LLOYD'S

Multi Factor Authentication (MFA)

Setup Guide

November 2022

What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) is an additional method of verification to your password enabling you to access Lloyd's Services (including MDC, SharePoint Online and SecureShare)

As the name suggests, Multi-Factor Authentication (MFA) requires two or more items to verify a user's identity and enable access to Lloyd's Applications. As well as your username and password, you will now be using the Microsoft Authenticator app to generate a random passcode.

Username & password **Authentication code via app** **Access**

1. Download and install the Authenticator app

Install the latest version of the **Microsoft Authenticator** app, based on your mobile operating system:

- **Android**. On your Android device, go to Google Play to download and install the *Microsoft Authenticator* app.

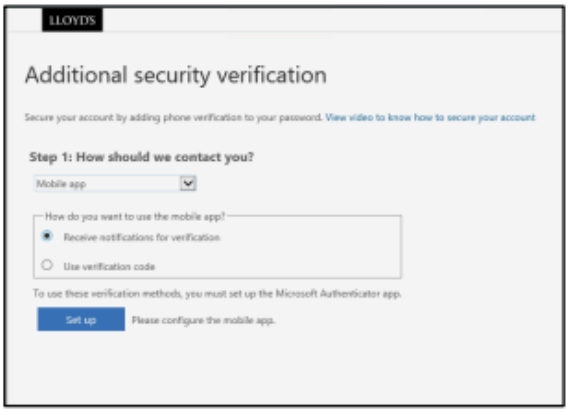
  Scan the QR code with your mobile phone to take you directly to the app download link

- **Apple iOS**. On your Apple iOS device, go to the App Store to download and install the *Microsoft Authenticator app*.

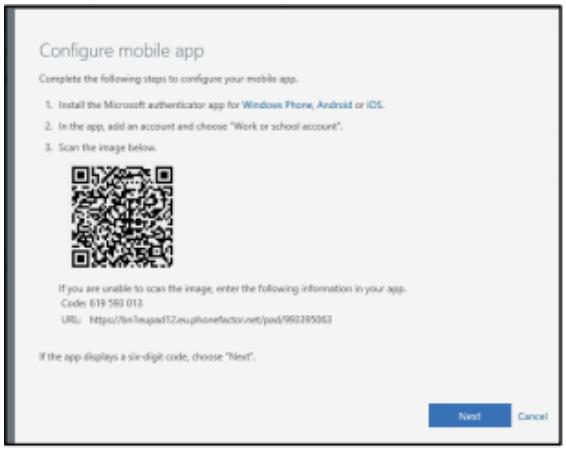
  Scan the QR code with your mobile phone to take you directly to the app download link.

2. MFA Enrolment

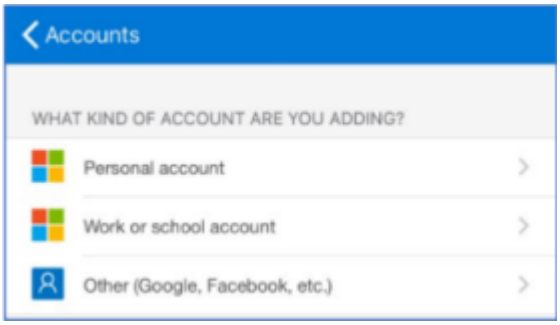
- Open your Internet Browser and browse to https://aka.ms/mfasetup
- Enter your registered username followed by selecting '**Next'**.
- Enter your password and select '**Next'**
- At this stage you will be presented with a screen asking for more information. Click ''**Next'**
- Select '**Receive notifications for verification'** and click **'Setup'**



- You will now be presented with a screen showing a QR code



- Open the Microsoft Authenticator app and select '**Add Account' or Scan QR code**. (note: if you are already using the Authenticator for another account please tap the + icon in the top right of the screen)
- Select the account type '**Other'** *(if you selected 'Add Account)*
- Select the option to 'Scan a QR code' and scan the QR code displayed on the screen with your mobile device.

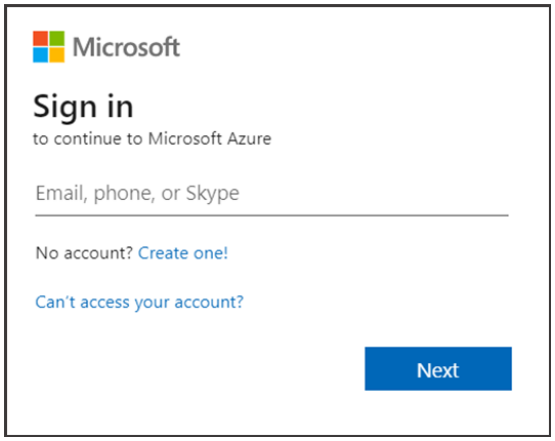


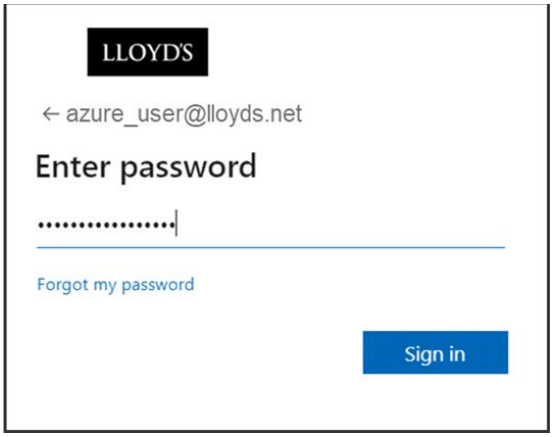
- Your account will then appear in the Accounts list within the Microsoft authenticator app.

3. Standard Login

Now you have enrolled with MFA, the steps below are the method to use going forward when accessing Lloyds Services

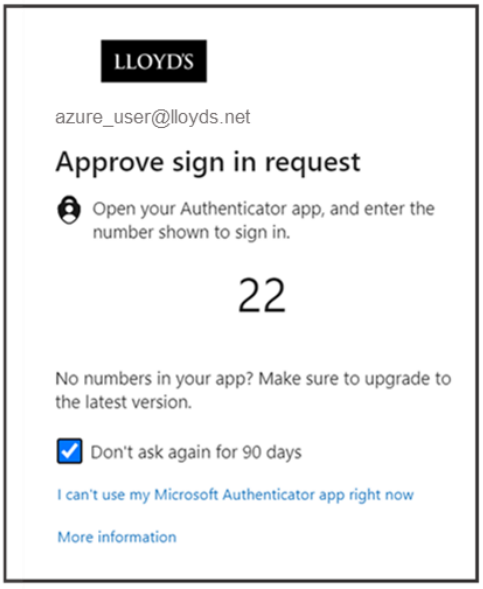
- Open browser and visit the site of the Azure AD Service you wish to access.
- Enter your registered username followed by selecting '**Next'**.





- Enter your password and select **'Sign in'.**

- You will now be presented with a 2-digit code that appears on your laptop/remote desktop. **Note:** Selecting the '*Don't ask again for 90 days'* tick box' will mean that unless your location, device you are using or service you are accessing changes or your password has changed, you will not be prompted to authenticate again for a 90-day period.



- The Microsoft Authenticator app will prompt you to enter the code into the app. Once entered and '**Yes'** is selected you can access the service. **Note:** Before selecting '**Yes'** confirm that the information detailed below is correct. Is your username, the app you are trying to access and location, correct? The location is a rough approximation and dependent on several factors.

- You will now be able to access the Lloyd's Service.

4. Re-name your Authenticator Connection *(Optional)*

Lloyd's recommend you re-name the saved account stored in the Authenticator app so that it can be easily identified if you are using multiple accounts. To do this please follow the below steps:

- Open the Authenticator app and tap onto the Lloyd's account.
- Tap onto the cog icon in the top right of the screen
- Tap onto the pen icon next to the current Account Name
- Please rename the connection to **LloydsServices**.

5. Using a hard token to authenticate (*Optional*)

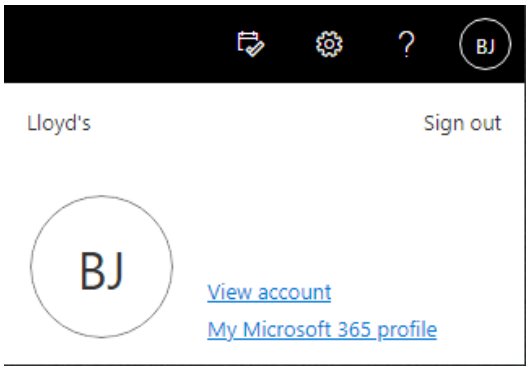
If you do wish to use an alternative to Microsoft Authenticator, Lloyd's can recommend YubiKey as a brand which has been tested successfully to access Lloyd's applications. There are also other brands which are available and can be found here. **Please note:** Lloyd's are not responsible for the procurement of hardware tokens.

Before you begin please ensure:

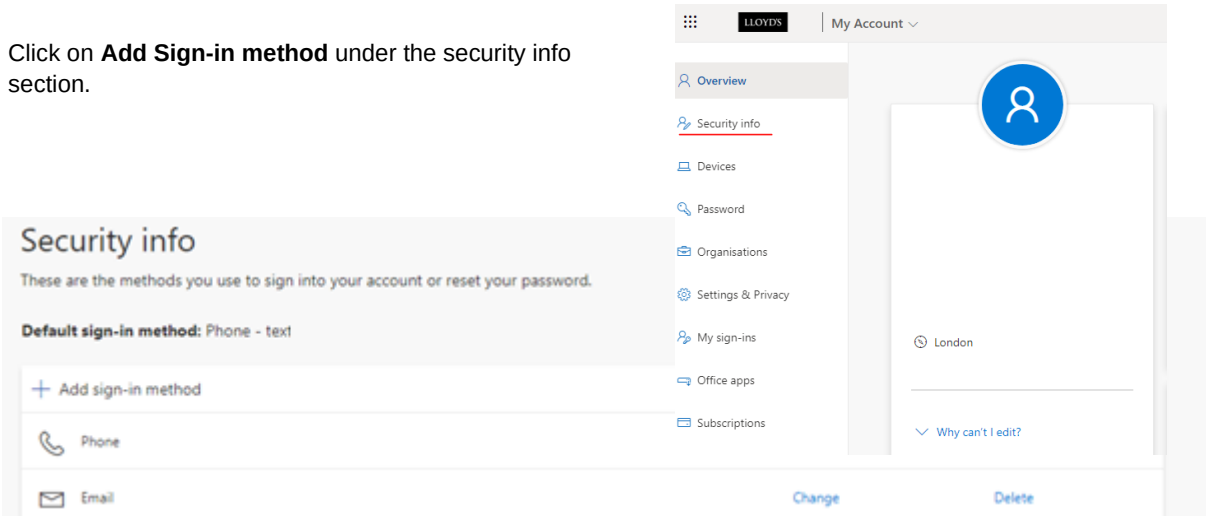
- The user account is set up in Azure Active Directory.
- You have a compatible hard token.

Register a hard token:

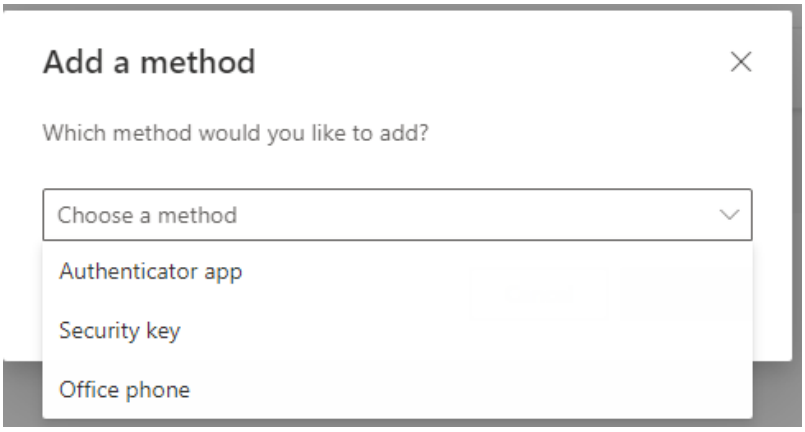
- Go to https://myprofile.microsoft.com and sign in with your registered account



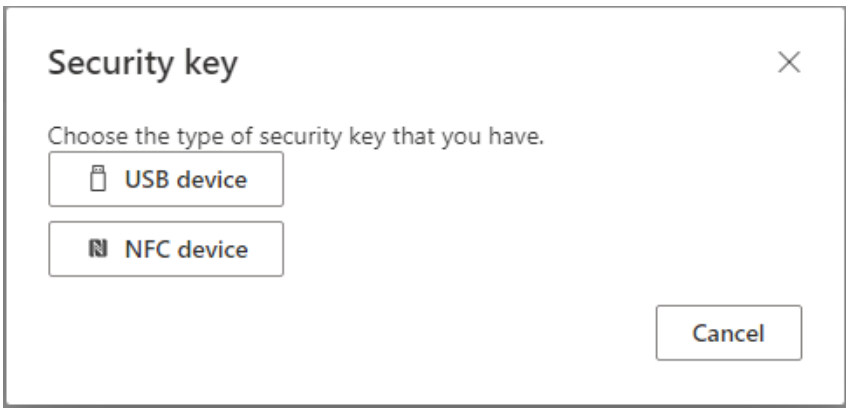
- Click on **Security Info** in the left-hand menu
- Click on **Add Sign-in method** under the security info section.



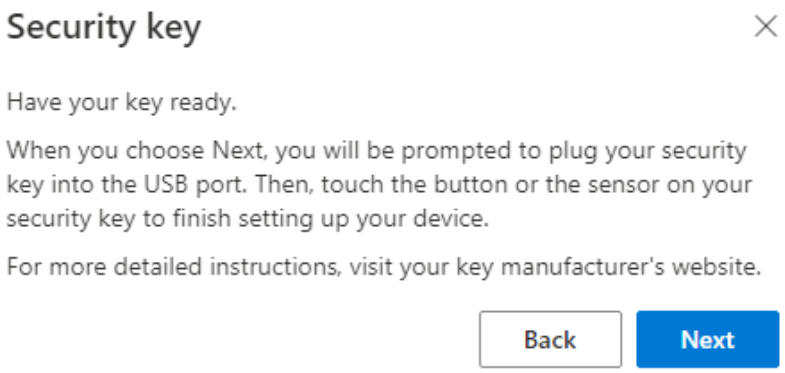
- Select **Security key** from the menu.



- Select **USB device** and click **next**

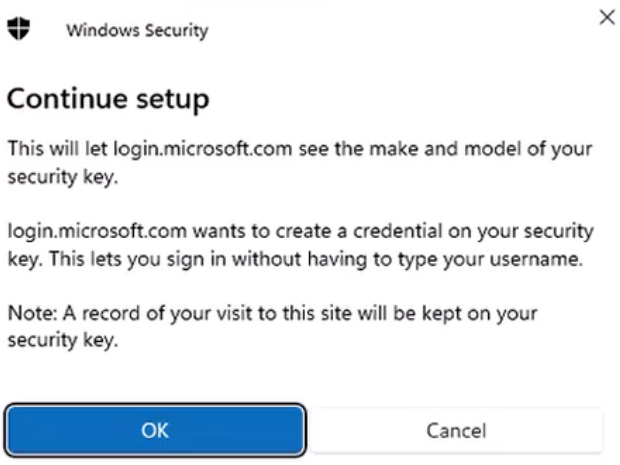


- Ensure you have your hard token ready and click **Next** on the "*Have your key ready"* message

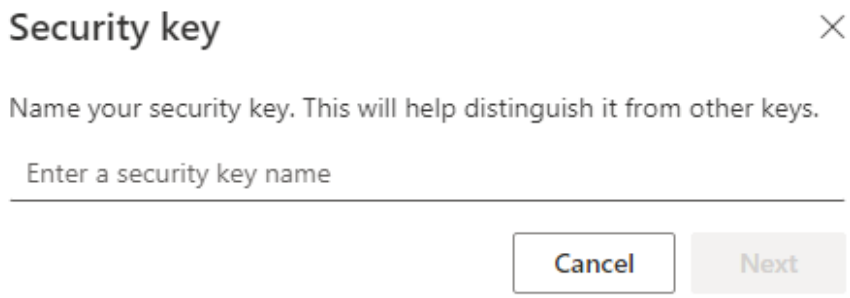


- Plug in your hard token to your devices USB drive.
- Check that the correct account name shows in the Security Key set up message and click **OK.**

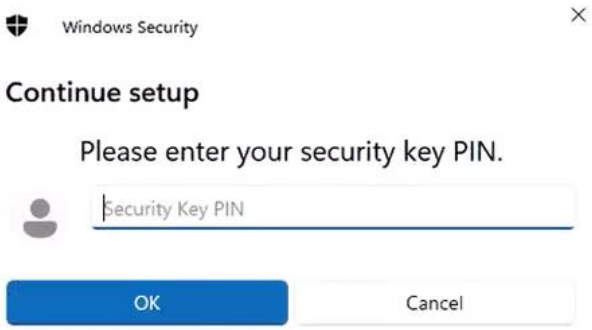
- Read and then click **OK** on the **Continue setup** pop-up.



- You will be prompted to enter a name for the key, for example “Primary Yubikey”, once entered click **Next** and **Done.**

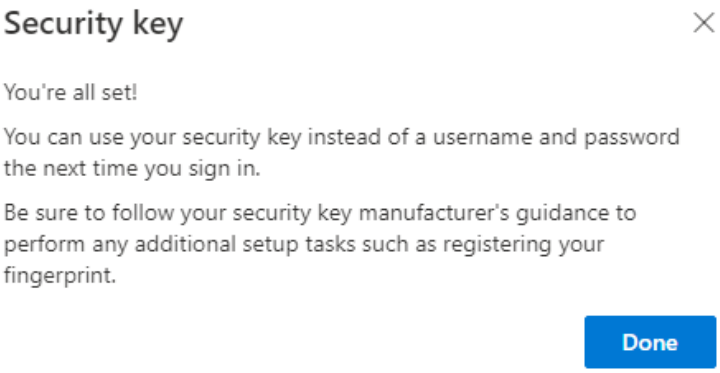


- Enter a **PIN** which will be used every time you use your hard token and click **OK**. You will need to remember this PIN so please use something that you will not forget.



- You will be prompted to touch your token. Lightly touch the front part of your key.

- You will get a message to say set up complete, click on **Done.**



- You have now successfully registered your token.