

Multi Factor Authentication (MFA)

Setup Guide

November 2022

What is Multi-Factor Authentication (MFA)?

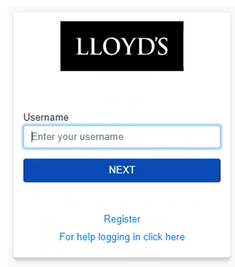
Multi-Factor Authentication (MFA) is an additional method of verification to your password enabling you to access Lloyd's Services (including MDC, SharePoint Online and SecureShare)

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



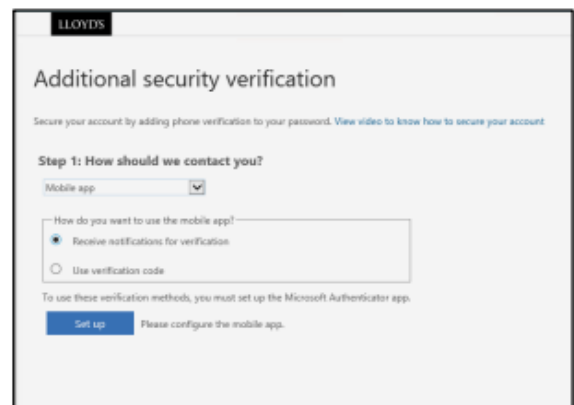
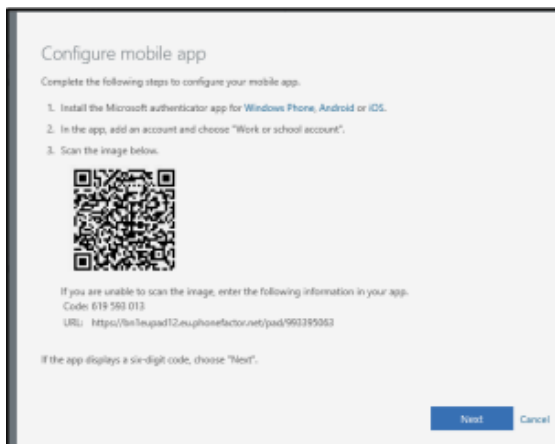
- **Apple iOS.** On your Apple iOS device, go to the App Store to download and install the *Microsoft Authenticator* app.

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

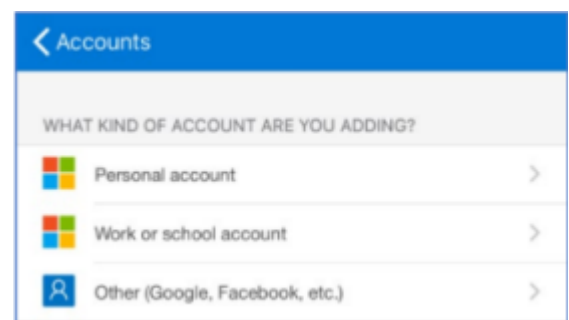


2. MFA Enrolment

- 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.

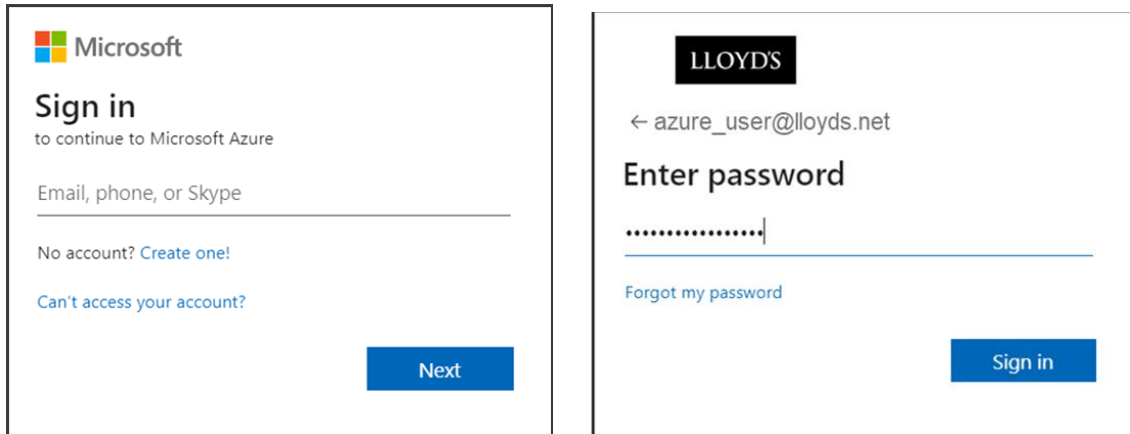


- Your account will then appear in the Accounts list within the Microsoft authenticator app.

3. Standard Login

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

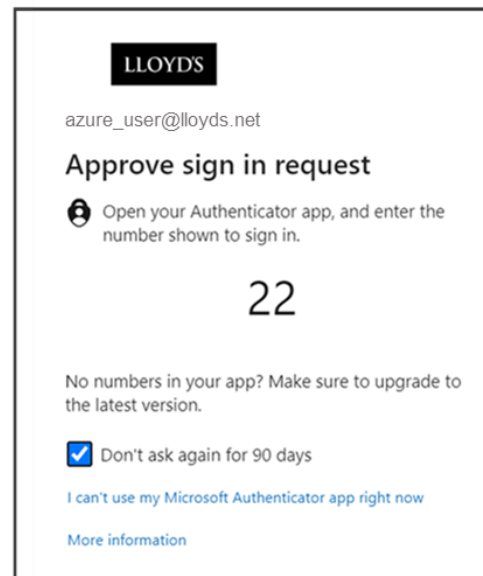
- Open browser and visit the site of the Azure AD Service you wish to access.
- Enter your registered username followed by selecting '**Next**'.



The first screenshot shows the Microsoft 'Sign in' page. It has the Microsoft logo at the top, followed by 'Sign in' and 'to continue to Microsoft Azure'. There is a text input field for 'Email, phone, or Skype'. Below the field are links for 'No account? Create one!' and 'Can't access your account?'. A blue 'Next' button is at the bottom right.

The second screenshot shows the LLOYDS 'Enter password' page. It has the LLOYDS logo at the top, followed by a back arrow and the email 'azure_user@lloyds.net'. Below is the heading 'Enter password' and a password input field with masked characters. There is a link for 'Forgot my password' and a blue 'Sign in' button at the bottom right.

- 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.



The screenshot shows the 'Approve sign in request' screen. It has the LLOYDS logo at the top, followed by the email 'azure_user@lloyds.net'. Below is the heading 'Approve sign in request' and an icon of a person. To the right of the icon is the text 'Open your Authenticator app, and enter the number shown to sign in.' Below this is a large display of the number '22'. At the bottom, there is a checkbox labeled 'Don't ask again for 90 days' which is checked. Below the checkbox are links for 'I can't use my Microsoft Authenticator app right now' and 'More information'.



The screenshot shows the Microsoft Authenticator app. It has the heading 'Are you trying to sign in?' and the email 'Lloyd's azure_user@lloyds.net'. Below is the text 'Enter the number shown to sign in.' and a map of the United Kingdom with a location pin. Below the map is a text input field for 'Enter number here' and two buttons: 'No, it's not me' and 'Yes'.

- 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**.

