How To Set up Multi-Factor Authentication-MFA

Multi-Factor Authentication-MFA

Multi-factor Authentication (MFA), also referred to as two factor authentication (2FA), adds an extra layer of security when accessing some online services. You may already use some form of MFA for online banking or to access your personal email account.

At Queen Mary, authentication requires a username and password. Some of our secure applications also require a two factor verification (2FA) when accessing outside the Queen Mary campus network (i.e. MYHR, Worktribe, AppsAnywher etc.). You can use your Mobile phone number, Authenticator app or personal Email as an authenticator method.

With MFA now setup you can access our secure applications and sites from off campus. You will need your Queen Mary username, not forgetting to add@qmul.ac.uk (abc123@qmul.ac.uk), your password and finally the verification code sent to either your mobile number, your personal email or the MS authenticator app.

1. On your computer open a web browser and go to http://sspr.qmul.ac.uk/

2. Enter your Queen Mary user name followed by '@qmul.ac.uk' then click Next.
3. Enter your password and click **Sign in**.

4. Once logged in you will see your SSPR profile. This is where you choose your method of authentication. Go to the **Security info** tab and Add method. **We recommend you use Phone**, this is easiest to configure and use.
Using Phone Method

5. If you would like to set up MFA using the Phone method, click on security info then select the Method Phone from the drop down list.

6. Click Add.
7. Select the Country and enter your mobile phone number. Select **Text me a code (or Call me)**, then follow the instructions to verify your phone number and complete the set up.

8. Click **Next**, you will receive verification code via text message on your mobile phone.

9. Enter the Verification code then select **Next**

10. Click on **Done** to complete the registration process.
• Using Authenticator App Method

11. If you would like to set up MFA using the Microsoft Authenticator app, select the method from the drop down list and click on Add.

12. Now Install the Authenticator App on your phone. For Apple devices go to the App Store and for Android devices go to the Play store, search Microsoft Authenticator.

13. Once the app is installed click Next.
14 Click **Next**.

15 Open your Authenticator app on your mobile phone then follow the instructions to scan the QR code then click on **Next**.
On your mobile or tablet, approve the **Sign-in** notification then click **Next** and follow the instructions to complete the set up using the Authenticator app.

The app is now configured. You have secure access to all our MFA activated services e.g. MYHR, Worktribe, Power BI, AppsAnywhere, VDI Pilot PC.

This second factor authentication token is stored throughout your session, you should only be prompted for it again if you:

- Sign out
- Re-launch your browser
- Completely close / stop the mobile app and re-open it

**Enrolment is Complete!**