

MFA Re-Authorization Guide

This guide outlines the steps needed to re-authorize your Multi-Factor Authentication (MFA) method for enhanced security.

1. Initial Login

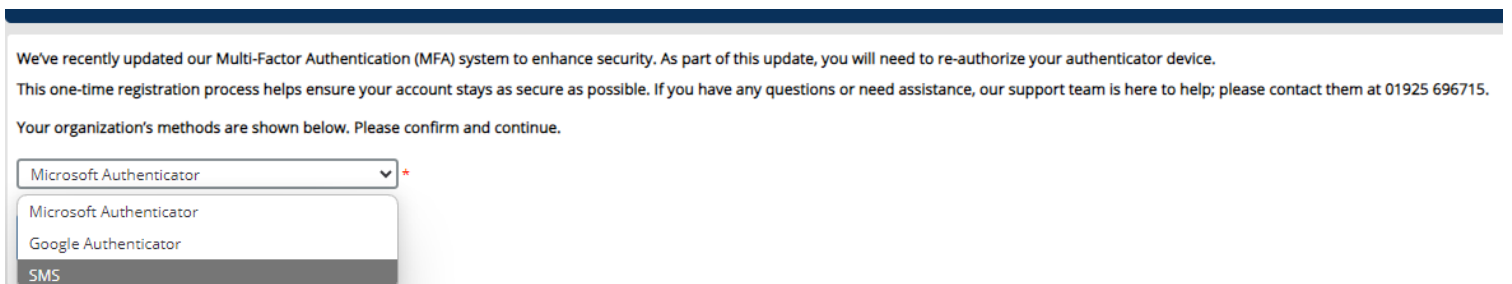
Begin by logging in with your username and password.



A screenshot of a web browser showing a login form. The Username field contains 'test2.mfa@yopmail.com' and the Password field contains several dots. To the right of the Password field is a 'Forgot password?' link and a 'Log In' button with a right-pointing arrow.

2. Select an Authentication Method

You will be prompted to choose one of the following authentication methods: **Google Authenticator**, **Microsoft Authenticator**, or **SMS Authentication**.

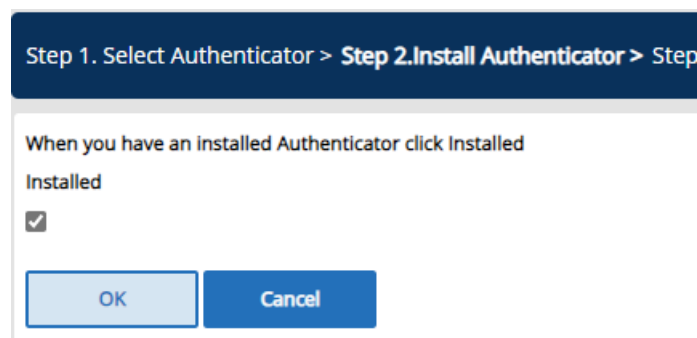


A screenshot of a re-authorization prompt dialog box. The text reads: 'We've recently updated our Multi-Factor Authentication (MFA) system to enhance security. As part of this update, you will need to re-authorize your authenticator device. This one-time registration process helps ensure your account stays as secure as possible. If you have any questions or need assistance, our support team is here to help; please contact them at 01925 696715. Your organization's methods are shown below. Please confirm and continue.' Below the text is a dropdown menu currently set to 'Microsoft Authenticator'. The dropdown is open, showing three options: 'Microsoft Authenticator', 'Google Authenticator', and 'SMS'.

Instructions for Microsoft & Google Authenticator

1. Confirm Authenticator Application Installation

If using the Microsoft or Google Authenticator method, confirm that the Authenticator app is installed on your device by ticking the checkbox, then click 'OK'.



A screenshot of a confirmation dialog box. At the top, a dark blue header bar contains the text 'Step 1. Select Authenticator > Step 2. Install Authenticator > Step 3. Confirm Authenticator Application Installation'. Below the header, the text reads: 'When you have an installed Authenticator click Installed'. Underneath, the word 'Installed' is followed by a checked checkbox. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

2. Scan QR Code

You will be prompted to either scan the QR code displayed on the screen or manually enter the code into your Microsoft Authenticator app.

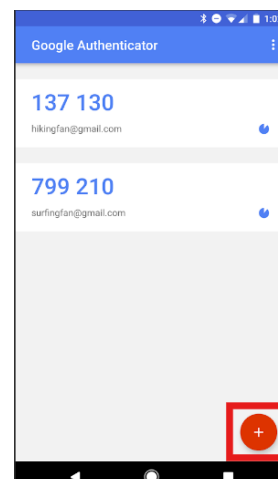
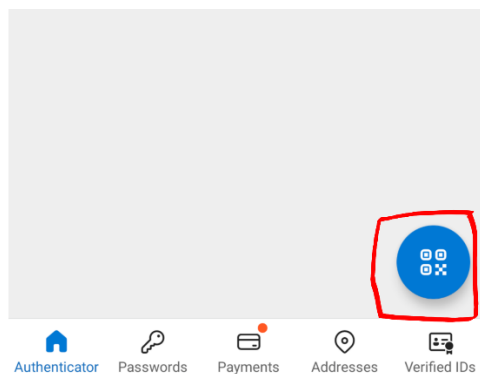
Please scan the QR code below with your Authenticator and click Continue when the Authenticator is registered



As an alternative you can enter this code manually into the Authenticator
MI3GCMJYMJSDMLLBME3DKLJUHBSTELLBHE2TKLJTG5RWKZRRG4YDSNZQGY



To scan, use the **Scan QR Code** option in your authenticator app, which appears as follows:



3. Verify QR Code

Once the QR code has been scanned, click 'OK' to proceed.



As an alternative you can enter this code manually into the Authenticator
MI3GCMJYMJSDMLLBME3DKLJUHBSTELLBHE2TKLJTG5RWKZRRG4YDSNZQGY



4. **Enter Authentication Code**

Enter the code displayed in your authenticator app into the provided field on the screen, then click 'Verify.'

Enter the code you just generated or were sent here and click Verify

5. **Completion Confirmation**

A confirmation screen will appear. Click 'Continue' to return to the login screen.

Thank you for Registering your Authenticator. You can now use it to log into OHIO. You will need it to access OHIO in the future but you should not need to Register an Authenticator again.

6. **Final Log-In**

Sign in again with your username and password, select your authentication method, and enter the code from your authenticator app. Click 'Log In' to complete the process.

Username Password [Forgot password?](#)

Authentication Code [Forgot Login Details](#)