The Multi-Factor Authentication (MFA) Project is responsible for providing all Oxford Single Sign-On (SSO) 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.

The project is adopting a phased approach to the second factor being switched on. You will receive communications in set intervals informing you of when you are due to go-live with your second factor.

When this is switched on, your access to existing applications will be suspended.

This guide will show you how to set up App Passwords. App Passwords can only be set up once your initial multi-factor authentication method has been set up, such as the authenticator app or a phone.

There is guidance on how to set this up on the multi-factor authentication project website.

An App Password is required in situations where you use apps or older devices that are incompatible with the multi-factor authentication method. The App Password proves to the system that you have multi-factor authentication set-up. When accessing an older application, such as Outlook 2013, you will be prompted for your multi-factor authentication details.

You must enter the App Password in place of your Single Sign-On password for the application or device you have created it for.

You can create up to 40 App Passwords. Each App Password is unique to an application.

Once this is done you will no longer be prompted for MFA for that specific application.

1. Following the successful set-up of a multi-factor authentication method go to the Microsoft Account page
2. Click Security Info
3. On the security info screen click Add Method
4. Click the drop-down menu and select App Password

5. Click Add

6. Enter an App Password name

7. Click Next
8. The App password screen will display

App password

App password was successfully created. Copy the password to clipboard and paste into your app. Then return here and choose 'Done'

Name:
Training

Password: 

Note: Keep this password in a safe place. It will not be shown again.

9. Click **Done** to complete the process

10. The App Password will now appear in your list of sign-in methods

11. **The App Password can now be entered for the relevant application or device instead of your Single Sign-On password**