



# MFA

## User Guide

NHS Arden & Greater East Midlands Health and Social Care Systems Support  
St John's House, 30 East Street, Leicester, LE1 6NB

W: [www.ardengemcsu.nhs.nuk](http://www.ardengemcsu.nhs.nuk)

## Review Process

A review of current SOPs should take place annually.

|              |  |
|--------------|--|
| Review Date: |  |
| Approved by: |  |
| Expiry Date: |  |

## Contents

|  |    |
|--|----|
| 1. Purpose .....   | 3  |
| 2. Installing the Google Authenticator on your phone ..... | 4  |
| 3. Set up Google Authenticator using a QR Code .....       | 6  |
| 4. Set-Up Google Authenticator in an App .....             | 9  |
| 1. Installing Microsoft Authenticator on your phone .....  | 14 |
| 2. Set up Microsoft Authenticator using a QR Code .....    | 16 |
| 3. Setting up MFA in an app.....                           | 18 |
| 4. Email Set-Up for MFA in an App .....                    | 23 |
| 5. SMS Authentication Set-Up .....                         | 25 |

## 1. Purpose

Multi-Factor Authentication will provide an additional layer of security to your login to applications that are authenticated through the OKTA application.

Normally you use your email address and password to log into your account. Multi-factor authentication (MFA) is an additional way of checking that it is really you when you log in to your account.


In addition to your email address and password, you will need to set up a second form of authentication, such as an authentication app on your mobile phone, or email. This second layer of security is designed to prevent anyone but you from accessing your account, even if they know your password.

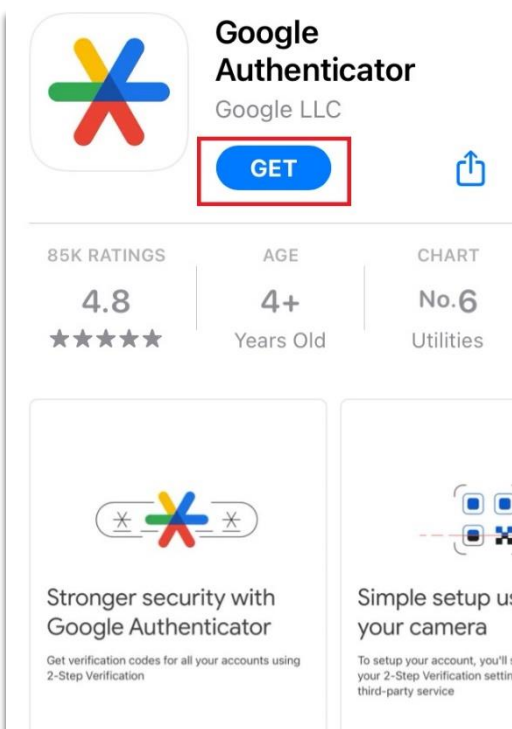
## 2. Installing the Google Authenticator on your phone

On your iPhone, launch the App Store



Search for Google Authenticator and download this to your phone. Click the Get button.

If you have previously downloaded the Authenticator app on a different device a cloud with a down facing arrow will show. Click this to download on this device. 

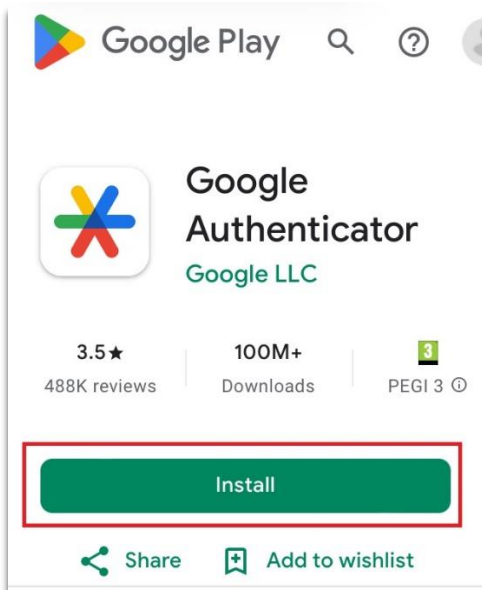


On Android devices, launch the Google Play Store

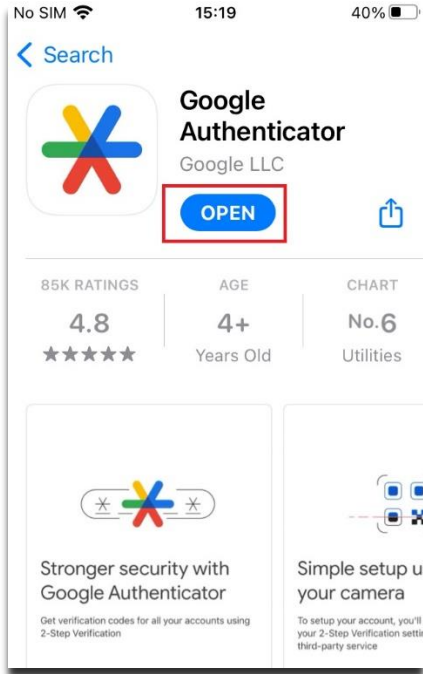


Search for Google Authenticator.

Click the install button.



Once downloaded, click the Open button.



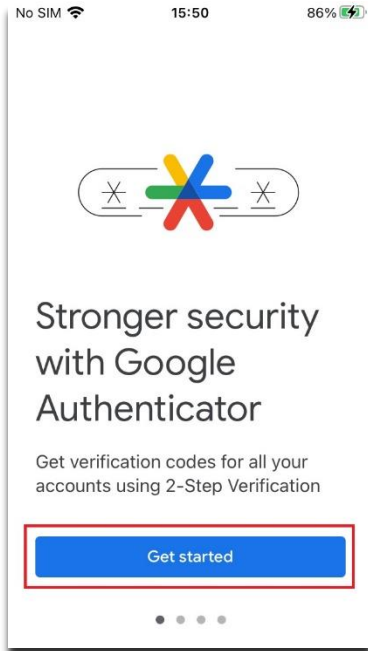
You can now close the authenticator.

### 3. Set up Google Authenticator using a QR Code

On your phone, launch the Google Authenticator

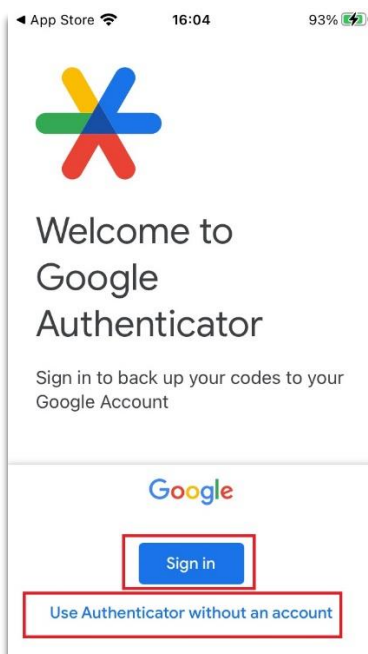


Then click Get Started

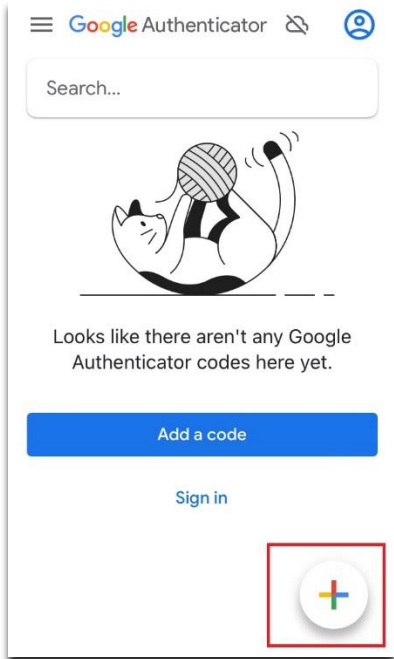


You will be asked to Sign in.

If you do not have a Google account, click the 'Use Authentication without an account' link.

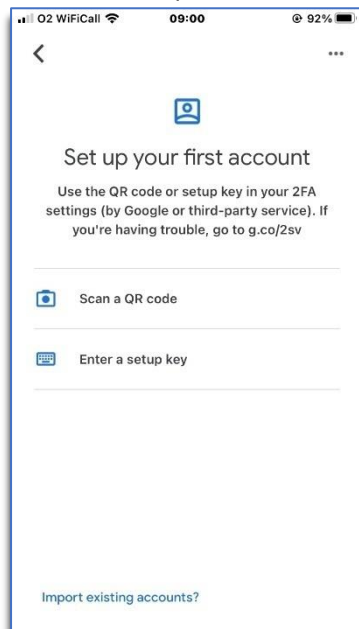


To set-up the MFA, select the Plus sign in the bottom right corner.



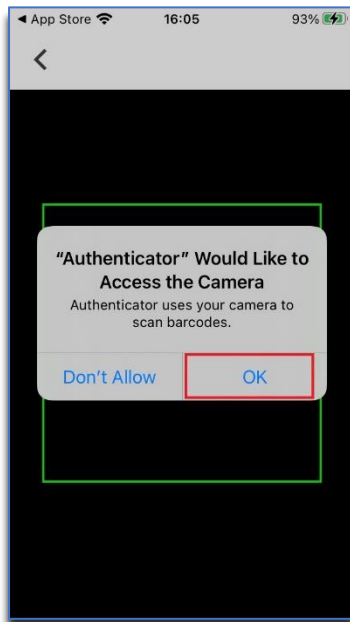
You will be presented with 2 options,  
'Scan a QR Code',  
'Enter a setup key',

Select **Scan a QR code**.





At this point, the rear camera on the phone will open. You may be prompted to give the Authenticator permission to use the camera at this point. Click OK.

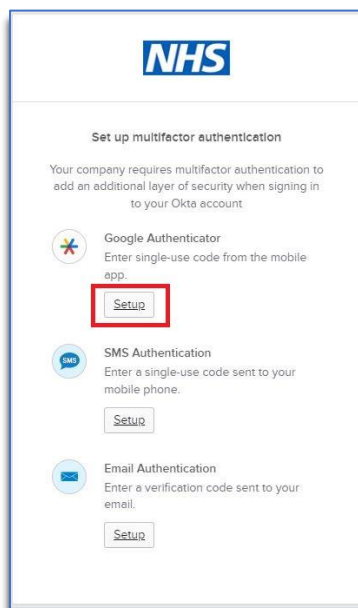


When you scan the QR code 6 Digits will show in the Authenticator app. These will change every 30 seconds.

## 4. Set-Up Google Authenticator in an App

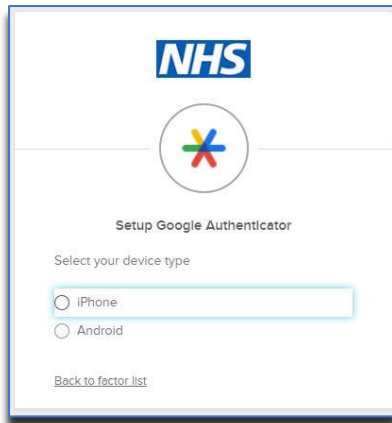
Logon to the required App in the web browser.

You will be prompted by a screen prompting you to install the Google Authenticator.

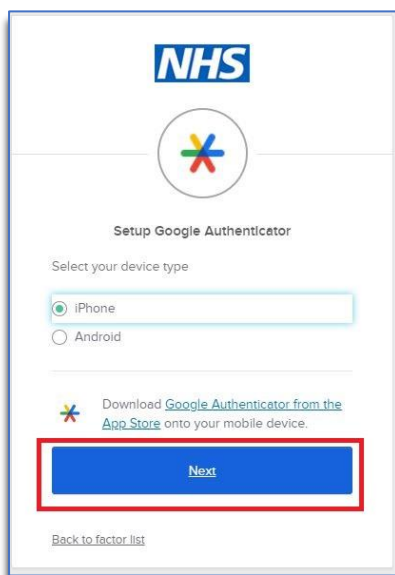


Below the Google Authenticator option, click the **Setup** button. **Do not select SMS Authentication.**

You should see a new page with the below in the centre.  
Select your phone type.



You will be presented with a new option.

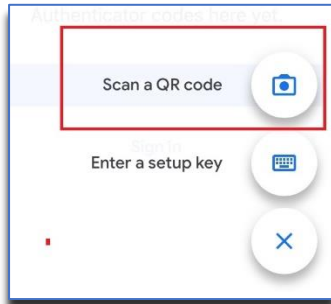


Click Next. You will be presented with a screen and a QR code to scan.

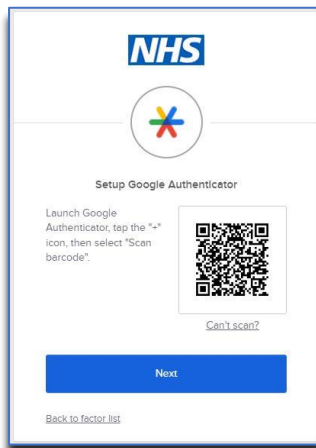
On your phone, launch the Google Authenticator and select the plus sign in the bottom right corner.



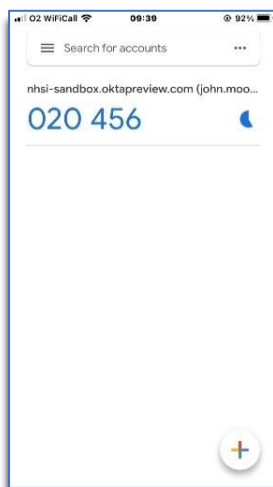
Select Scan a QR code from the next screen.



This will open the phone camera. Point the camera at the QR code onscreen.



Once the QR code has been captured, you will see an image like the below. This will present automatically. The 6 digits refresh every 30 seconds.



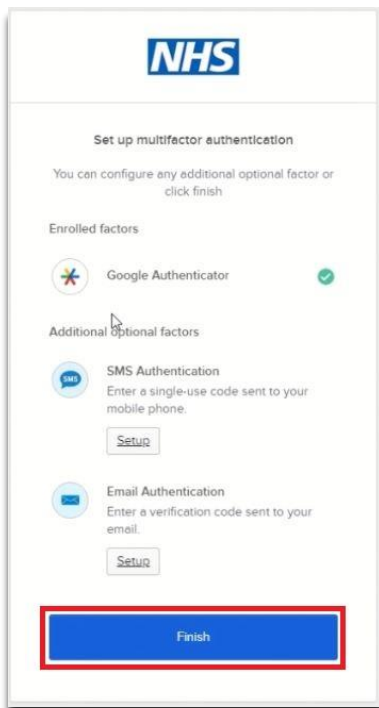
You will be asked to enter the series of 6 numbers in to the “Enter code” field. Then click verify.

You will see a small icon on the left of the screen – this is a timer of 30 seconds. You have 30 seconds to enter the code before these change to a new number (note that the number will change to red in the last 5 seconds.) It is OK to allow the numbers to change before you enter them if they are showing as RED when they appear on your screen.

This will effectively pair the Authenticator installed on your phone to your AGEM Apps / OKTA account.

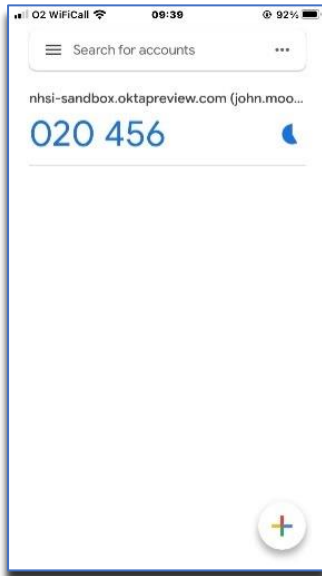


You will then see this screen. Click ‘Finish’ to complete the set up.



Set up is now complete.

Each time you log in from now on, you will be asked to add the numbers displayed in the App, onto the app log-in screen.




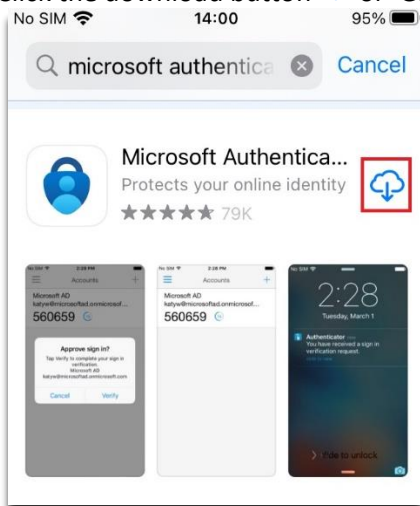
## 1. Installing Microsoft Authenticator on your phone

On your iPhone, launch the App Store



Search for Microsoft Authenticator and download this to your phone.

Click the download button  or 'GET'.

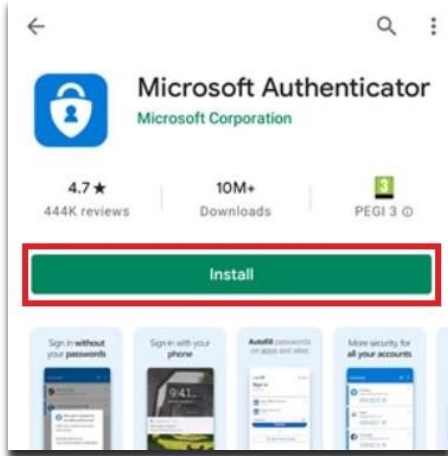


On your Android, launch the Google Play Store

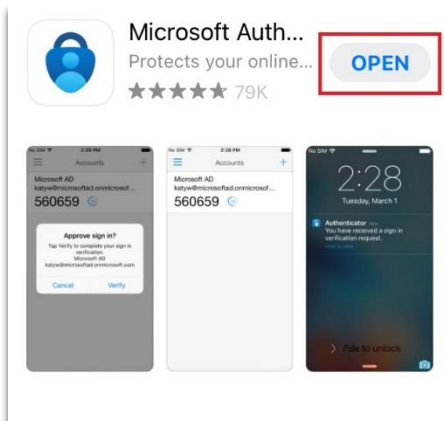


Search for 'Microsoft Authenticator'.

Select 'Install'.



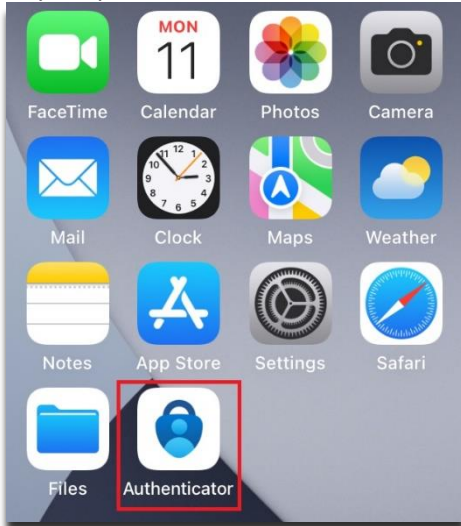
Once downloaded, click the Open button.



You can now close the authenticator.

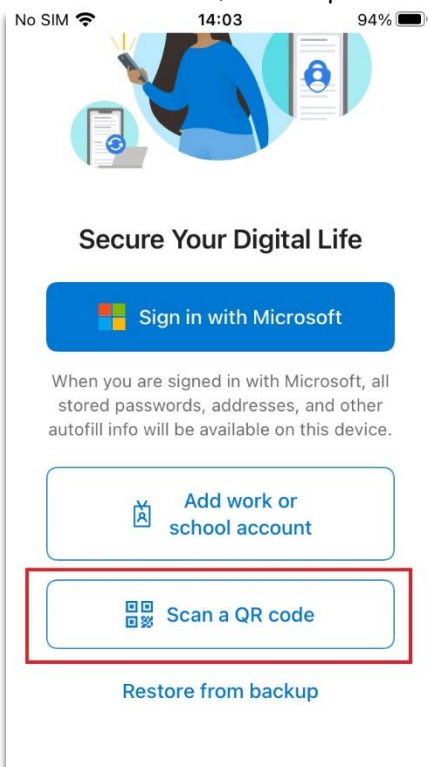
## 2. Set up Microsoft Authenticator using a QR Code

On your phone, launch the Microsoft Authenticator



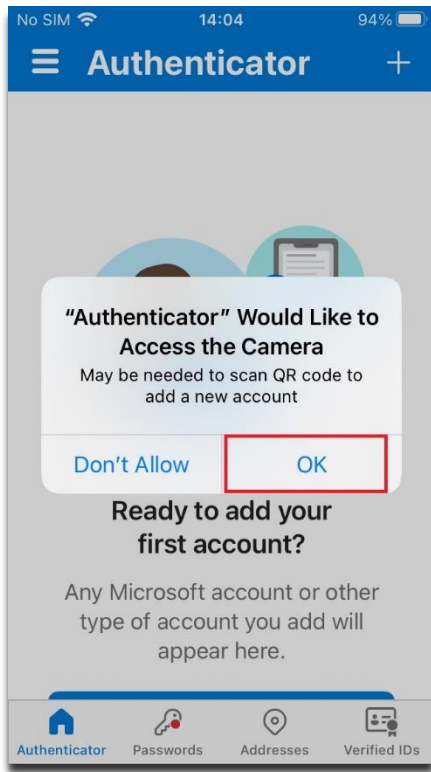
If you are asked, agree to the Terms.

Select the Scan a QR Code option.

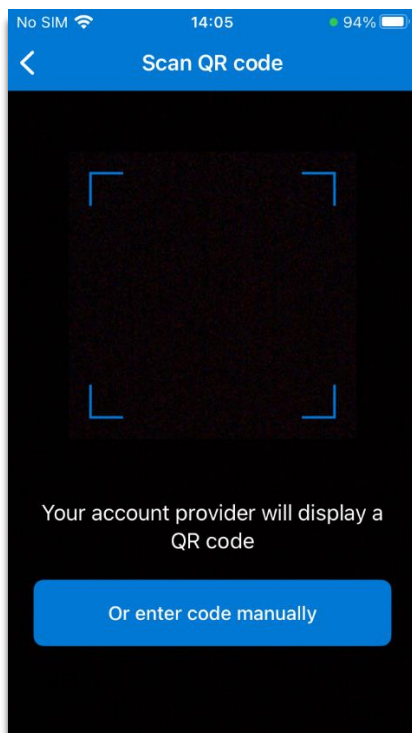




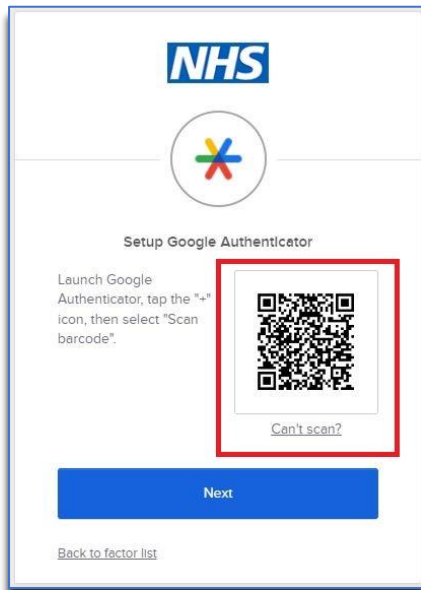
Select **Scan a QR code**. At this point, the rear camera on the phone will open. You may be prompted to give the Authenticator permission to use the camera at this point. Click OK.



This will open the phone camera.



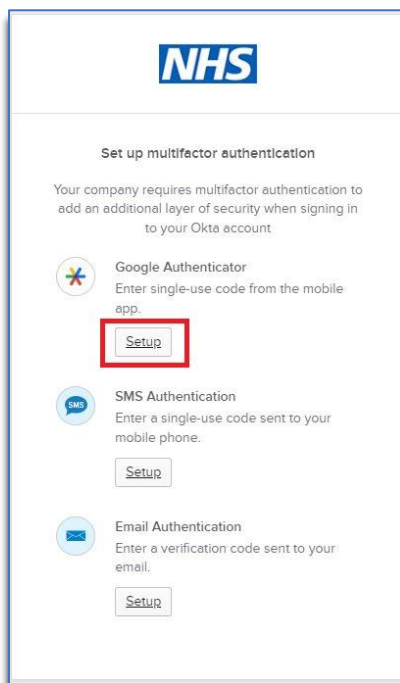
Point the camera at the QR code onscreen.



### 3. Setting up MFA in an app.

Logon to the required App in the web browser.

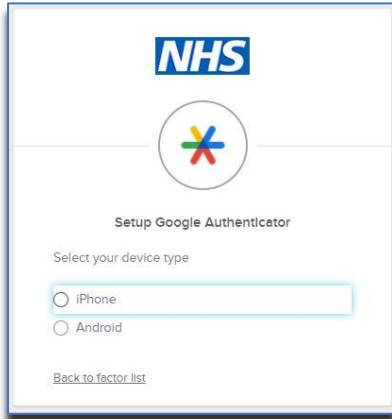
You will be prompted by a screen prompting you to install the Google Authenticator.



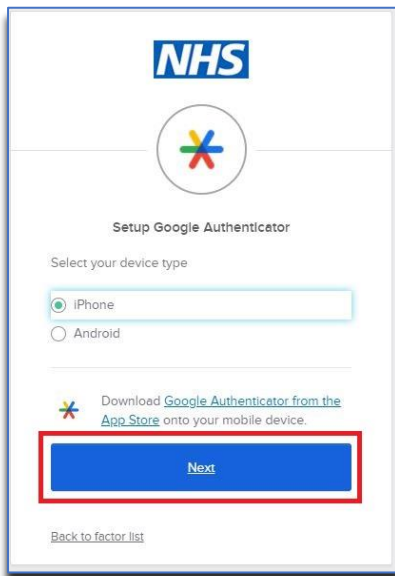
Below the Google Authenticator option, click the **Setup** button.

Please note the Google Authenticator option can also be used for Microsoft Authenticator set up, as an alternative to Google.

You should see a new page with the below in the centre.  
Select your phone type.

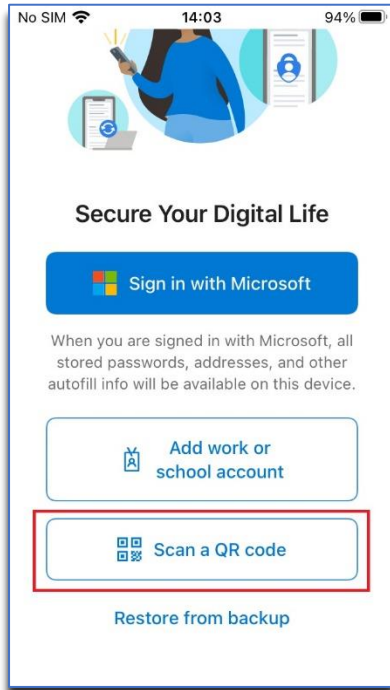


You will be presented with a new option. Select Next.

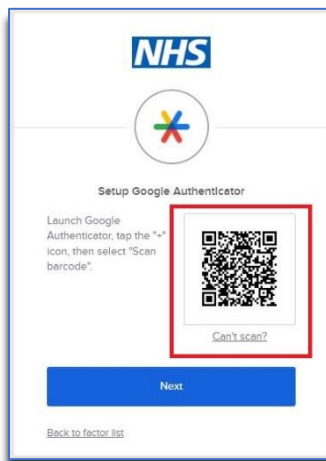


You will be presented with a screen and a QR code to scan.

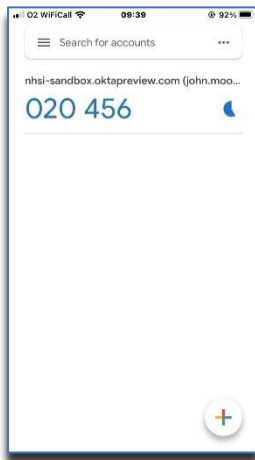
On your phone, launch the Microsoft Authenticator. Select Scan a QR code.



This will open the phone camera. Point the camera at the QR code onscreen.



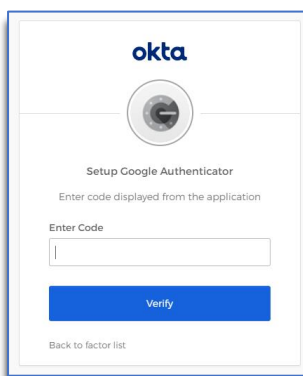
Once the QR code has been captured, you will see an image like the below. This will present automatically.



You will be asked to enter the series of 6 numbers in to the “Enter code” field. Then click verify.

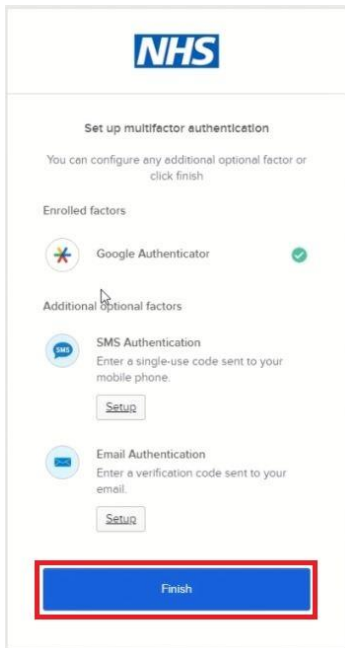
You will see a small circular icon on the left of the numbers – this is a timer of 30 seconds. You have 30 seconds to enter the code before these change to a new number. It is OK to allow the numbers to change before you enter them, if they are about to change.

This will effectively pair the Authenticator installed on your phone to your AGEM Apps / OKTA account.



You will be asked to perform this step one more time to complete the set up. Enter the new set of numbers and you will be sent to the required AGEM App login screen.

You will then be asked to Finish.



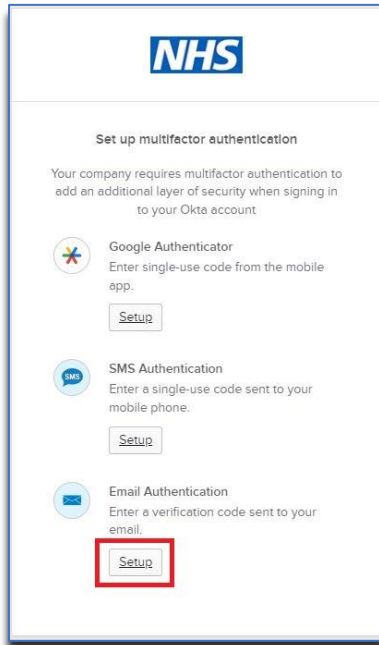
Set up is now complete.

Each time you log in from now on, you will be asked to add the numbers displayed in the App, onto the app log-in screen.

## 4. Email Set-Up for MFA in an App

Logon to the required App in the web browser.

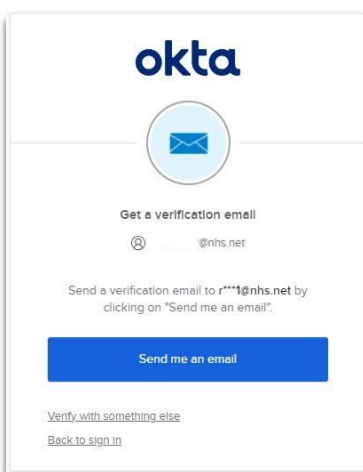
You will be prompted by a screen prompting you to choose an option.



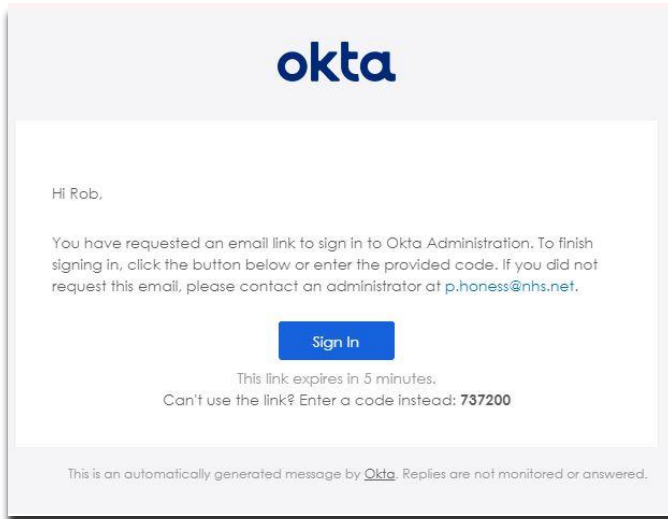
Below the Email Authentication option, click the **Setup** button.

You will see the below prompt.

Select the blue "Send me an email" button.

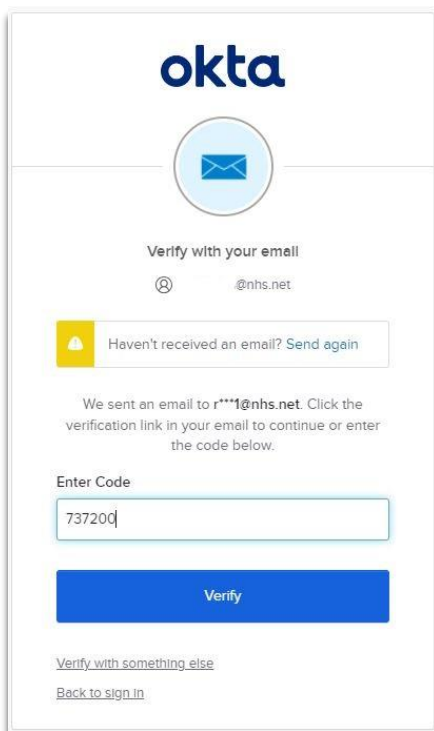


An email will be sent to your mailbox, with an authentication code and a “Sign In” button. If the Sign in button is selected a web page will open to the app you require access to. If the app is already open the 6 digit number can be copied across to the app.



Copy the 6 Digits from the email to the screen below.

Select Verify once the code has been entered. You will then be logged into the app.

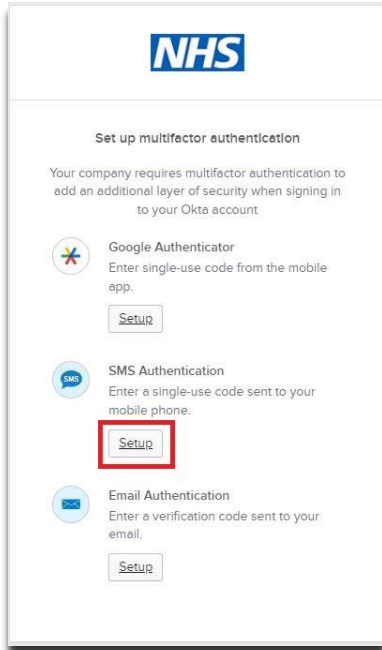




## 5. SMS Authentication Set-Up

For SMS Authentication when accessing an app, you will be presented with a choice of Authentication methods.

Select 'Setup' beneath the SMS Authentication option.



**NHS**

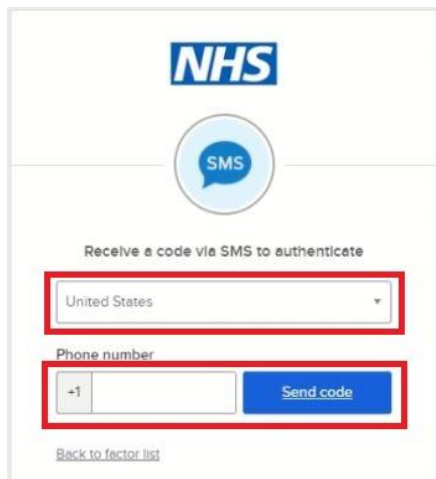
Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account.

- Google Authenticator**  
Enter single-use code from the mobile app.
- SMS Authentication**  
Enter a single-use code sent to your mobile phone.
- Email Authentication**  
Enter a verification code sent to your email.

You will be presented with the following box where you will need to select your country and add your phone number.

Followed by the 'Send code' button.



**NHS**

**SMS**

Receive a code via SMS to authenticate

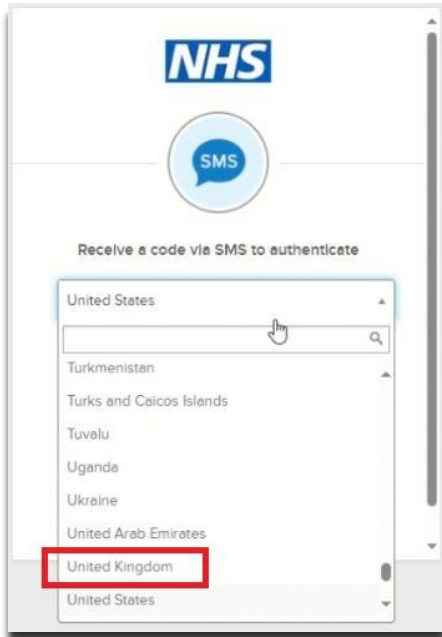
United States

Phone number

+1

[Back to factor list](#)

First change the country from the drop-down menu.



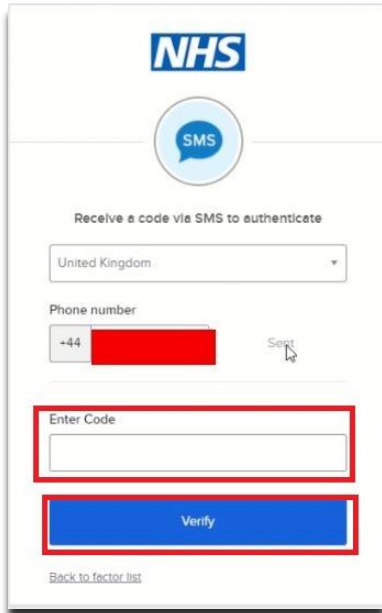
When the correct country has been selected the country code will show in the 'Phone Number' section.

Enter your mobile number here and select 'Send code'.



A text message will be sent to you with a code on.

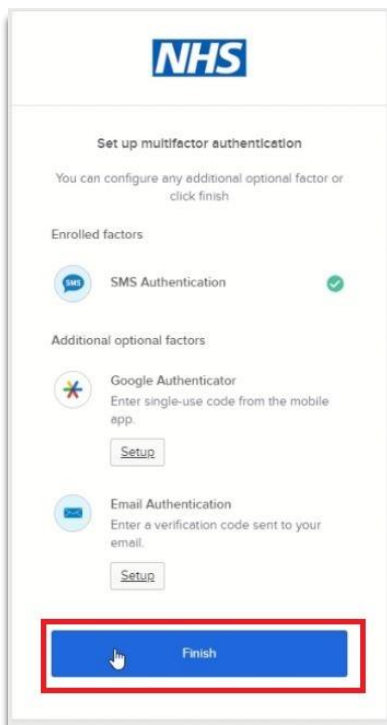
Add the code from the text message to the box and select 'Verify'.



The screenshot shows the NHS SMS authentication interface. At the top is the NHS logo. Below it is a blue circular icon with 'SMS' inside. The text 'Receive a code via SMS to authenticate' is centered. There is a dropdown menu for 'United Kingdom'. Below that is a 'Phone number' field with a '+44' prefix and a redacted number, followed by a 'Send' button. A red box highlights the 'Enter Code' input field. Below that is a blue 'Verify' button, also highlighted with a red box. At the bottom left is a link 'Back to factor list'.

You will then be asked to 'Finish' setup.

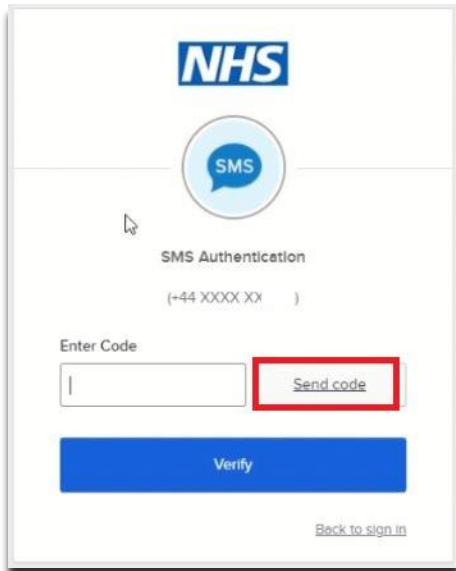
Click the 'Finish' button.



The screenshot shows the NHS 'Set up multifactor authentication' screen. At the top is the NHS logo. Below it is the title 'Set up multifactor authentication' and the instruction 'You can configure any additional optional factor or click finish'. Under 'Enrolled factors', 'SMS Authentication' is listed with a green checkmark. Under 'Additional optional factors', 'Google Authenticator' and 'Email Authentication' are listed, each with a 'Setup' button. A red box highlights the blue 'Finish' button at the bottom of the screen.

From this point onward when you log into an OKTA authenticated app you will be able to request a code be sent to your phone.

Upon receipt of the code select 'Verify' in order log in.



The screenshot shows the NHS SMS Authentication interface. At the top is the NHS logo. Below it is a blue circular icon with 'SMS' inside. The text 'SMS Authentication' is displayed, followed by a phone number placeholder '(+44 XXXX XX )'. There is an 'Enter Code' label above a text input field. To the right of the input field is a 'Send code' button, which is highlighted with a red rectangular border. Below the input field and 'Send code' button is a large blue 'Verify' button. At the bottom right, there is a link that says 'Back to sign in'.

## Version History

| Version    | Date       | Author       | Approver     | Changes                                       |
|------------|------------|--------------|--------------|---|
| <b>1.1</b> | 04/05/2022 | Vicky Nelson |              | Added a note about RED authenticator numbers. |
| <b>1.2</b> | 26/07/2023 | Andy Clarke  |              | Authenticator Logo updated                    |
| <b>1.3</b> | 08/02/2024 | Jack Waters  |              | Updating Header logos                         |
| <b>2</b>   | 06/03/2024 | Rob Orton    | Vicky Nelson | Updated authenticator types and template      |
|            |            |              |              |   |