# Provider Portal MFA (Multi-Factor Authentication)

## Login Flow Overview

When a user logs in with valid credentials, the system redirects them to the MFA screen where they must choose an authentication method (Email OTP or Authenticator App).

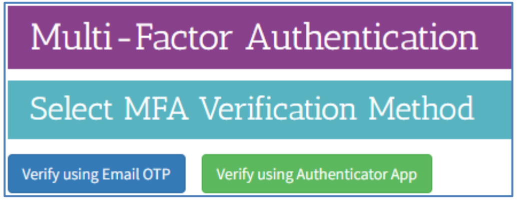
After completing setup, you will be prompted to enter a verification code each time you log in to the Inclusa Provider Portal. The code will be delivered using the method you select during multi-factor authentication setup.

## MFA with Email OTP (One-Time Password)

Step 1: Navigate to the Provider Portal login page.

Step 2: Enter valid username and password, then click Log in.

Step 3: On the MFA selection screen, choose 'Verify using Email OTP'.

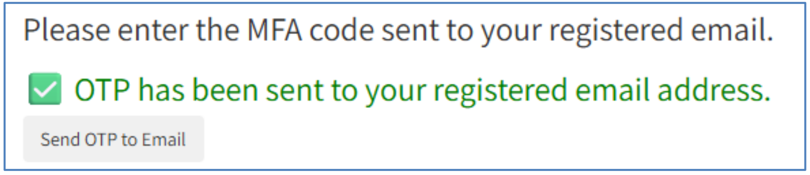


Multi-Factor Authentication

Select MFA Verification Method

Step 4: Select ‘Send OTP to Email’

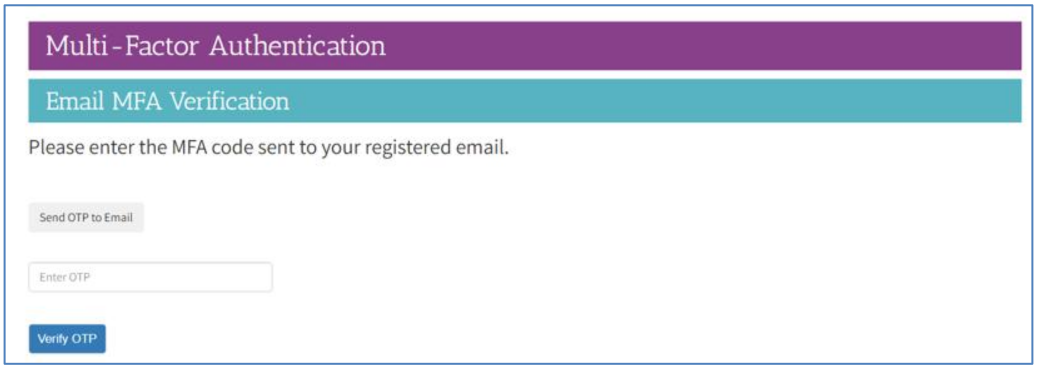
- ➢ System sends a 6-digit OTP to the registered email.



Please enter the MFA code sent to your registered email.

✓ OTP has been sent to your registered email address.

Step 5: Enter the OTP in the provided input field.



Multi-Factor Authentication

Email MFA Verification

Please enter the MFA code sent to your registered email.

Step 6: Click 'Verify OTP'.

- ➢ NOTE: the OTP is only valid for 5 minutes. If you do not enter the code within that time frame, select ‘Send OTP to Email’ to receive a new code.

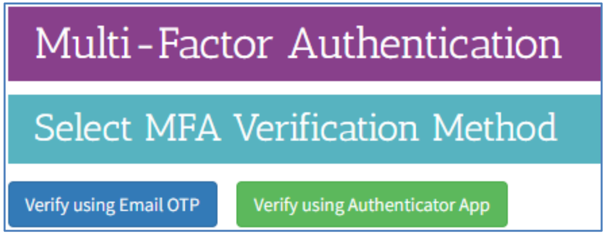
Users should be successfully authenticated and redirected to the dashboard.

## MFA with Authenticator App

Step 1: Navigate to the Provider Portal login page.

Step 2: Enter valid username and password, then click Log in.

Step 3: On the MFA screen, choose 'Verify using Authenticator App'.

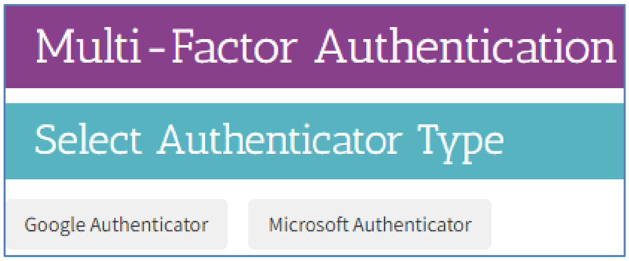


Multi-Factor Authentication

Select MFA Verification Method

Step 4: Select an authenticator app to use ‘Google’ or ‘Microsoft’,

- NOTE: if you do not have the app installed on your phone, download Microsoft Authenticator or Google Authenticator.

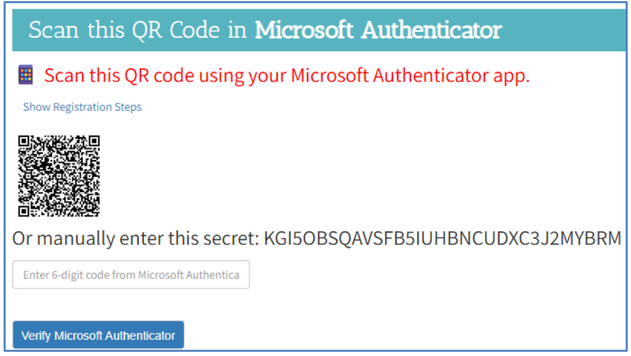


Multi-Factor Authentication

Select Authenticator Type

Step 5: Scan the displayed QR code using the authenticator app.

- NOTE: do not use the QR code in the images below, use the QR code that appears on the screen.



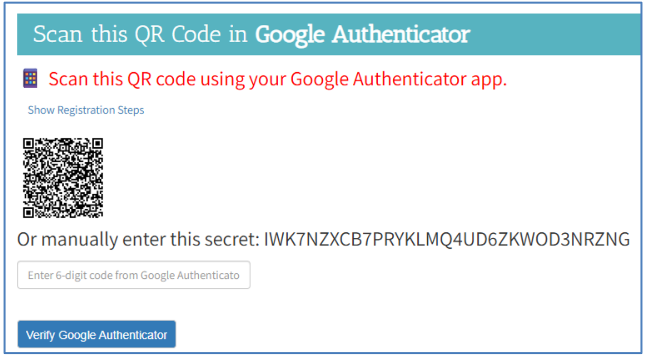
Scan this QR Code in **Microsoft Authenticator**

Scan this QR code using your Microsoft Authenticator app.

Show Registration Steps

Or manually enter this secret: KGI5OBSQAVSFB5IUHBNCUDXC3J2MYBRM

Enter 6-digit code from Microsoft Authentica



Scan this QR Code in **Google Authenticator**

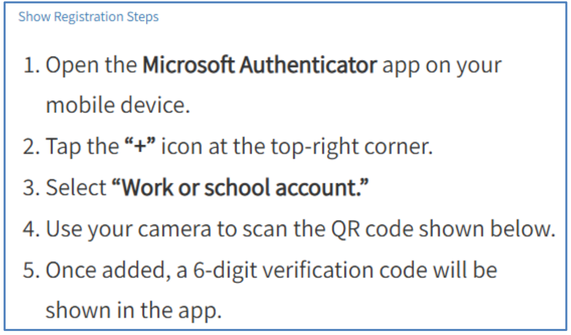
Scan this QR code using your Google Authenticator app.

Show Registration Steps

Or manually enter this secret: IWK7NZXCB7PRYKLMQ4UD6ZKWOD3NRZNG

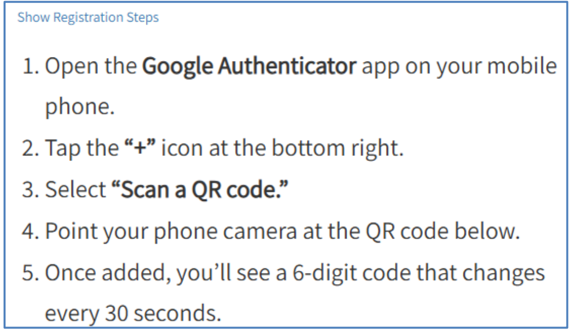
Enter 6-digit code from Google Authenticato

- For more information on how to set up the authentication, select ‘Show Registration Steps’



Show Registration Steps

1. Open the **Microsoft Authenticator** app on your mobile device.
2. Tap the **“+”** icon at the top-right corner.
3. Select **“Work or school account.”**
4. Use your camera to scan the QR code shown below.
5. Once added, a 6-digit verification code will be shown in the app.



Show Registration Steps

1. Open the **Google Authenticator** app on your mobile phone.
2. Tap the **“+”** icon at the bottom right.
3. Select **“Scan a QR code.”**
4. Point your phone camera at the QR code below.
5. Once added, you’ll see a 6-digit code that changes every 30 seconds.

Step 6: The app generates a 6-digit verification code.

Step 7: Enter the 6-digit code on the portal.

Step 8: Click 'Verify Microsoft Authenticator' or ‘Verify Google Authenticator’.

- Avoid hitting Enter, as it will require you to input the code again.

Users should be successfully authenticated and logged into the application.