

HSC Pharmacy Multi-Factor Authentication Setup

WIN OTP APP

Prepared for
Community Pharmacies
Version 0.1

Prepared by
Noel O'Kane

Date: 25/07/2025

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change Reference

Reviewers

Name	Version Approved	Position	Date

Terms & Abbreviations

Term/Abb	Meaning
HSCNI	Health and Social Care Northern Ireland
MFA	Multi-Factor Authentication
VDI	Virtual Desktop Infrastructure

Table of Contents

Introduction	3
Audience	3
Pre-Requisites	3
Section 1 - Connect to VDI	4
Section 2 – Setup Using WIN OTP App on Surface Pro	10
Section 3 - Logging into VMS using the WinOTP App (daily after set up)	15

Introduction

The purpose of this document is to guide Community Pharmacists on the process of setting up Multi-Factor Authentication use the Authenticator App on an Android or iPhone.

Audience

Community Pharmacies in Northern Ireland.

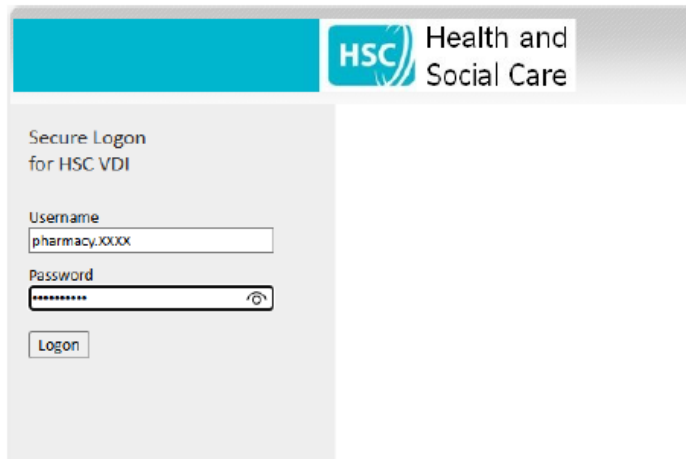
Pre-Requisites

1. Pharmacy PC to log in to VDI
2. Access to Pharmacy / Vaccine email address
3. WIN OTP App downloaded on to device
4. This must be completed with both your Pharmacy and Vaccine email addresses.

Section 1 - Connect to VDI

1. Open Microsoft Edge and navigate to the below web address. The below screen will appear <https://vdi.hscni.net/portal/webclient/#/home>

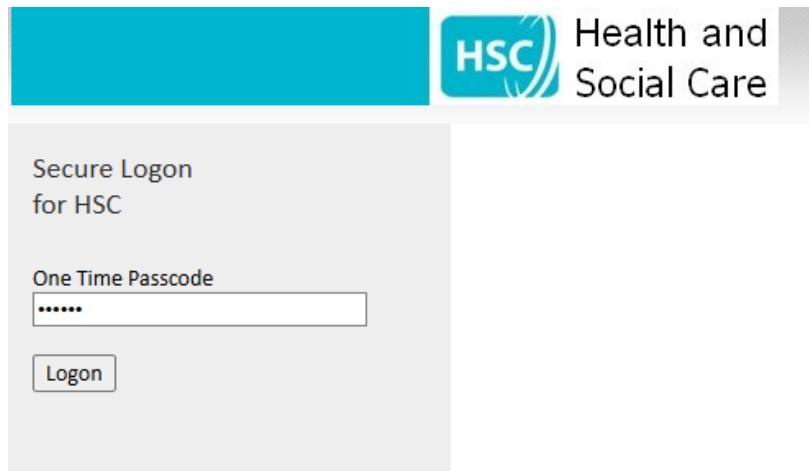
Login with your pharmacy or vaccine usernem. Eg **pharmacy.1234** or **vaccine.1234**. You do not need to put @hscni.net at the end of the username. The numbers correspond to your pharmacy contractor number.



The screenshot shows the login interface for the HSC VDI portal. At the top, there is a blue header with the HSC logo and the text 'Health and Social Care'. Below this, the text 'Secure Logon for HSC VDI' is displayed. The login form contains two input fields: 'Username' and 'Password'. The 'Username' field is populated with 'pharmacy.xxxx'. The 'Password' field is masked with asterisks. A 'Logon' button is located below the password field.



The screenshot shows the login interface for the HSC VDI portal, similar to the one above. The 'Username' field is now populated with 'vaccine.xxxx'. The 'Password' field remains masked with asterisks. The 'Logon' button is still present below the password field.



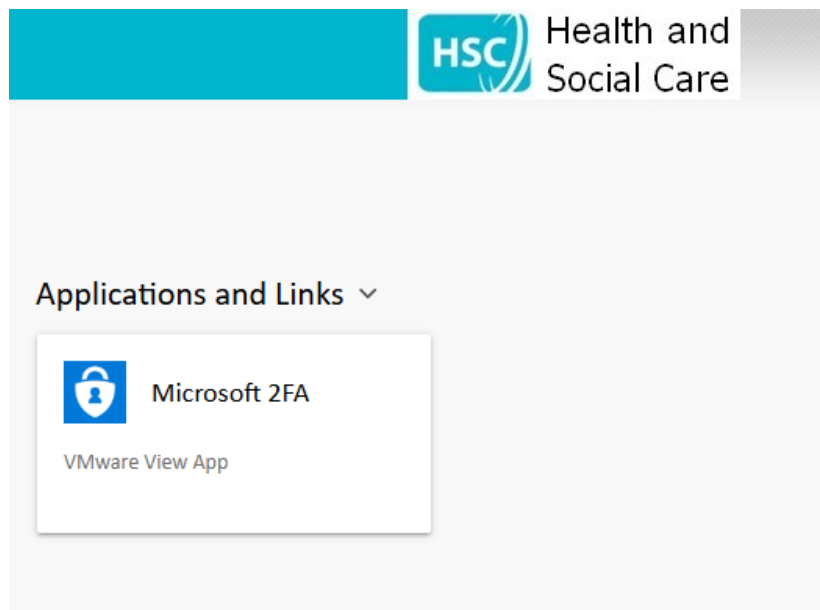
Secure Logon
for HSC

One Time Passcode

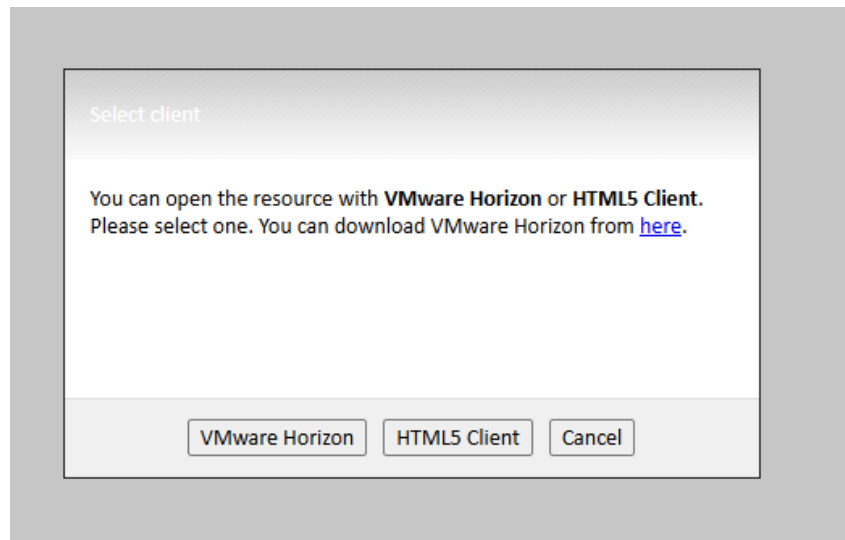
.....

Logon

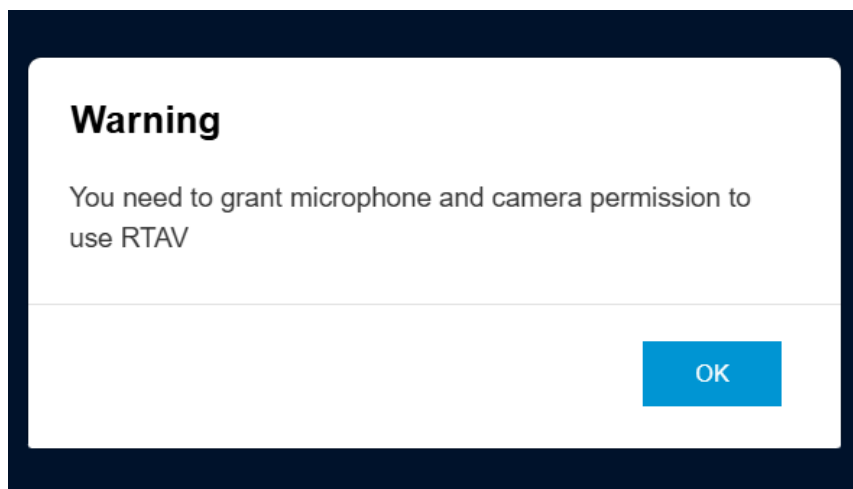
2. Log on to your pharmacy.XXXX@hscni.net email address and you will have received a One Time Passcode, enter this in as shown in the above screenshot and click on Logon.



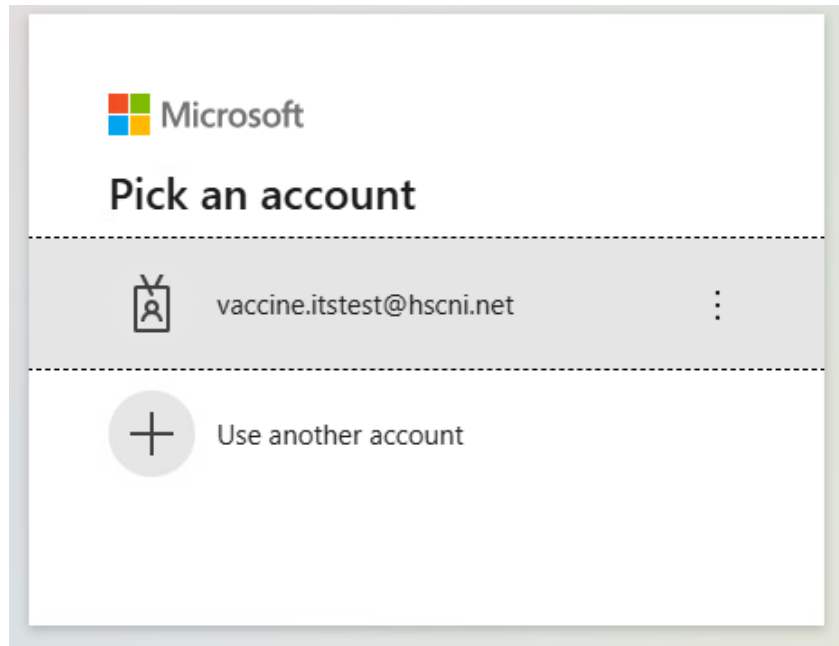
3. Click on the Microsoft 2FA box



4. Click on HTML5 Client – this opens the VMWare Horizon Web Application



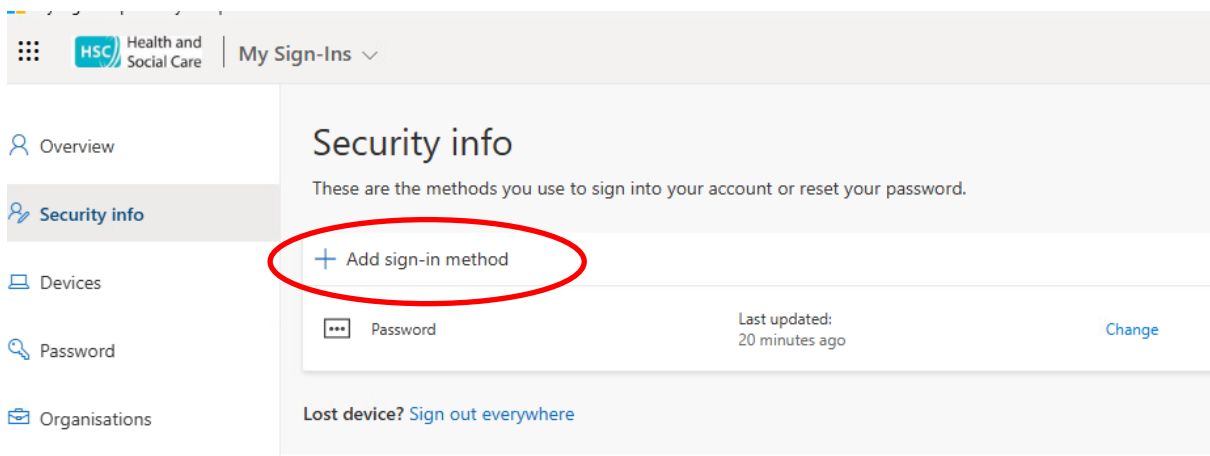
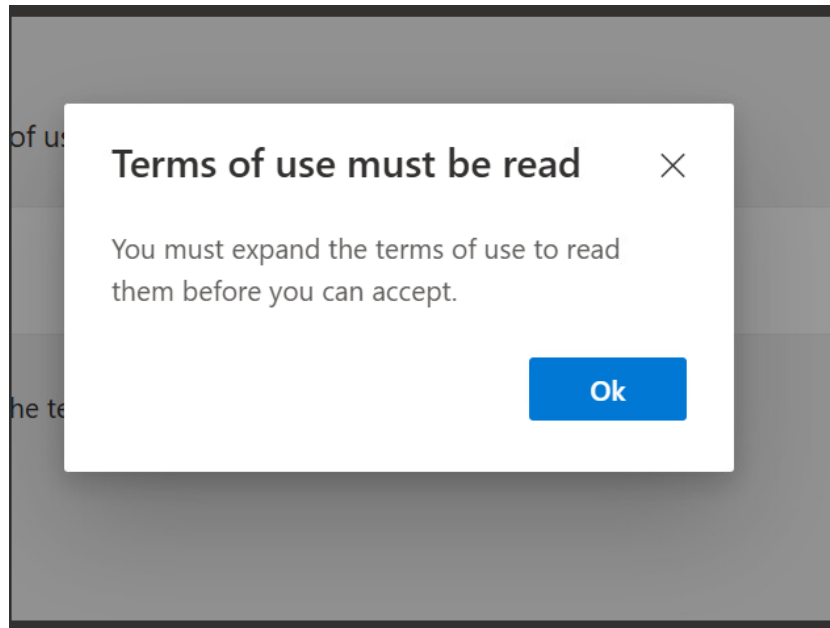
5. If the above screen appears, click on OK. It may appear again on the top left-hand side of Edge, if it does click on Allow



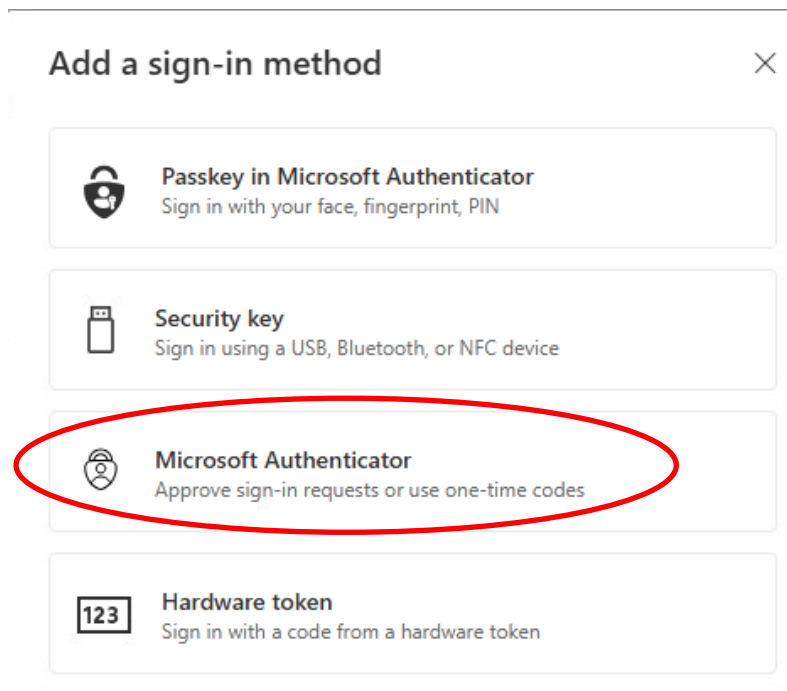
6. Click on your pharmacy/vaccine email – whichever one you have logged in to



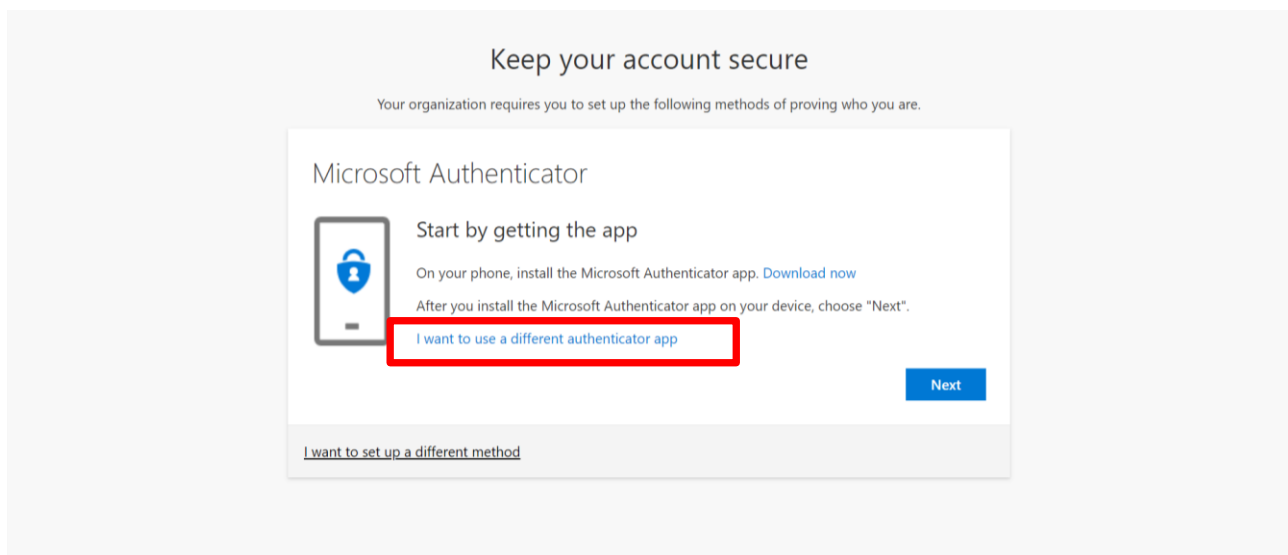
7. You may be presented with a HSCNI Terms of use. You need to click on the arrow to the right of HSC Terms of Use and read the Terms of Use before Clicking on Accept. If you try to click on Accept you get the below screenshot.



8. Click on + Add sign-in method

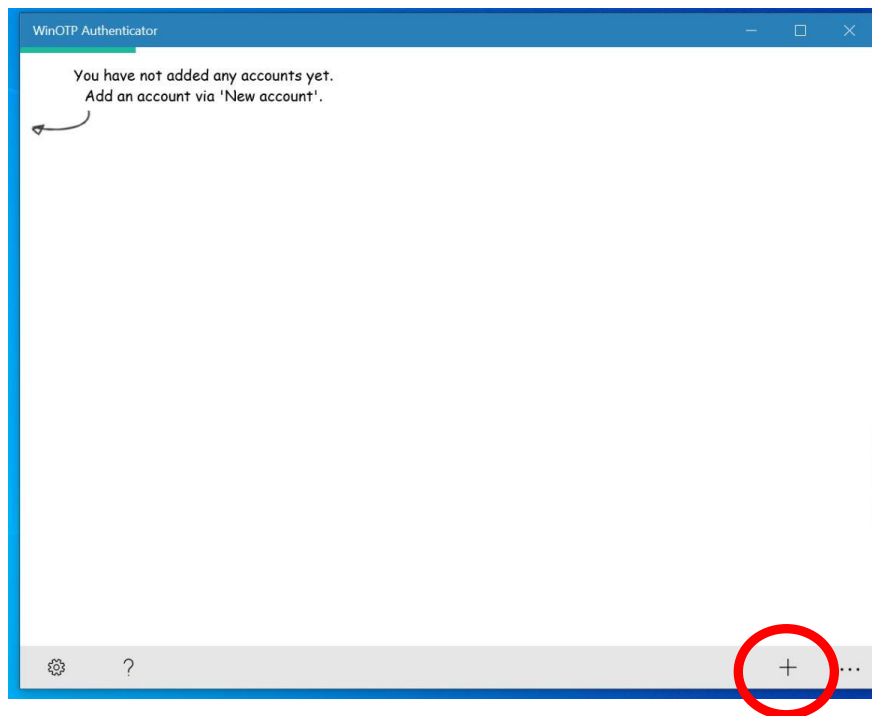


9. Click on Microsoft Authenticator



10. On the next screen click on I want to use a different authenticator app

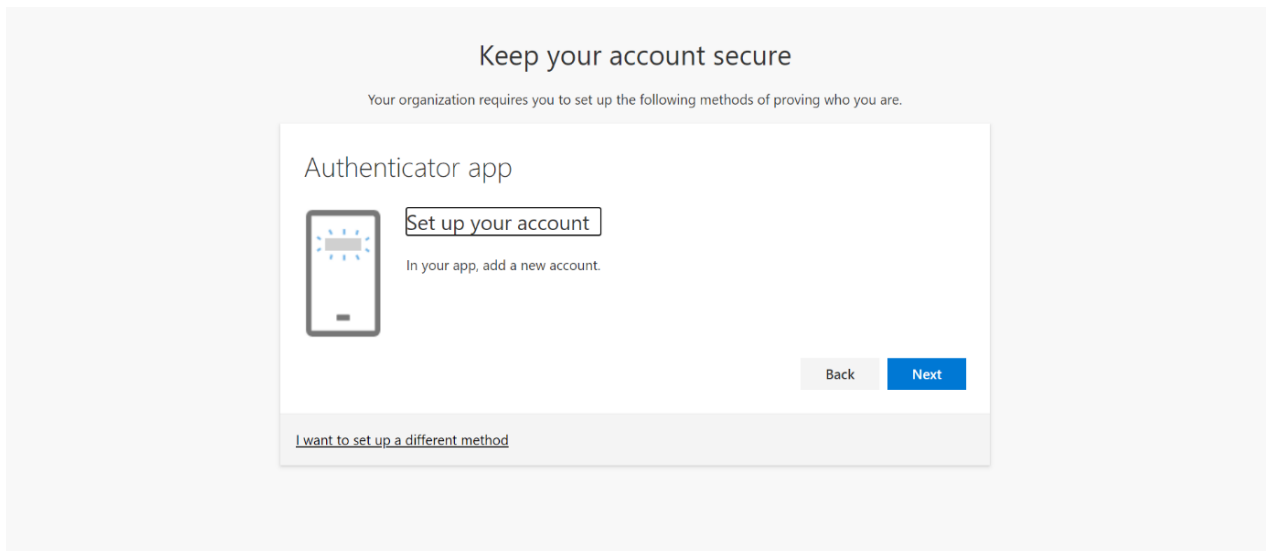
Section 2 – Setup Using WIN OTP App on Surface Pro



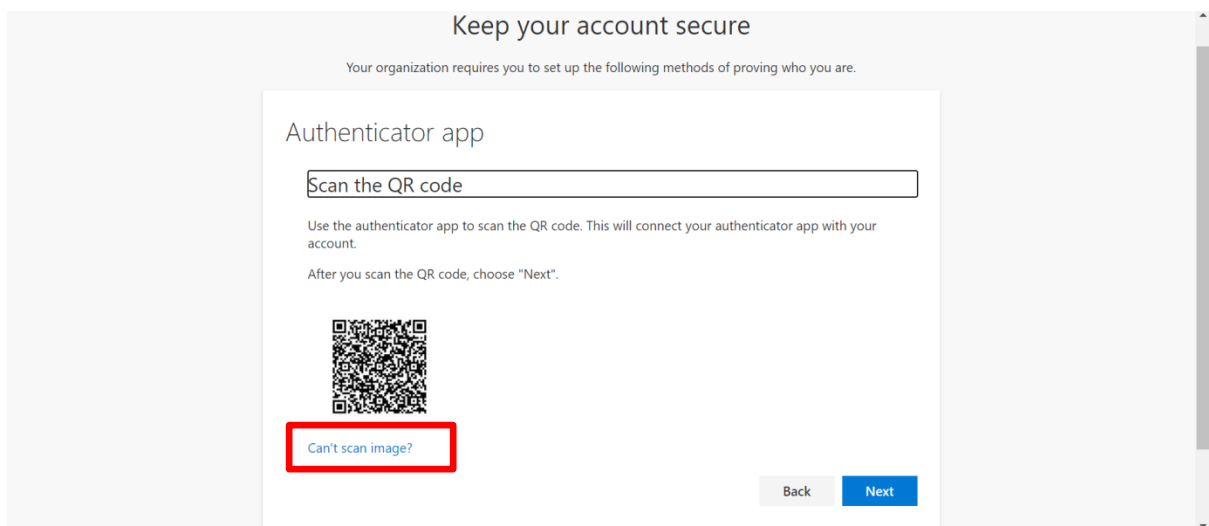
1. Open the Authenticator App on the Surface Pro and tap on the + on the bottom right-hand corner

A screenshot of the WinOTP Authenticator application window showing the 'Add new account' screen. The window has a blue title bar with the text 'WinOTP Authenticator'. Inside the window, there is a message: 'Enter the information that you received from the provider of the two step authentication service. If you have a camera available, you can also use it to scan a QR code if it's available. Dragging a QR code from the website of the service into the app will also read the QR code.' Below the message are three input fields: 'Service', 'Username', and 'Code'. At the bottom is a 'Save' button and a link 'What do I enter where?'.

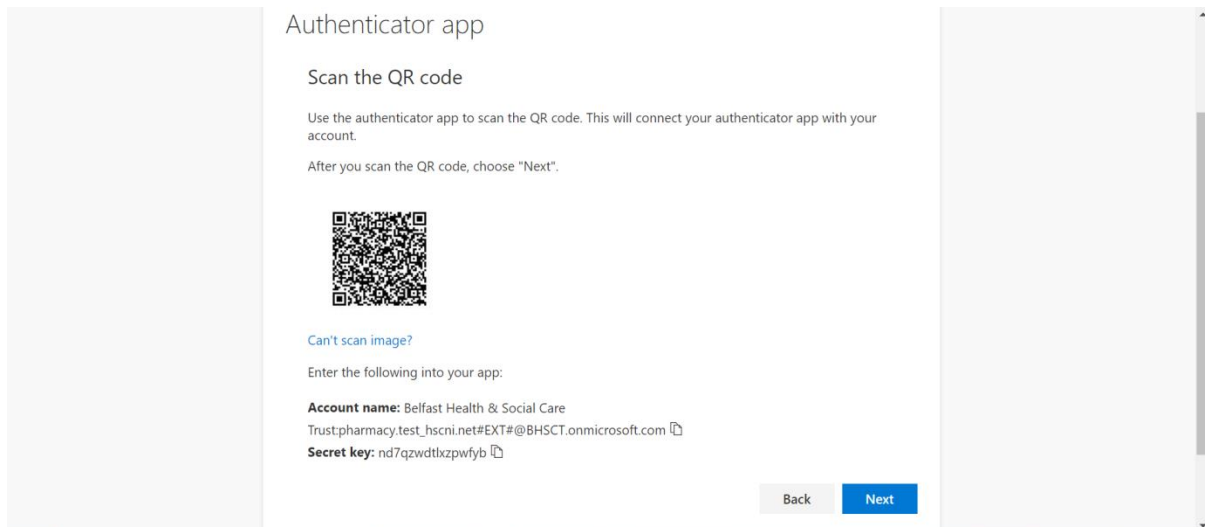
2. Enter the Service as **"HSCNI - VMS"** to differentiate from the current VMS name. Put the pharmacy/vaccine email address in as Username. The Code field will be completed later.



3. On your computer screen click on Next

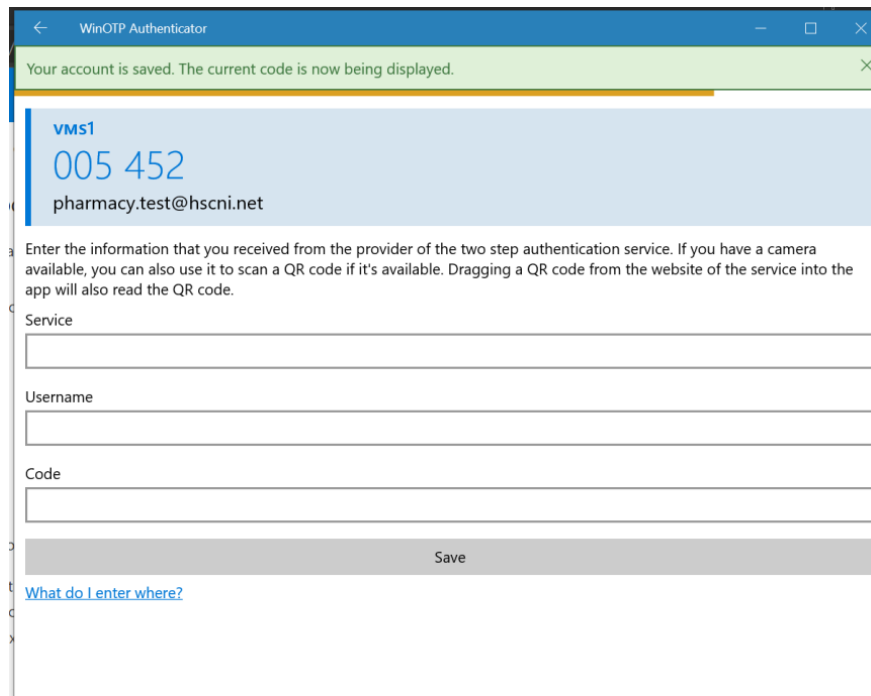


4. A screen with a QR code will then appear, tap on 'Can't scan image?' just below it

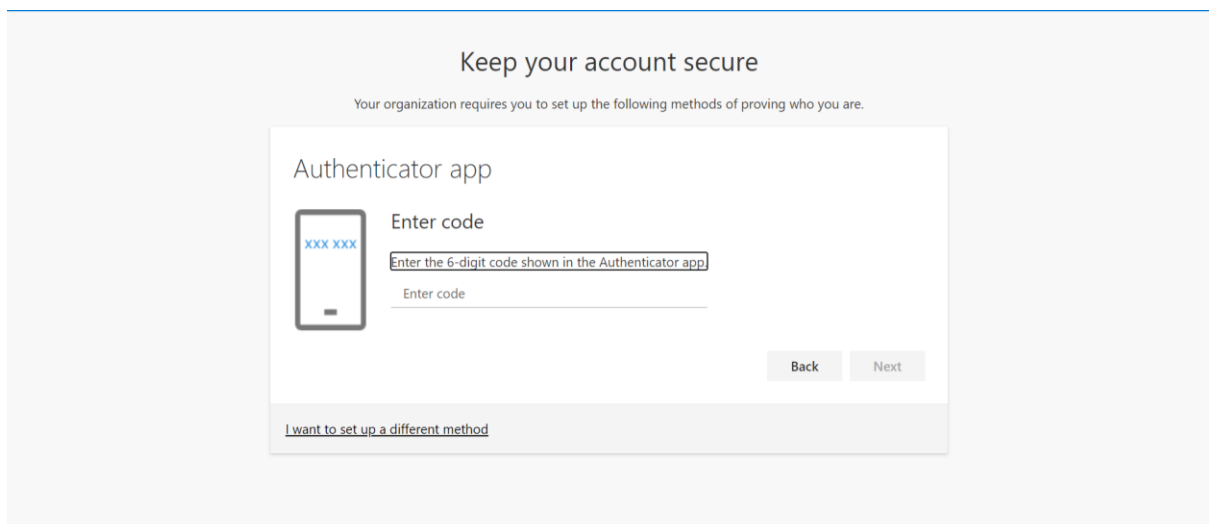


5. A Secret Key will then appear on the PC screen (do not use the code shown in the above screenshot) – this needs to be typed in to the Code field on the Authenticator App on the Surface Pro

6. Type the Secret Key that has appeared on the PC screen into the Code field on the Authenticator App and then tap on Save. A 6-digit code will then be generated on screen as shown in the screenshot below. Make a note of the 6-digit number that has appeared on your Surface Pro

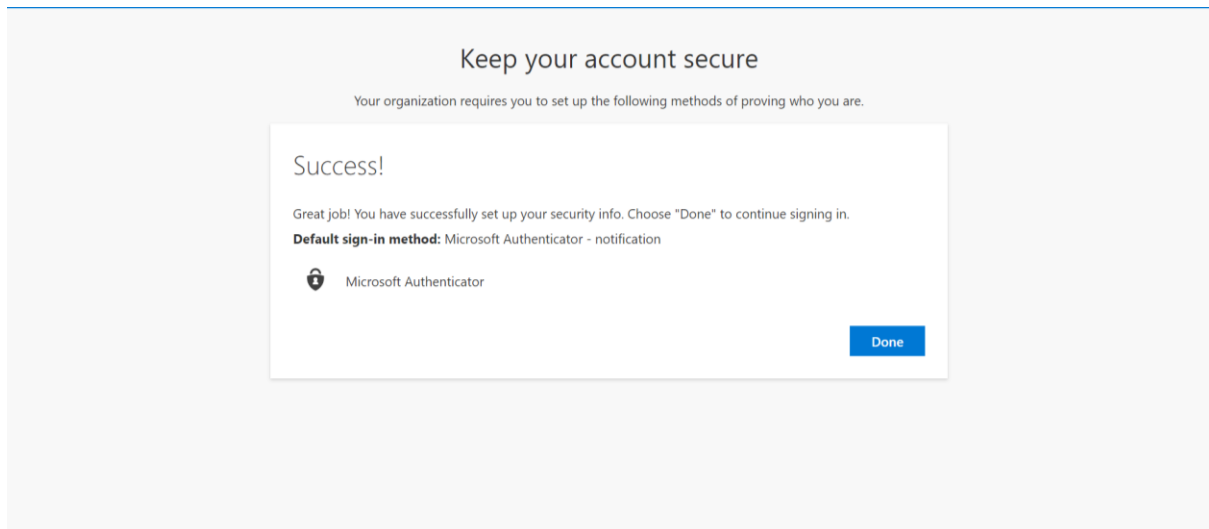


The image shows the WinOTP Authenticator application window. At the top, a green status bar displays the message: "Your account is saved. The current code is now being displayed." Below this, a blue header area contains the text "vms1", a large blue 6-digit code "005 452", and the email address "pharmacy.test@hscni.net". The main content area has a light blue background and contains the following text: "Enter the information that you received from the provider of the two step authentication service. If you have a camera available, you can also use it to scan a QR code if it's available. Dragging a QR code from the website of the service into the app will also read the QR code." Below this text are three input fields labeled "Service", "Username", and "Code". At the bottom of the form is a grey "Save" button and a blue link that says "What do I enter where?".

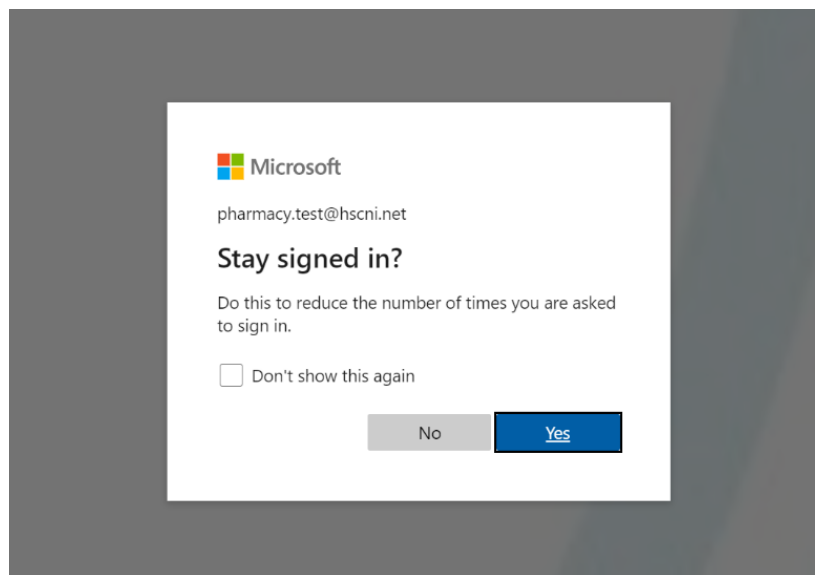


The image shows a "Keep your account secure" screen. At the top, the heading "Keep your account secure" is displayed, followed by the subtext "Your organization requires you to set up the following methods of proving who you are." Below this is a white box titled "Authenticator app". Inside this box, on the left, is an icon of a smartphone displaying "xxx xxx". To the right of the icon is the text "Enter code" and a text input field with the placeholder "Enter the 6-digit code shown in the Authenticator app". Below the input field is a smaller "Enter code" label. At the bottom right of the white box are two buttons: "Back" and "Next". At the bottom left of the white box is a link that says "I want to set up a different method".

7. On the PC click on Next on the screen where the QR code appeared and then enter the 6-digit number you took a note of and then click on Next



8. You should then be presented with the above screen. MFA has been registered and you can click on Done



9. You may be presented with a screen asking if you wish to stay signed in, if you select '**No**' you will need to use your username and password along with the 6 digit number from the authenticator app each time you sign in. If you select '**Yes**' your details will be stored for 1 day
10. If done using the pharmacy email address, please repeat with the vaccine email address

Section 3 - Logging into VMS using the WinOTP App (daily after set up)

1. Navigate to <https://vms.healthandcareni.net/pharmacy>
2. Select Sign in
3. Enter your email address and select “Next”
4. Enter your password and select “Next”
5. Open up the WinOTP app and enter in the six digit number.
6. Select “Next” and your sign in will be completed.

If you have any issues with your Multi-Factor Authentication log a call with the BSO Service Desk for Attention of the Cloud Services Team – include as much detail as possible and any error messages you may be receiving.

If you get a new Mobile phone or Tablet Device, you will need to log a call with the BSO Service Desk to get the Multi-Factor Authentication reset. You will then need to follow these instructions again to set it up again.

Service Desk email address is – supportteam@hscni.net