Our digital journey »»

NHS
Gloucestershire Hospitals
NHS Foundation Trust

Our Digital Journey – Safe, Secure and Cyber Aware

The digital landscape is changing and organisations and businesses are becoming more vulnerable to sophisticated cyber-attacks. Cyber safety does not stand still and during 2022 you will see new and updated measures come into force, both nationally and locally.

One of these steps is to make access to our systems through our Citrix environment (our virtual desktop) as secure as it can be. This involves a move to multi-factor authentication.

Moving to Multi-Factor Authentication

Many of you will be used to multi-factor authentication (MFA), it’s used to provide security on shopping and e-commerce sites. It usually involves a code sent to your smart phone when you log in and helps prevent hackers accessing your profiles easily.

Who does this impact?

This affects users who use a device to access Trust systems from home.

- *You’ll know if you’re affected because you will access Citrix to log in at home.*
- *This **does not** impact devices in our hospitals that use Citrix.*

We need every user of Citrix VDI to install authenticator software onto a smart phone or tablet **by no later than 5th April 2022.** After this date, users won’t be able to access trust systems through VDI without authentication. If you set up before this date, MFA won’t be required until 5th April.

Link to: User Guide for setting up authentication.

Our digital journey

NHS
Gloucestershire Hospitals
NHS Foundation Trust

Setting up authenticator software for Citrix MFA

<< Use this guide to set up your authenticator, or watch the video guide here (you will need to open this link in Chrome or Edge) **>>**

What you'll need to start this process:

- Your smart phone/tablet you want to use for authentication.
- Your work laptop or PC you use to access Virtual Desktop.

Step 1: Download an authenticator app to your device or smartphone from the Google Play or Apple store.

If you have already got an authenticator app you can go to Step 2.

Android Device	Apple Device
Microsoft Authenticator requires Android OS 6.0 or above Google Authenticator is device specific for the version that can be installed	Both Microsoft Authenticator and Google Authenticator require iOS 11.0 or later or iPadOS 11.0 or later

Search for either:

- Google Authenticator
- Microsoft Authenticator

Click **Install.** *You may need to log into the App Store to download applications – you do not need to log in within the application.*

Step 2: Citrix Device Registration

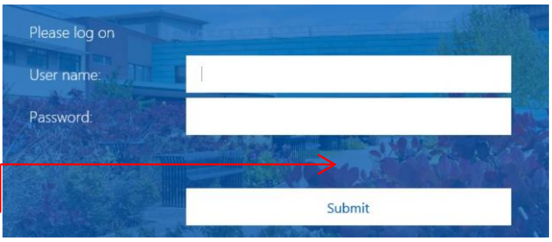
On the laptop or PC, you usually use to access trust systems, you'll need to register your device and log on using your Active Directory username and password.

The web address to register your One Time Passcode to your Authenticator App is as follows:

https://desktop.glos.nhs.uk/manageotp

https://sunrise.glos.nhs.uk/manageotp

NOTE: Both are the same OTP setup; just choose the link you are planning to use.



NOTE 2: If you see ✓ First factor below the "Passcode" box, then you are not on the device registration link. Please retry the above links or clear your browser cache (restart browser).

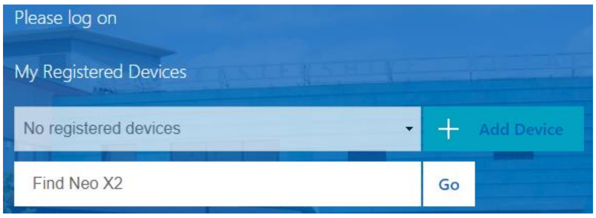
Log in using your usual active director username and password.

You'll then get this screen (shown):

Click on "+ Add Device"

Enter a name you want your device to be called (example: Martins Pixel 4XL). AVOID USING SPECIAL CHARACTERS

Once a name has been entered press Go, you will now see a QR code displayed.



Please log on

My Registered Devices

No registered devices ▾ | + Add Device

Find Neo X2 | Go

Here you will need to open up your Authenticator App on your smartphone/tablet to scan the QR code for registering the One Time Passcode to your account.

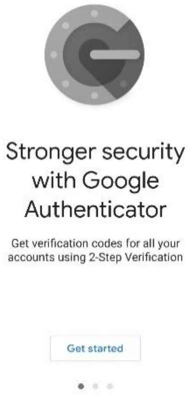
Step 3: Authentication App Setup

Guide to Google authenticator is first. For Microsoft authenticator, scroll down.

Using Google Authenticator

Open up Google Authenticator Application on your phone.

Click on the Get Started button (see picture) and it will take you through a guide to what the authenticator is.



Stronger security with Google Authenticator

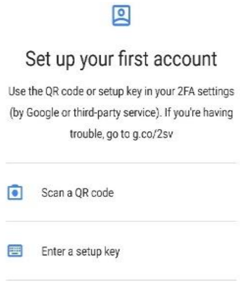
Get verification codes for all your accounts using 2-Step Verification

Get started

Once you've passed through the first four information screens you'll reach **"Set up your first account".**

Left and below: Select the option to **Scan a QR Code** and point the device camera at the screen with the code on.

If the QR code doesn't scan, or is not visible, zoom in by either holding CTRL and using the mouse wheel or selecting the 3 dots ... at the top-right of the screen and increasing 'Zoom'



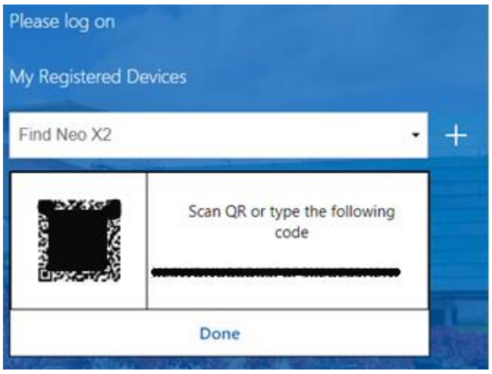
Set up your first account

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

Scan a QR code

Enter a setup key

Once scanned press "Done". You'll get a message confirming your device has been added successfully.



Please log on

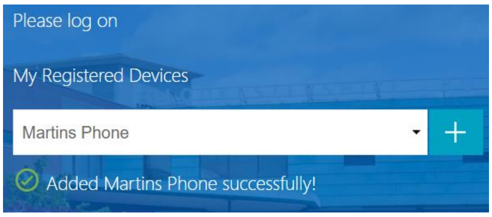
My Registered Devices

Find Neo X2 ▾ | +

Scan QR or type the following code

[redacted]

Done



Please log on

My Registered Devices

Martins Phone ▾ | +

Added Martins Phone successfully!

Using Microsoft Authenticator

Open up the Microsoft Authenticator app on your smart device

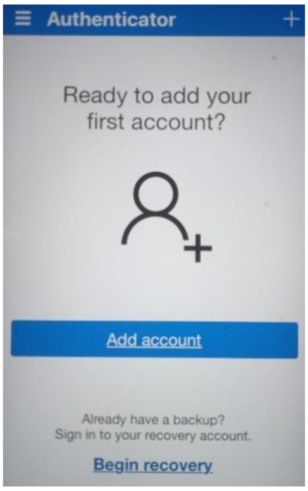
You will then see the ‘Ready to add account?’ page, click on the **Add Account** button.

Now you will need to select the option for **Work or School Account** and then select the option to **Scan QR Code**

Now you can point the device’s camera at the screen and scan the QR code displayed

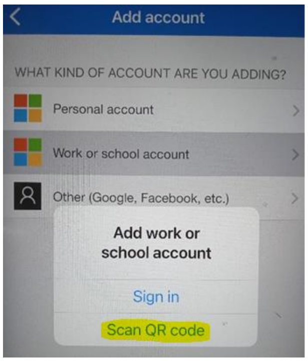
If the QR code doesn’t scan, or is not visible, zoom in by either holding CTRL and using the mouse wheel or selecting the 3 dots ... at the top-right of the screen and increasing ‘Zoom’

Once scanned press “Done”. You will see a message similar to what is shown below, this will confirm that your device has been registered successfully.



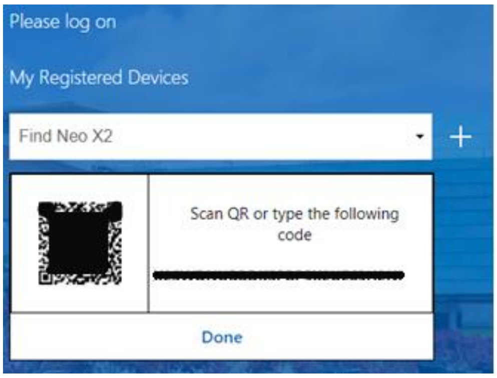
Ready to add your first account?

Already have a backup?
Sign in to your recovery account.



WHAT KIND OF ACCOUNT ARE YOU ADDING?

Add work or school account



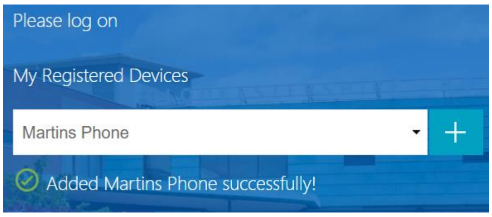
Please log on

My Registered Devices

Find Neo X2

Scan QR or type the following code

[redacted]



Please log on

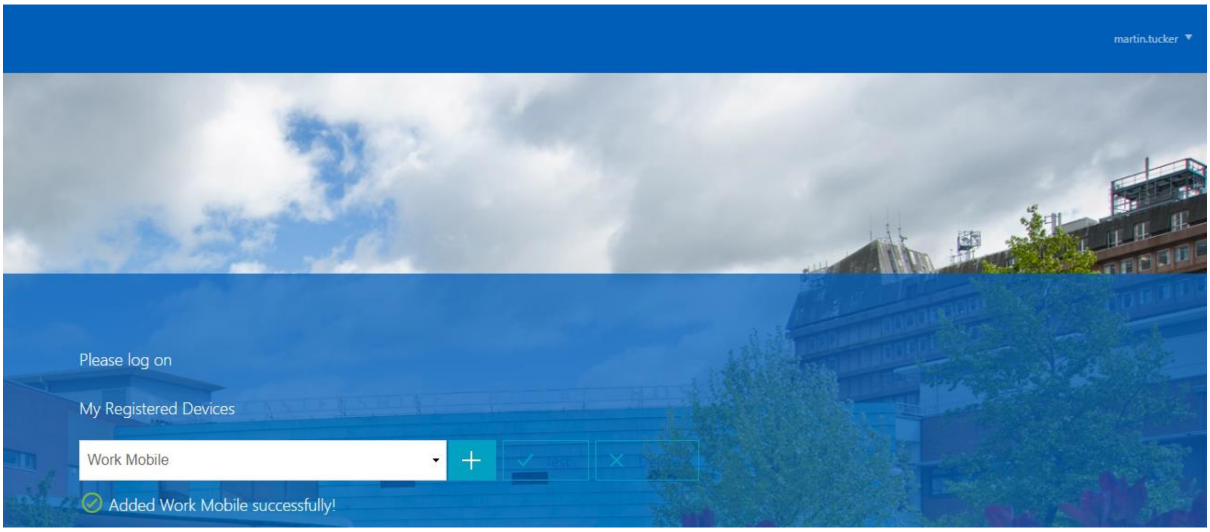
My Registered Devices

Martins Phone

Added Martins Phone successfully!

Login in to Citrix using MFA

Next click your name at the top-right of the screen and select “Log Off”



martin.tucker

Please log on

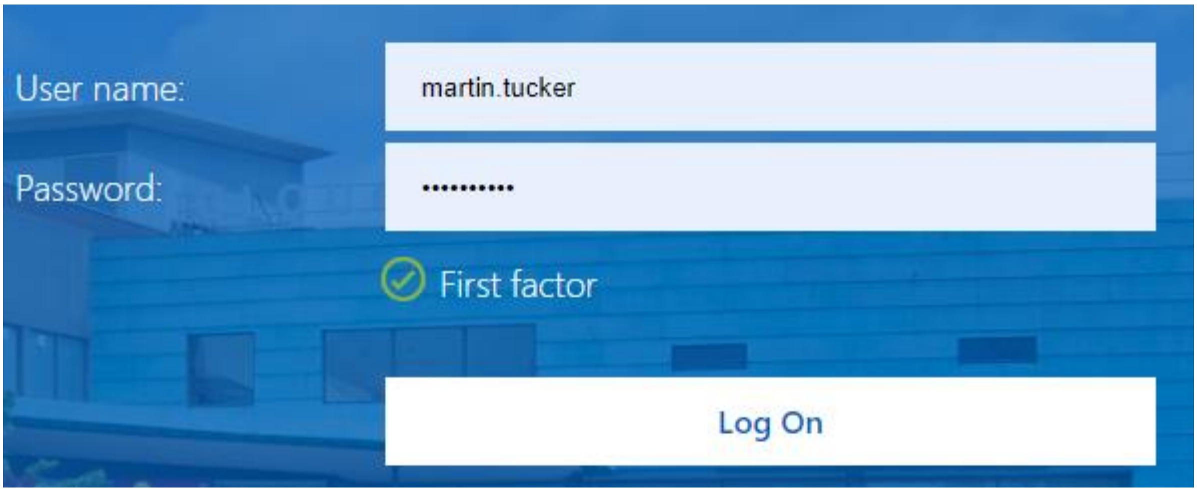
My Registered Devices

Work Mobile

Added Work Mobile successfully!

Then click “Log on” which will then take you to the new logon screen

If you see “First Factor” then you are on the correct screen



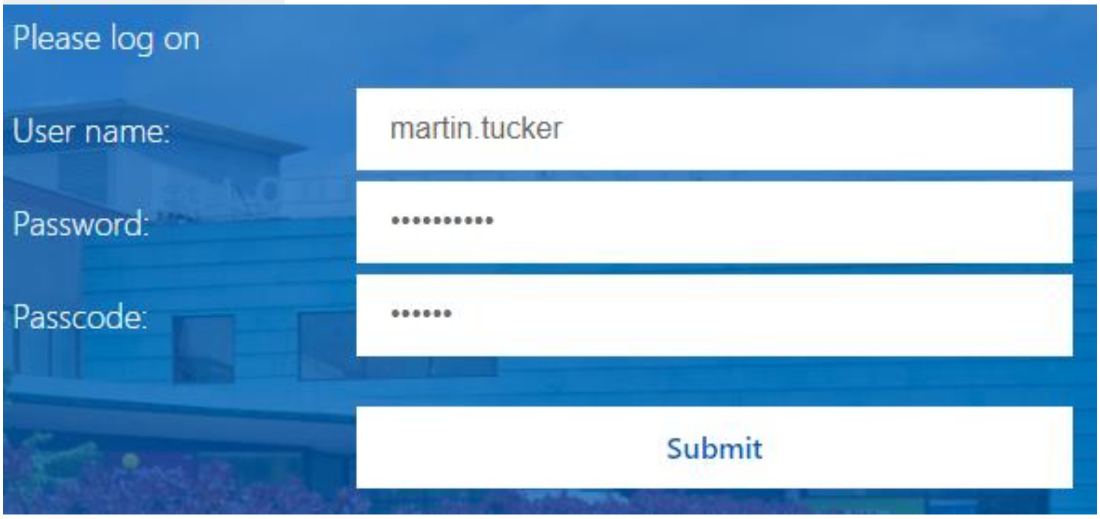
User name: martin.tucker

Password: •••••••••••

First factor

Log in with your standard user (AD) credentials

When you have logged in, if OTP is enabled, you will then be prompted for a “Passcode”



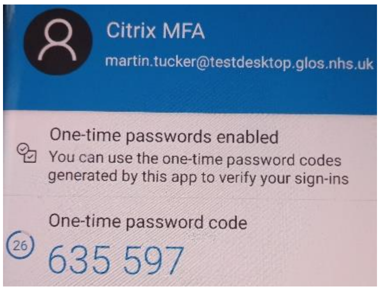
Please log on

User name: martin.tucker

Password: •••••••••••

Passcode: ••••••

Go back to your chosen application where you scanned the QR code and insert the 6 digit code.



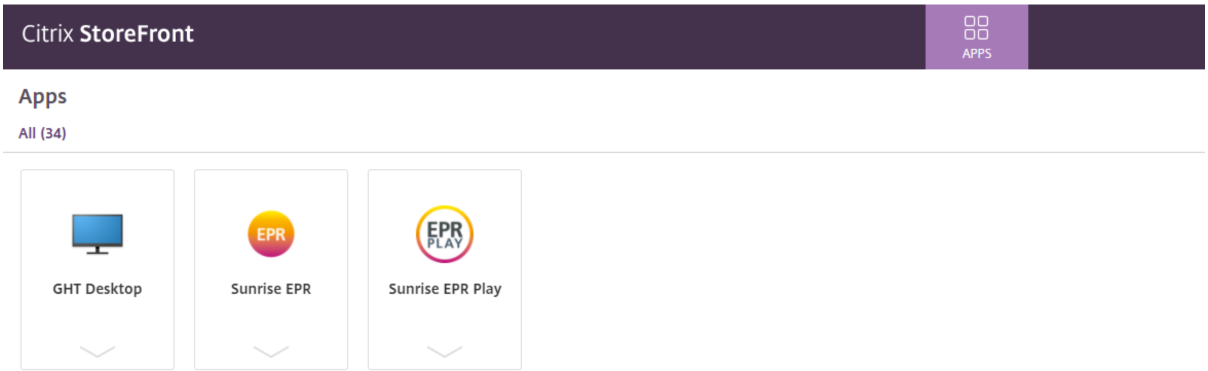
Citrix MFA
martin.tucker@testdesktop.glos.nhs.uk

One-time passwords enabled
You can use the one-time password codes generated by this app to verify your sign-ins

One-time password code
635 597

WARNING: These codes are only valid for 30 seconds. If you have not entered the code and clicked the submit button by this time the code will change and you will have to enter the newly generated code. If the code is not working you may need to do a “Time Correction” in settings.

If successful, you will be presented with the StoreFront as per the picture below (with different applications/desktops)



Citrix StoreFront

Apps
All (34)