

This guide will take you through the steps required to log on to the LVS Online Portal for site readiness assessment and online ordering. **You will need:**

1. **Google Chrome** or **Microsoft Edge** installed on your workstation. The LVS Online Portal is not optimised to work in other internet browsers, and **will not work in Internet Explorer**.
2. **Your iPhone or Android smart phone**.

## Setting up two-factor authentication and accessing the LVS Online Portal

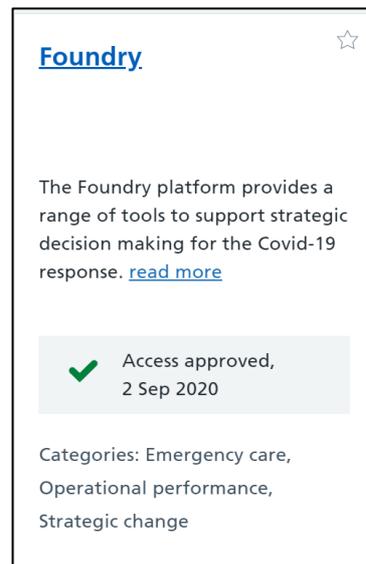
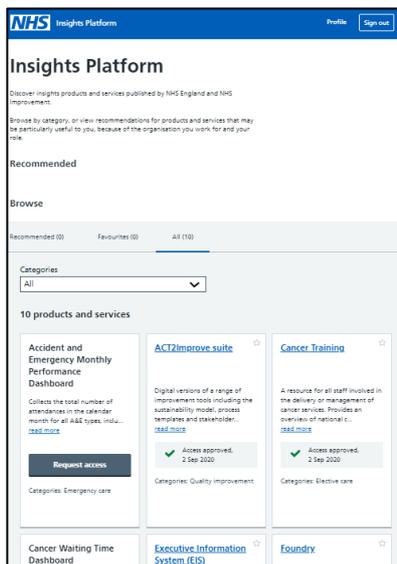
In order to access the LVS Online Portal for site readiness assessment and online ordering, you must verify your identity through a process called “two-factor authentication”. This is also known as “multi-factor authentication”. It is an increasingly common and important security step that ensures only you can use your account and ensures the security of the data in the LVS Online Portal.

Two-factor authentication requires using a second device that only you have access to, such as a mobile phone, to generate short temporary passcodes 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.

### 1. Verifying your email address

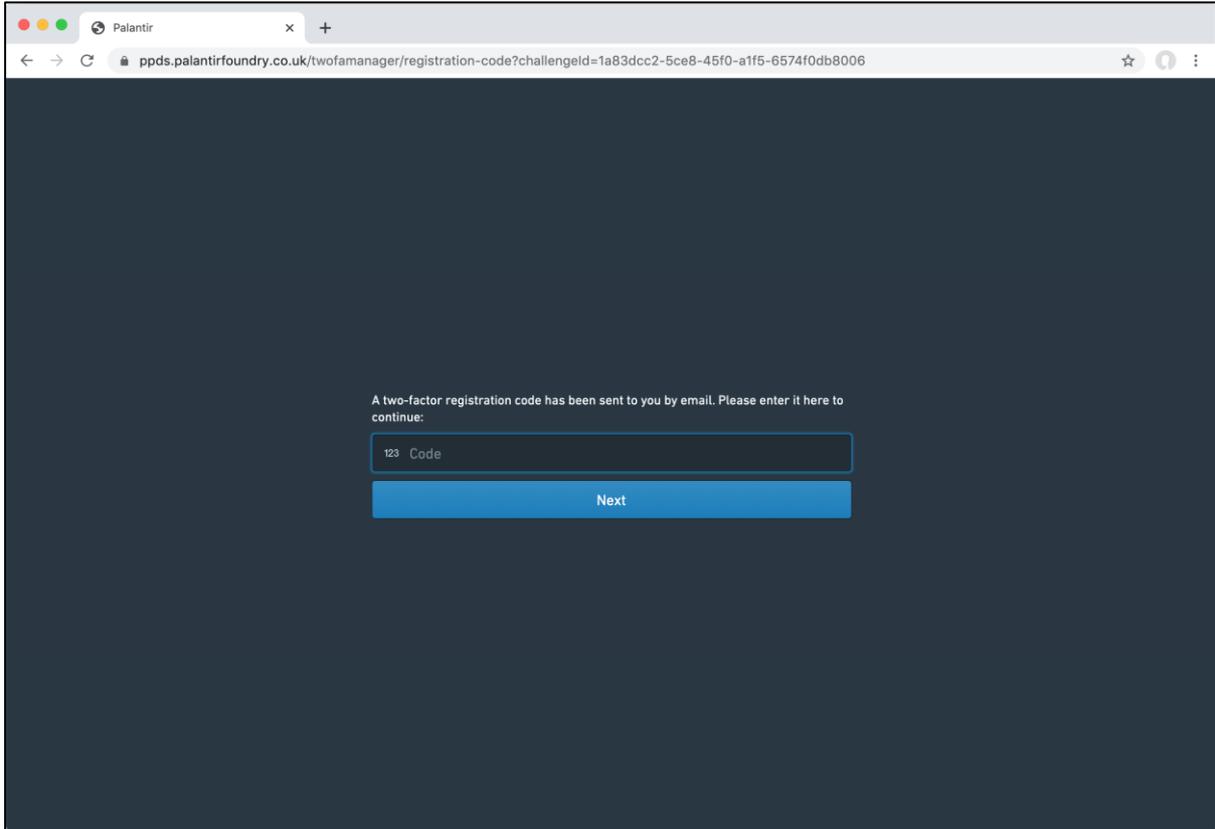
When you have logged into your insights account, you should see a screen that looks like the below (the applications available to you may be slightly different). Look for the tile titled “Foundry” and click the link.







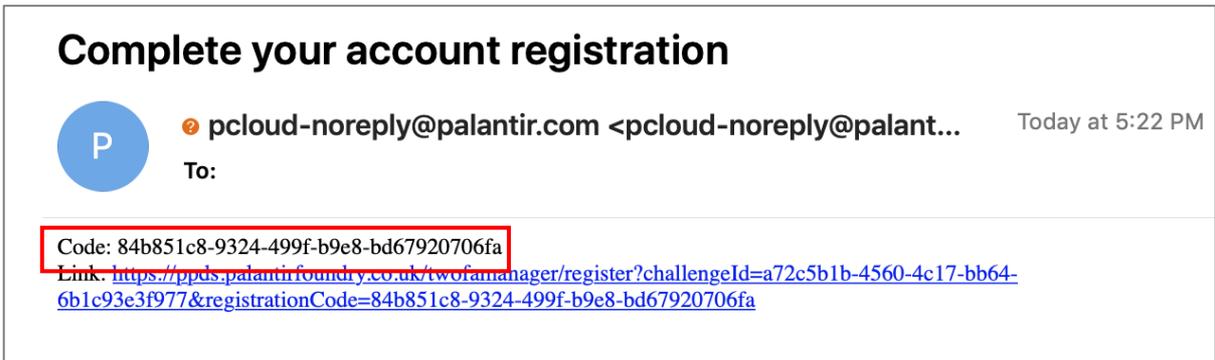
You will be taken to the screen below prompting you for a two factor registration code:



This code will have been sent to your email, the same email address you used to register for your Okta/NHS Improvement account. It may take a minute to arrive. *If you do not see this page please go to the [troubleshooting section](#).*

Remember to check your Spam / Junk Email for the code. The Email will have the subject **“Complete your account registration”**.

The code is the long string of characters highlighted in red below. Copy it and paste it back into the screen shown above, or click the link in the email body - either will bring you to the same page shown in the next steps.



## 2. Registering your two-factor authentication device

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

We recommend Google Authenticator, a trusted method for two-factor authentication.

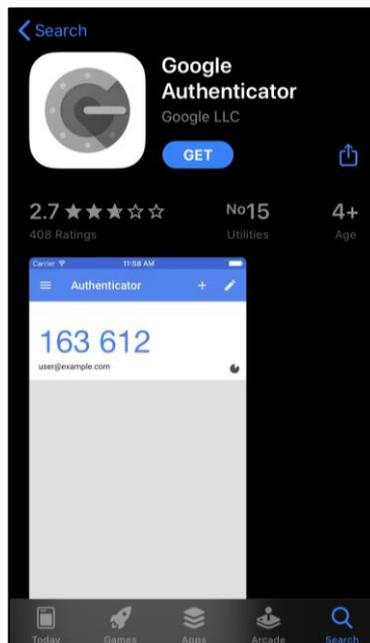
## 3. Downloading Google Authenticator

*If you already have Google Authenticator, skip to Step 4 below.*

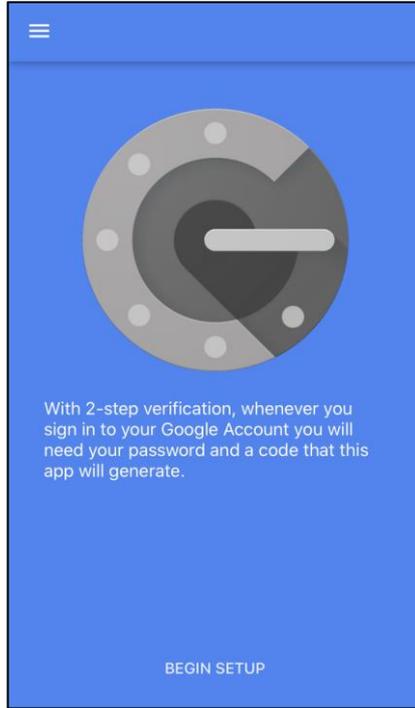
Search for "Google Authenticator" in the appstore app on your smartphone, or open the camera app on your phone and point your device at the code below. Your smartphone should open your app store on the correct page.



The App Store page will look similar to this:

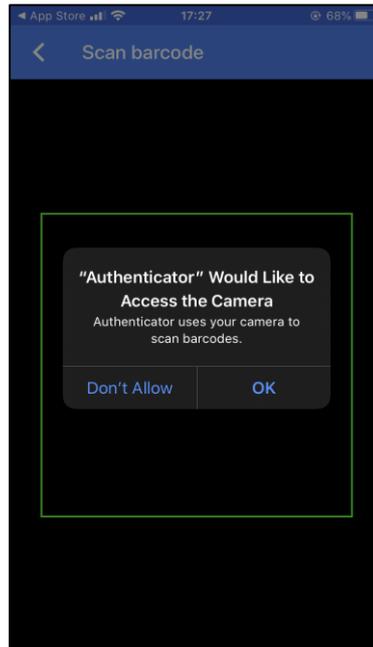
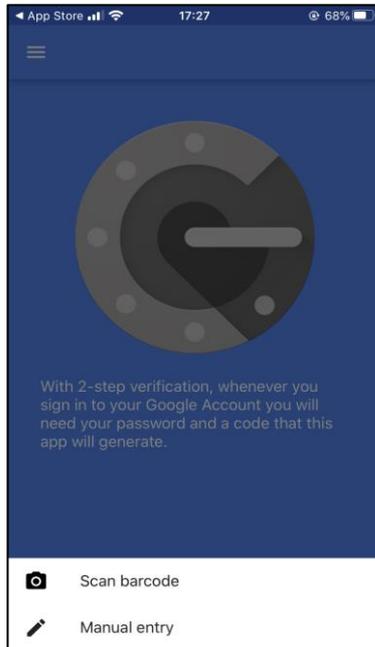


Download the app, open it, and you should see this screen, explaining how it works. Click Begin Setup at the bottom of the screen:

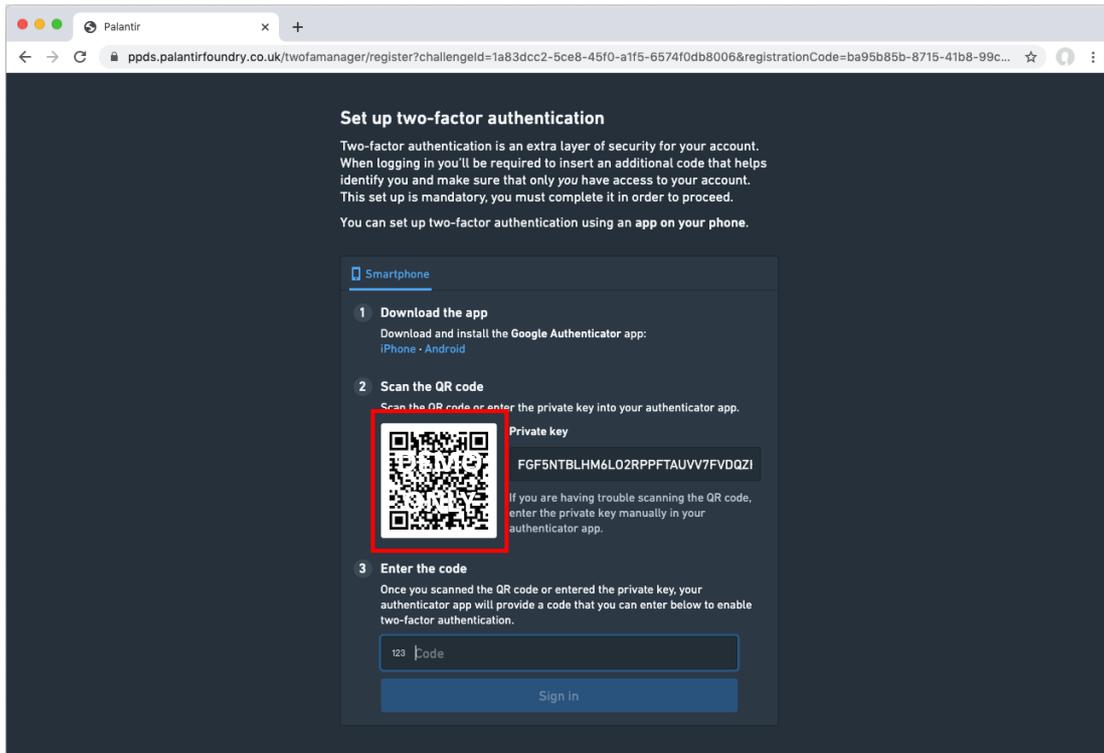


#### 4. Using Google Authenticator

You'll need to use your phone's camera to scan a barcode; hit "Scan barcode" in the app, and say "OK" to the prompt that pops up granting Authenticator access to your phone's camera. You can always revoke this access later in your phone's Settings menu.



Back on your computer, you will see this page. **Using the Google authenticator app only**, scan the QR code on your screen – not the one shown in this guide.



This will register the LVS Online portal in Google Authenticator. A six-digit code will flash on your phone's screen. Enter the code into the field at the bottom of the page. Note that the code is both one-time-use and time-based and will change every 30 seconds.

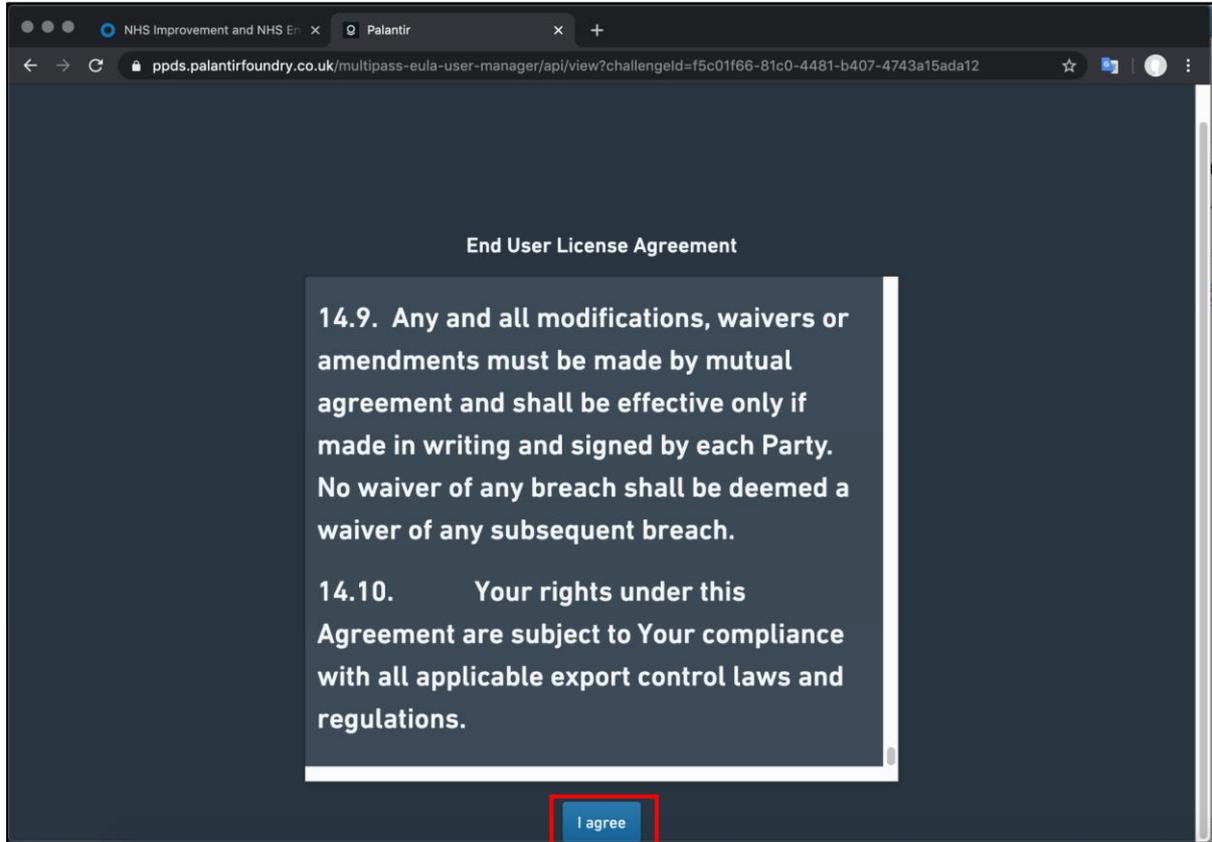
You are now set up with two-factor authentication. **Do not delete the app** - on every log in you'll need to look up a new temporary time-based code from the Google Authenticator app.

*Please ensure that the clocks on your phone and computer are in sync – in order for the OTP code to authenticate, they need to be within 1 minute of each other.*

*If you change phones you will need to have your Google Authenticator token reset. Please contact [agem.vaccinationstocktake@nhs.net](mailto:agem.vaccinationstocktake@nhs.net) to initiate the reset. You will then need to follow the steps below again.*

## 5. Agreeing to the End User License Agreement

Once you've authenticated, you'll be prompted to agree to the LVS Online Portal end user license agreement. Read the text in the box and then click "I agree" once content.



Your registration is complete. You will now be logged in to the LVS Online Portal.

## 6. Accessing the correct workspace

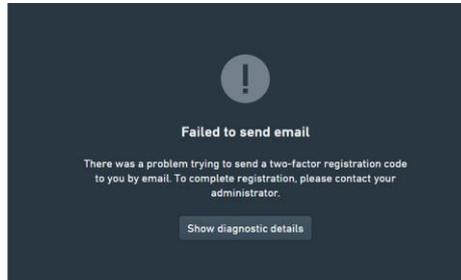
Once in the LVS Online Portal click the link below or copy and paste into your browser address bar. This will take you to the correct workspace.

<https://ppds.palantirfoundry.co.uk/workspace/carbon/ri.carbon.main.workspace.8a82681c-7f9d-478c-b487-dce12b14cbbd/home>

**Save this as a bookmark/favorite to use for quick, direct access in future.**

## Troubleshooting:

***When I try and log in to the LVS Online Portal I see the following screen:***



Your account is yet to be activated – please try and log in again later. If this persists for more than 24hrs please reach out to [agem.vaccinationstocktake@nhs.net](mailto:agem.vaccinationstocktake@nhs.net)

***My OTP generated by Google Authenticator is not being recognised or I get the “Incorrect OTP Error”***

Please check that the clocks on your phone and computer are in sync. They need to be within 1 minute of one another.

Only Scan the QR code shown at Step 4 with your authenticator app. Using any other QR reader, including the one built into your phone’s camera app will not produce a useable code.

***I have got a new phone and need to reset my Google Authenticator token.***

1. Reach out to [agem.vaccinationstocktake@nhs.net](mailto:agem.vaccinationstocktake@nhs.net) who will request your token reset and confirm back to you once it has been completed.
2. Once you have confirmation please follow the [authorisation process in Step 2.a](#)