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 applications.

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.

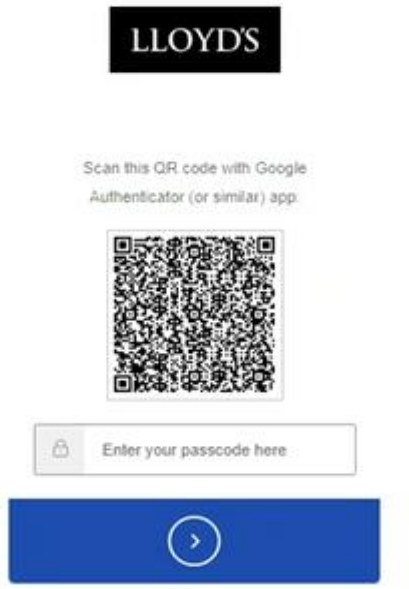
  Scan the QR code with your mobile phone to take you directly to the app download link

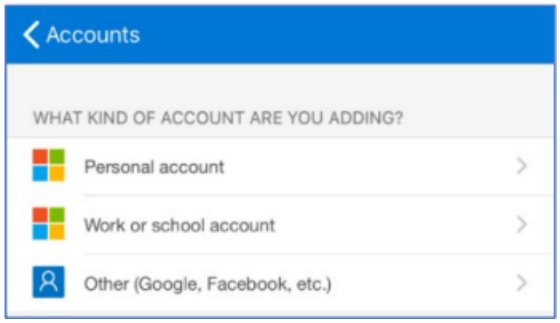
- **Apple iOS**. On your Apple iOS device, go to the App Store to download and install the *Microsoft Authenticator app*.

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

2. MFA Enrolment

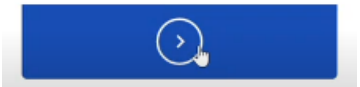
- Open your Internet Browser and visit the site of the Lloyd's Application you wish to access
- Enter your registered username followed by selecting '**Next'**.
- Enter your password and select '**Next'**
- At this stage you will be presented with a QR code to enrol you into the MFA process.
- Open the Microsoft Authenticator app and select 'Add Account'. (*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'**





- This will then create a Lloyd's account entry into the Microsoft Authenticator app.
- Tap onto this to reveal a **One-time password code** (example of a code →)

- Then enter that code into the space provided and select the blue button



- You'll then be presented with a recovery code which you will need to take a note of and store somewhere secure. If in the event of your device being lost, stolen or upgraded you can use this code to log in as an alternative to the Authenticator app.

- Tick the box to confirm you have safely recorded this code. You will then be taken to the Lloyd's application you are accessing.

3. Standard Login

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

- Open your Internet Browser and visit the site of the Lloyd's Application you wish to access

- Enter your registered username followed by selecting '**Next'**.

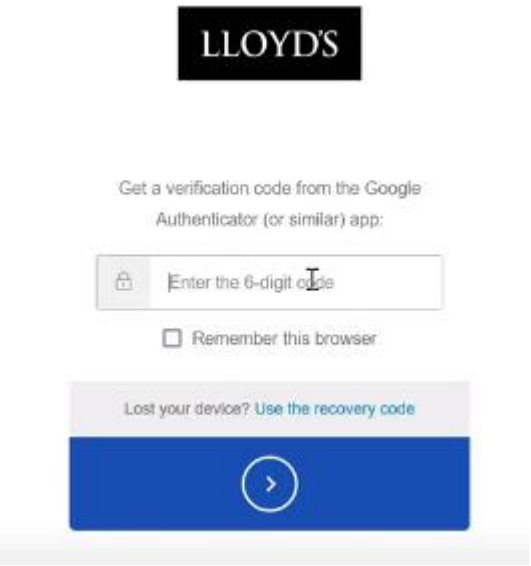
- Enter your password and select '**Next'**

- You will now be prompted to enter the 6 digit-code to authenticate you. Open up the Microsoft Authenticator app and select the Lloyd's account listed to reveal the rolling counter.

- Enter the current **6-digit code**

- Then select the blue next arrow.

(Note: If you have lost your device, or have a problem with your current device you can select the Use the recovery code open to enter one of your remembered recovery codes which were generated during the MFA enrolment steps)



- Then select the blue next arrow.

- You will be then taken to the application.

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 **LloydsApps**.

If you are also a user of Secure Share, MDC and SharePoint online, we recommend you additionally rename that account entry to **LloydsServices**

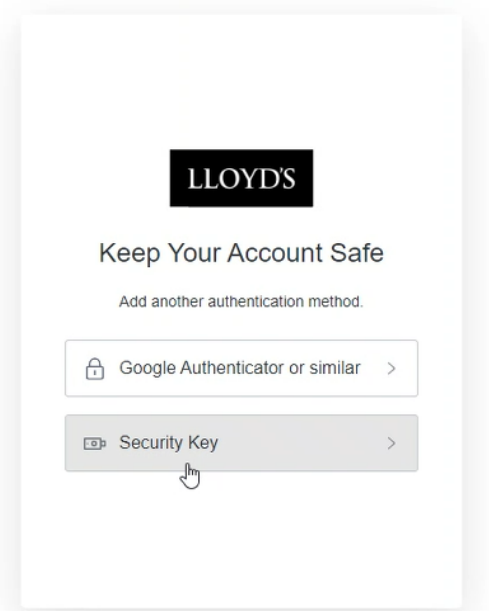
5. Using a hard token to authenticate (*Optional*)

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. **Please note:** Lloyd's are not responsible for the procurement of hardware tokens.

Register a Hard Token for MFA

Once this has been completed, please proceed with the following steps:

- Open your Internet Browser and visit the site of the Lloyd's Application you wish to access
- Enter your registered username followed by selecting '**Next'**.
- Enter your password and select '**Next'**
- You will now be presented with two options. Select the option **'Security Key'**
- You will then be taken to a second screen where you will be asked to Add your security key as an additional authentication factor.



- Depending on the type of token you are using you will need to insert the hard token into the usb port of the device you are using. Then select **'Use Security key'.**
- You will then be prompted to **create a pin number** for the security key. (**Please note**: you will only need to do this once)
- You should then be prompted to touch your security key *(model dependant)*
- Once your token has been detected you will be asked to name your key.
- Click **Continue** and copy the recovery code to a safe location.
- You have now successfully registered.

6. Logging in with hard token

- Now you have enrolled, the steps below are the method to use going forward when accessing Lloyds Applications.
- Open your Internet Browser and visit the site of the Lloyd's Application you wish to access
- Enter your registered username followed by selecting '**Next'**.
- Enter your password and select '**Next'**
- Select **'Use Security key'** (ensure the key is plugged into your device)
- Enter the **pin** you set during the registration process, and you will then be logged into the application.