NHS National Data Platform (Foundry) Onboarding Guide

Table of Contents

Onboarding Requirements

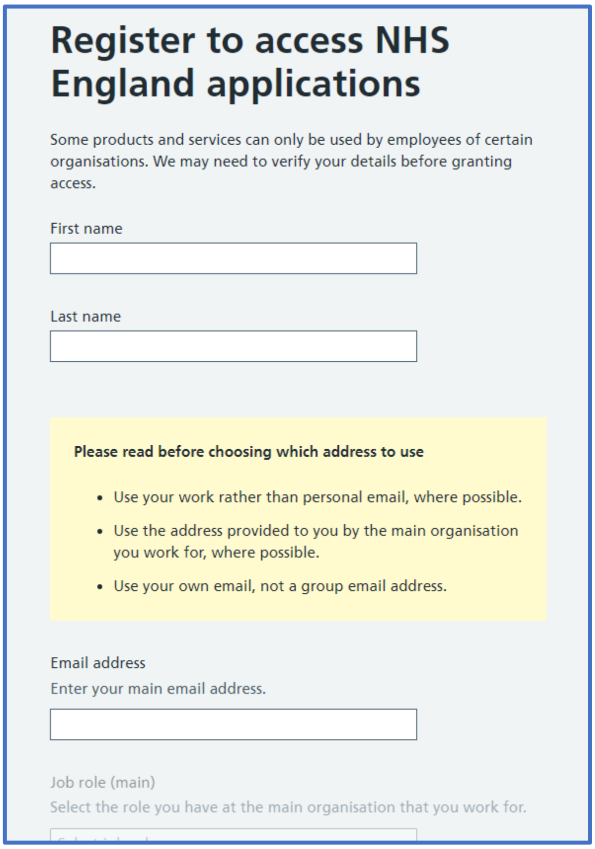
This guide will take you through the steps required to get access to the NHS Data Platform (Foundry).

You will need:
1. Either **Google Chrome** or **Microsoft Edge** installed on your workstation
2. Your **iPhone or Android smartphone** (this can be your work or a personal device)

Step 1: Registering for an Okta account

Okta is a cloud-based identity management service used to manage access to Foundry. Essentially this portal acts as a central entrance point to many of our existing platforms. If you already have an Okta account, proceed directly to Step 2.

1.1. Click here to register for an Okta account.



Register to access NHS England applications

Some products and services can only be used by employees of certain organisations. We may need to verify your details before granting access.

First name

Last name

Please read before choosing which address to use

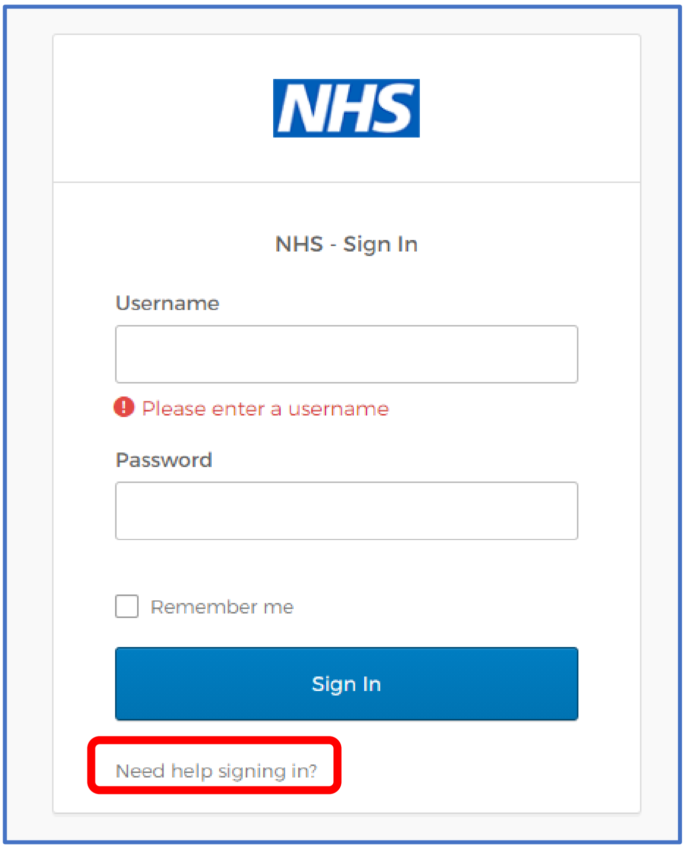
- Use your work rather than personal email, where possible.
- Use the address provided to you by the main organisation you work for, where possible.
- Use your own email, not a group email address.

Email address
Enter your main email address.

Job role (main)
Select the role you have at the main organisation that you work for.

1.2. Complete the details on this page and then click **'Register'**. Be sure to choose a strong password, then proceed to setup your password security questions and answers in case you forget your password.

1.3. If you already have an Okta account but cannot remember your login details, visit this link, click **‘need help signing in?’**, select one of the options available and then follow the instructions.



NHS - Sign In

Username

Please enter a username

Password

□ Remember me

Step 2: Applying for access to the Foundry platform

2.1. You will now need to apply for access to Foundry itself by completing Foundry System Access - Form A.

2.2. Once completed, e-mail the form to foundry.support@england.nhs.uk
Please note the following with regard to Section 2 of the form:

- If you only need access to training resources on Foundry at this point, then only complete the first box in section 2
- If you know which purpose(s) or tool(s) you need access to on Foundry, then complete the second and/or third box in Section 2
- If you only need basic access to Foundry at this stage, then you do not need to complete section 2

Step 3: Setting up two-factor authentication (2FA) with the NHS Foundry Platform

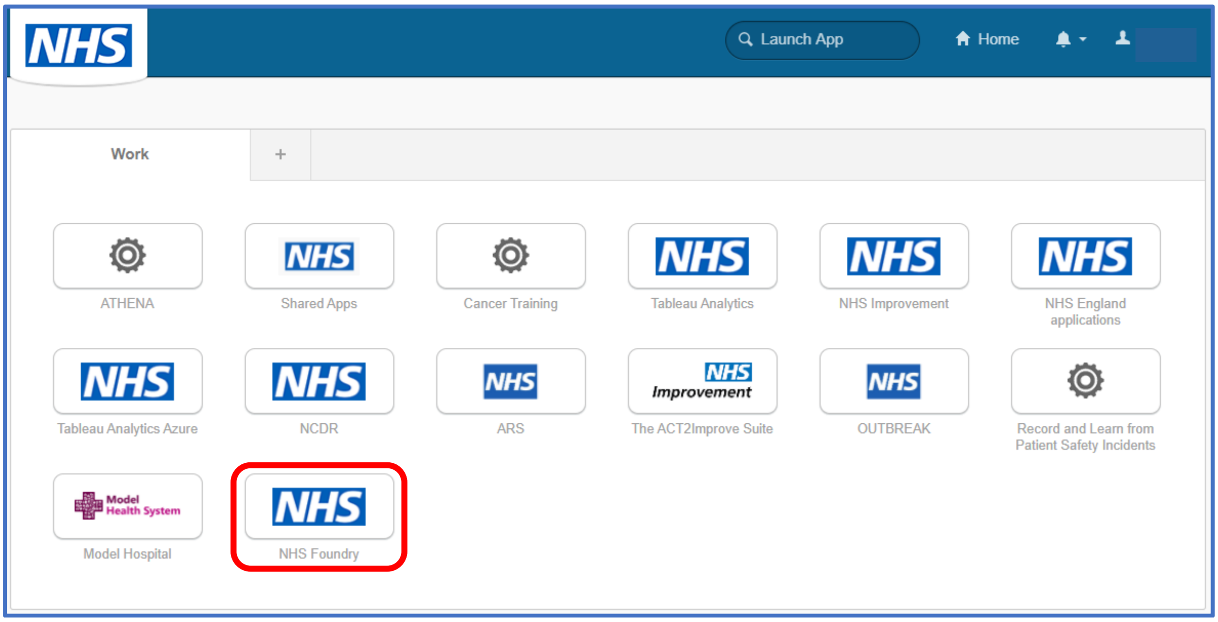
In order to access the NHS Foundry platform, you must verify your identity through a process called ‘two-factor authentication’. This is also known as ‘multi-factor authentication’. It is an increasingly common and important security step that ensures only you can use your account and it also ensures the security of the data in the NHS Foundry platform.

Two-factor authentication requires using a second device that only you have access to, such as a mobile phone, to generate short temporary passwords every time you want to log in.

The instructions below describe how to register your phone as a two-factor authentication device with your account.

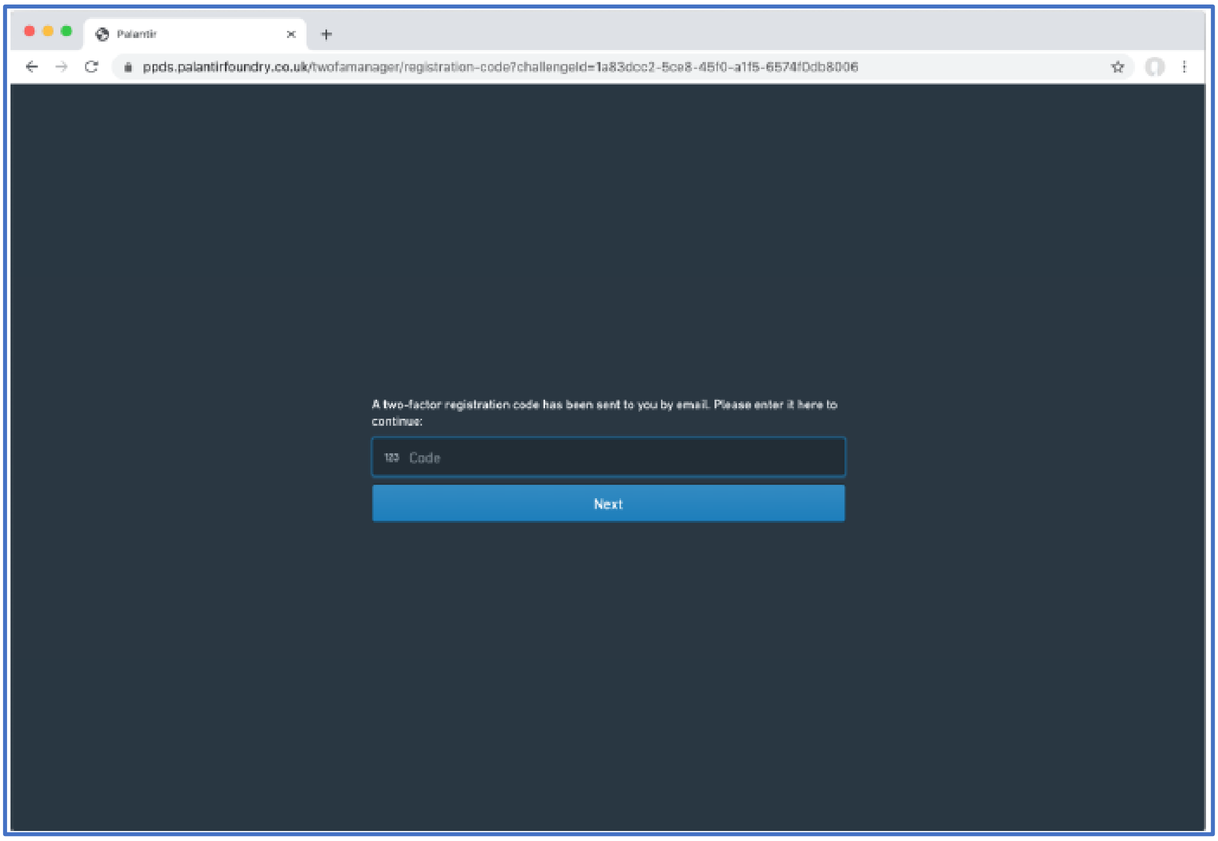
Step 3a: Verifying your email address

3.1. When you have logged into Okta using this link, you should see a screen that looks like the image below. Depending on your role, the applications available to you may be slightly different. Click on the **‘NHS Foundry’** icon.



3.2. This will take you to the screen below prompting you for a two-factor registration code.

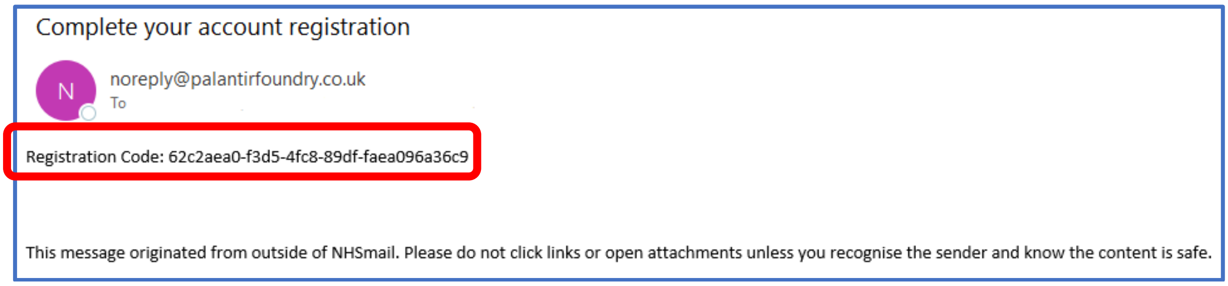
[screenshot on following page]


Palantir
ppds.palantirfoundry.co.uk/twofamanager/registration-code?challengeId=1a83dcc2-5ce8-45f0-a1f5-6574f0db8006
123 Code
Next

A two-factor registration code has been sent to you by email. Please enter it here to continue:

3.3. The two-factor registration code will have been sent to your email address, the same email address you used to register for your Okta account. It may take a few minutes to arrive but check your Spam/Junk e-mail for the code if not.

3.4. The code is the long string of characters highlighted in red below. Copy the registration code and paste it back into the screen shown above or click the hyperlink.



Complete your account registration

N noreply@palantirfoundry.co.uk
To

Registration Code: 62c2aea0-f3d5-4fc8-89df-faea096a36c9

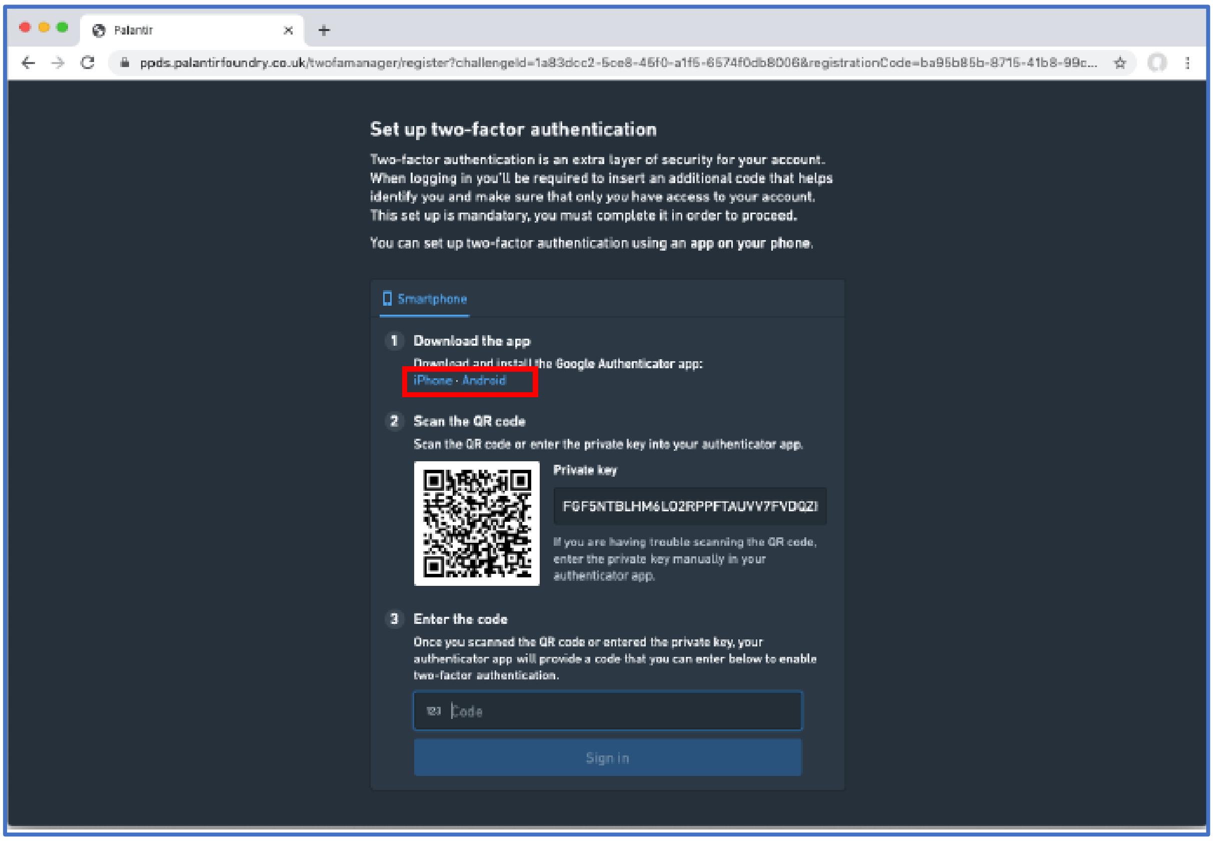
This message originated from outside of NHSmail. Please do not click links or open attachments unless you recognise the sender and know the content is safe.

Step 3b: Registering your two-factor authentication device

3.5. Now that you've validated your email address, the next step is to register your phone as a two-factor authentication device. As described in Step 3, two-factor authentication is in place to further verify your identity.

3.6. We recommend Google Authenticator as a trusted method for two-factor authentication. If you already have Google Authenticator, skip to Step 4b below.

3.7. The screen below should be available on your workstation. It guides you through the process of registering your phone as a two-factor authentication device.



ppds.palantirfoundry.co.uk/twofamanager/register?challengeId=1a83dcc2-5ce8-45f0-a1f5-6574f0db8006&registrationCode=ba95b85b-8715-41b8-99c...

Set up two-factor authentication

Two-factor authentication is an extra layer of security for your account. When logging in you'll be required to insert an additional code that helps identify you and make sure that only you have access to your account. This set up is mandatory, you must complete it in order to proceed.

You can set up two-factor authentication using an **app on your phone**.

1 Download the app

Download and install the Google Authenticator app:
iPhone · Android

2 Scan the QR code

Scan the QR code or enter the private key into your authenticator app.

Private key: FGF5NTBLHM6LO2RPPFTAUVV7FVDQZI

If you are having trouble scanning the QR code, enter the private key manually in your authenticator app.

3 Enter the code

Once you scanned the QR code or entered the private key, your authenticator app will provide a code that you can enter below to enable two-factor authentication.

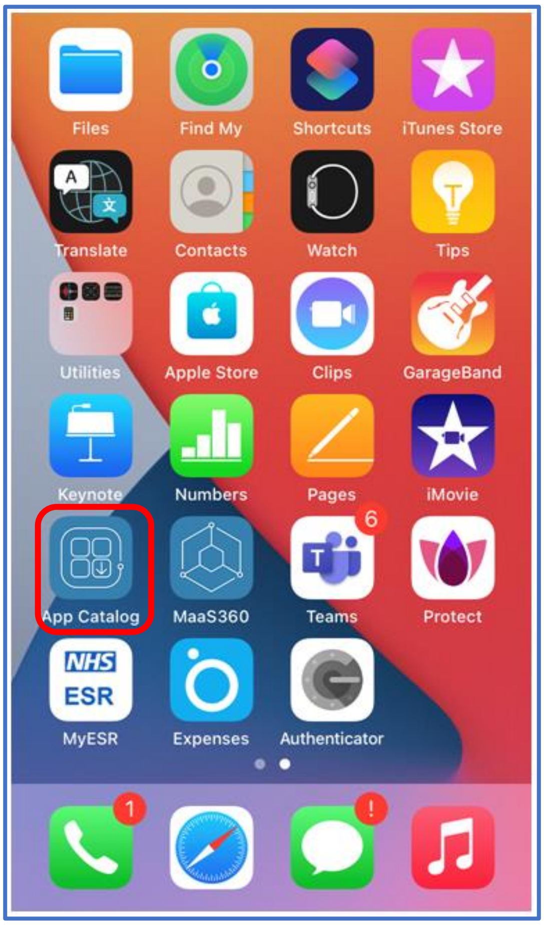
3.8. Choose iPhone or Android depending on your smartphone's operating system. These links provide direct access to download the Google Authenticator app in their respective application stores; however, you will need to visit the App Store or the equivalent means of downloading apps that features on your phone, to download the appropriate app for your device.

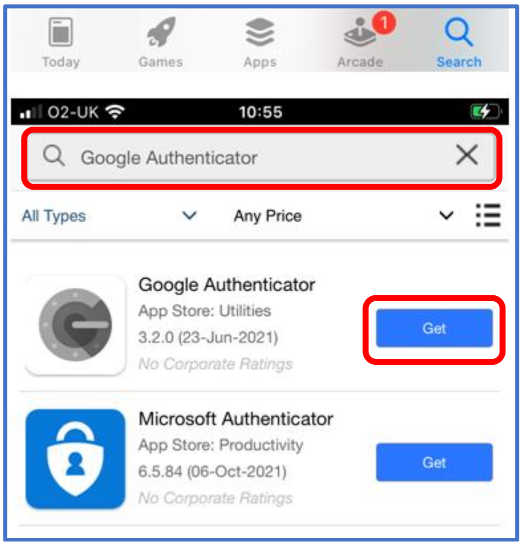
Step 4: Two-factor Authentication

The following guidance is based on an NHS standard issue iPhone; however, the guidance is fairly similar for Android and other devices/platforms. Please keep this in mind if the steps or images vary slightly.

Step 4a: Downloading Google Authenticator

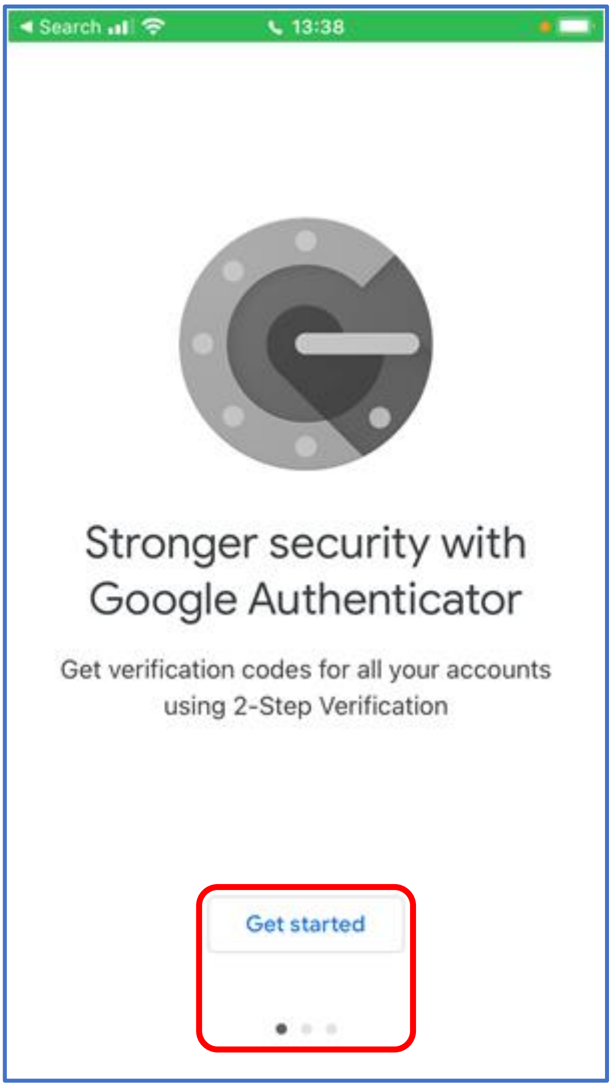
4.1. If you have an NHS iPhone, go to the **'App Catalog'** and search for **'Google Authenticator'** and select **'Get'** to download the app. If you have any other device, please search for the same within your app store.





4.2. Once it has finished downloading, open it, and you should see the screen below. Swipe left for info on how the app works. Click **'Get Started'** at the bottom of the screen.

[screenshot on following page]



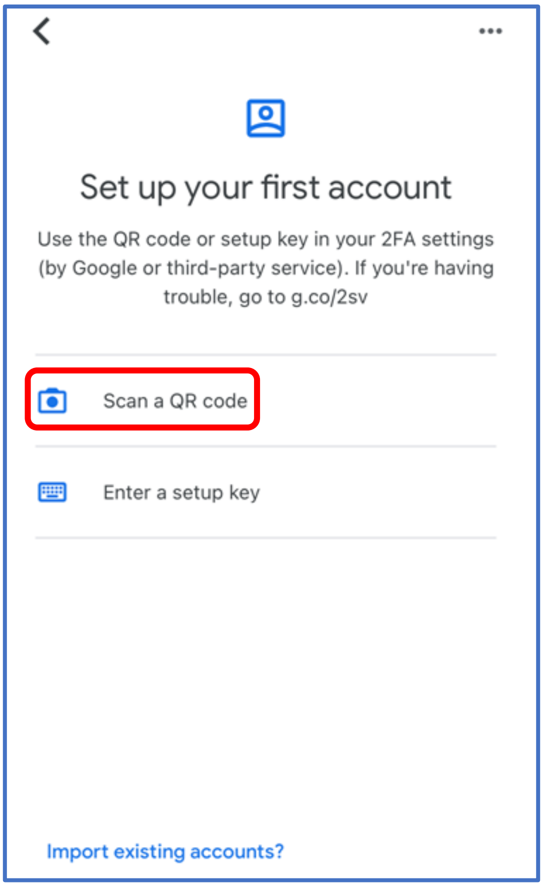
Stronger security with Google Authenticator

Get verification codes for all your accounts using 2-Step Verification

Step 4b: Using Google Authenticator

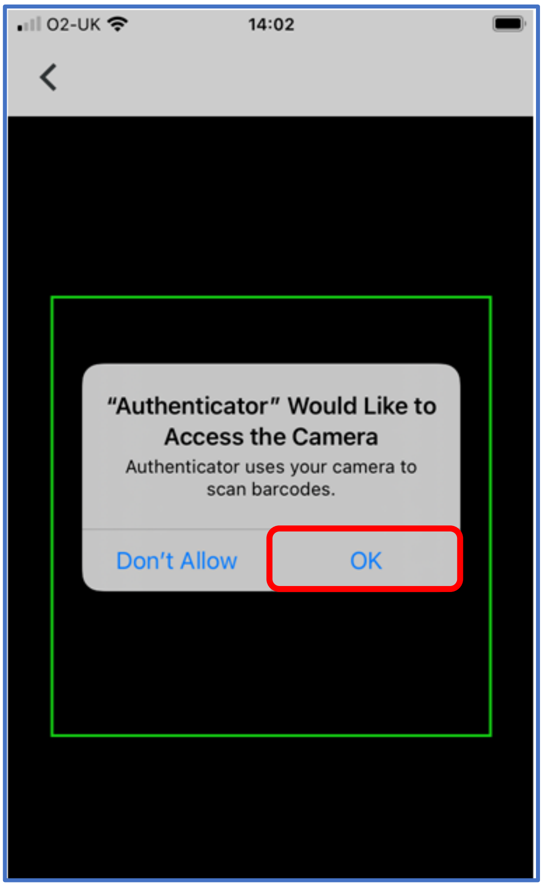
4.3. You'll need to use your phone's camera to scan a barcode. Once you have opened the Google Authenticator app, click **'Scan barcode'** and then **'OK'** to the pop-up request regarding granting Authenticator access to your phone's camera. You can always revoke this access later in your phone's settings.

[screenshots on following page]



Set up your first account

Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

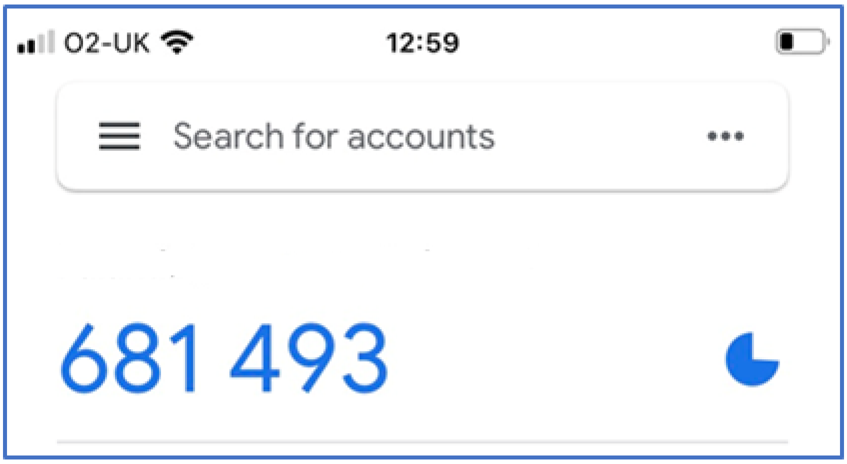


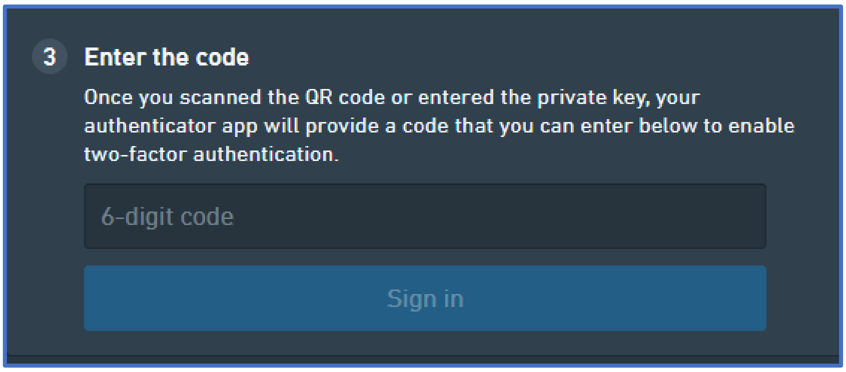
“Authenticator” Would Like to Access the Camera

Authenticator uses your camera to scan barcodes.

4.4. Point your phone’s camera at the QR code which should still be present on your workstation screen. **Please do not scan the QR within this guide**. Scanning the QR code will register NHS Foundry in Google Authenticator.

4.5. A six-digit code will flash on your phone’s screen. Enter the code into the field at the bottom of the page on your workstation. Note that the code is both one-time-use and time-based and will change every 30 seconds.





3 **Enter the code**

Once you scanned the QR code or entered the private key, your authenticator app will provide a code that you can enter below to enable two-factor authentication.

4.6. You are now set up with two-factor authentication. On every log in you'll need to look up a new temporary time-based code from the Google Authenticator app.

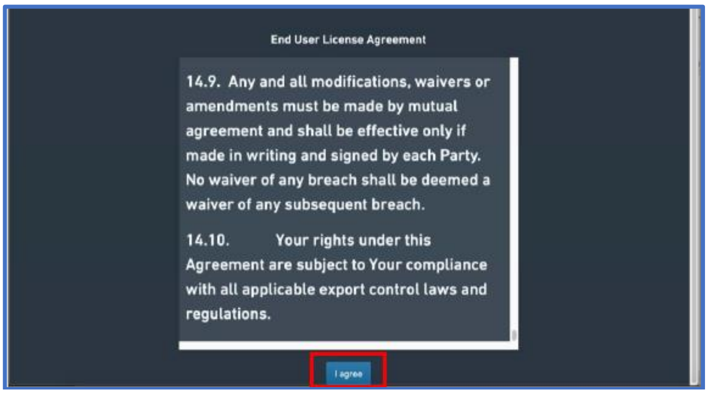
Authentication Troubleshooting

I. If you are not greeted with the two-factor authentication set-up screen and instead it takes you directly to the screen asking you to input the code, then it may be that two-factor authentication needs to be reset. If so, please e-mail foundry.support@england.nhs.uk and ask for this reset.

II. If you are using an Android smartphone and the authenticator screen does not accept the code that has been generated by the app, this could be due to a time setting issue. Select the ellipsis at the top right of your mobile device (3 dots), click **'Settings'** from the drop down menu that opens and then **'Time correction for codes'**. Select **'Sync now'** and this should resolve the issue; however if you are still unable to get pass the authentication stage, please e-mall foundry.support@england.nhs.uk for support.

Step 5: Agreeing to the End User License Agreement

5.1. Once you've authenticated, you'll be prompted to agree to the NHS Foundry end user license agreement. Read the text in the box and then click **'I agree'**.



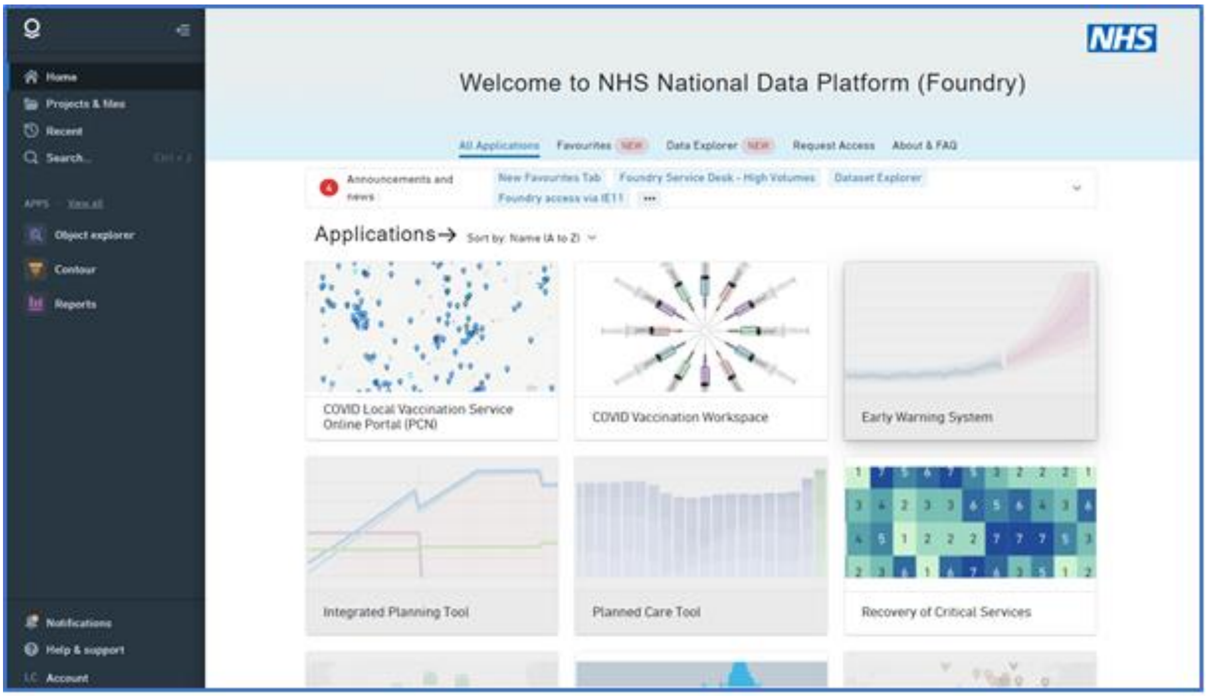
End User License Agreement

14.9. Any and all modifications, waivers or amendments must be made by mutual agreement and shall be effective only if made in writing and signed by each Party. No waiver of any breach shall be deemed a waiver of any subsequent breach.

14.10. Your rights under this Agreement are subject to Your compliance with all applicable export control laws and regulations.

5.2. Your registration is complete. You will now be logged in to NHS Foundry platform.

NOTE: if you haven’t applied for any purposes/data sets during the application process you won’t have access to any data or applications when you first log in. For more information on how to apply for the data that you need please click the ‘Request Access’ tab on the NHS Foundry platform Homepage, which will explain how you can apply through the Purposes User App.



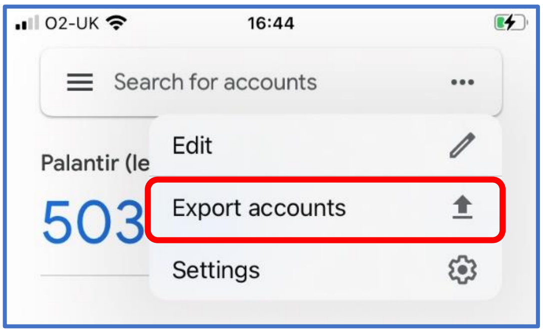
You have now successfully completed the onboarding process.

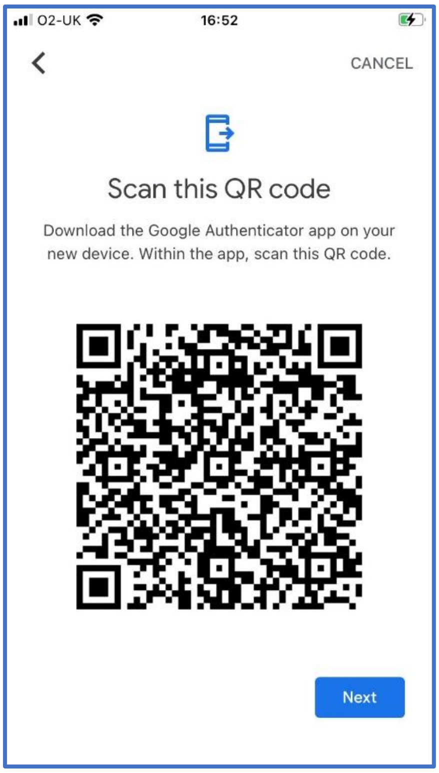
Transferring your Two-factor Authentication

1.1. On your **new mobile device**, download **Google Authenticator** (See Step 4a for guidance).

1.2. On your **old mobile device**, open the **Google Authenticator app**, tap the **ellipses icon** (3 vertical dots at the top right), click on ‘**Export accounts’** and follow the guidance to generate a QR code.

[screenshots on following page]





Scan this QR code

Download the Google Authenticator app on your new device. Within the app, scan this QR code.

1.3. On your **new mobile device**, open the **Google Authenticator app**, tap the **ellipses,** and click on **Import.** Follow the guidance to **scan the bar code** generated **on your old mobile device**.

NOTE: Contact foundry.support@england.nhs.uk if you have reset your old device, to have your authenticator reset.

If you require any further support, please email foundry.support@england.nhs.uk

For NHS National Data Platform Admin Use Only

Programme/Project Name		NHS National Data Platform (Foundry)	
Guide Created By		Leon Carr, Training Content Development Manager	
Guide Approved By		Alison Stott, Head of Training and Deployment	
Version	Final v3	**Date**	14/11/2022