside from entering a password.

While MFA alone will not mitigate all attacks, it is an enormous step towards decreasing the chance of your account being compromised and is part of the steps now being taken to improve cyber security here at Royal Holloway.

Once MFA is set up, it will only be noticeable if you are logging into your College account whilst off campus and/or from a laptop or desktop which is not your normal work machine.

If you never login from home and/or never use any machine other than your work one you will not be asked to authenticate because the system is confident that it is you logging in and not someone else.

1.1. Further Information

As part of the MFA rollout to all colleagues, there are a number of resources available to help you understand and complete the self-registration process.

Frequently asked questions (FAQs) and a video tutorial can be found on the staff intranet.

During the registration period (March 17 to March 30 inclusive) you can also get assistance from the IT MFA Support Centre, located in the Davison Building, from 9am-5pm.

You can also call the IT Service Desk on 01784 41 4321 or email them at itservicedesk@royalholloway.ac.uk.

Further information can be found on the staff intranet.
2. Implementation steps
Step one: Microsoft Outlook sign in
The first step is to open an internet browser window (any browser) and go to www.outlook.com.

You will then be presented with the below sign in screen:

Enter your Royal Holloway email address and click the ‘Next’ button.
Microsoft will automatically open another screen to enter your password.

Complete your login and click the ‘Sign In’ button.
Step two: More information required
Microsoft now requests you to provide further information. Click the ‘Next’ button.

![Microsoft Outlook message](image)

Step three: MFA enrolment
The first screen for enrolling for MFA is shown below. Follow the instructions on the screen. Step four shows you what to do on your mobile phone as part of this.

If you do not want to enrol at this point in time simply click the ‘Skip setup’ button at the bottom of the screen. Note you can skip completing enrolment for up to 14 days from Tuesday 17 March.

![Microsoft Authenticator setup](image)
Step four: Download mobile app
On your mobile phone go to the App Store (if on an Apple device) or the Play Store (if on an Android phone), and search for an app called Microsoft Authenticator. It will look like the image below:

Once you have downloaded the app onto your phone open it.

Step five: Setup mobile account
The app will then present you with the screen below on your phone. Click the ‘Add Account’ button.

Select "add account" then select "Work or school account":

---

---
Step six: Link Royal Holloway account and mobile app

In the web browser screen that you have open on your laptop or desktop from Step 4, click the ‘Next’ button. The screen below with a QR code (the black and white box at the bottom left) will be shown.

Using your phone, scan the QR code to sync the app to your Royal Holloway work Office 365 account.

The app itself will scan the QR code using the phone camera. If you have manually disabled access to the camera this will cause an issue so you will either need to enable it or get assistance from the MFA Support Centre in the Davison Building, from Tuesday 17 March, or by contacting the IT Service Desk.

Alternatively, if you cannot scan the image click the option ‘Can’t scan image?’ as shown in the screen shot above under the QR code. You will be presented with a 16 digit code to manually enter.

After scanning or entering the code, click the ‘Next’ button in the browser.

Your Royal Holloway account will then appear on your phone:
Step seven: Verify authentication is working
Microsoft will now test the completed configuration. The screen below will be shown in your internet web browser on your desktop or laptop. Select the box ‘Approve the notification we’re sending to your app’ and then click the ‘Next’ button.

Once next is clicked, Office 365 will send a test notification. This will arrive in your phone like this:

Click ‘Approve’ in your phone; the internet web browser screen subsequently provides confirmation. Click ‘Next’ to move on to Step 8:
Step eight: Set-up a telephone number

Setting up a personal telephone number is the next stage and is required so that you can manage the MFA configuration itself.

If you do not want to do this or do not have a mobile phone then you can select the option at the bottom of the screen ‘I want to set up a different method’. This will allow you to set up a personal email address as your second means of contact.

Enter your personal mobile number in the ‘Enter phone number’ field shown.

In the screenshot above the option for receiving a code via text is selected. If you would prefer to receive a phone call to your mobile you can select the radio button for ‘Call me’.

Once you have chosen the options you want click the ‘Next’ button.

Step nine: Receive a code by telephone

You will either receive a text on your mobile phone or a call or an email, depending on the choice you have made. Enter the code you have been given and click the ‘Next’ button.
Microsoft Office 365 will confirm that the code is correct:

Congratulations! You have completed setup for both use of the authentication app and a telephone number for either receipt of texts or phone calls:

Click the ‘Done’ button to continue to your email account.
3. Setting up MFA if you do not have a mobile device
On the standard screen (with skip buttons on bottom left) you will need to select the option "I want to setup a different method"

A pop up box will then appear to select from
Please select ‘email’:

You will then need to enter your personal email address and click next:

A six digit code will then be sent to your personal email address (example of which is below)
You will then need to enter this code and then click next:

Once you click next, the system will verify that this is correct and assign the personal email address to your profile:

You will then need to setup secret questions. There are nine to select from and five of those will need to be populated by you.

This cannot be used to approve MFA sign in but can be used to rest your password if it’s forgotten:
4. Confirming security details after 60 days

In order for Microsoft to ensure your security details are up-to-date you will be prompted every 60 days to verify them.

It’s important to keep your security information up to date. This is how you can prove who you are when you sign in or lose your password.

Step one: When you sign into your Office 365 staff account you will be asked to authenticate:

Step two: You will be advised that more information is required. Click 'Next' to continue:

Step three: Your current details will be shown which you will either need to confirm or update (if they have changed or you want to change them):
If the details are ok just click 'OK'. If you need or want to edit them click 'Edit info'. A screen will open allowing you to make changes.