Purpose:

The purpose of this document is to guide you through the new Citrix Windows 10 Desktop access setup process to support working remotely.

Please note: The Citrix desktop is designed primarily for PC and Laptop users and is **not** supported on **iPad / Android.**

Prerequisites:

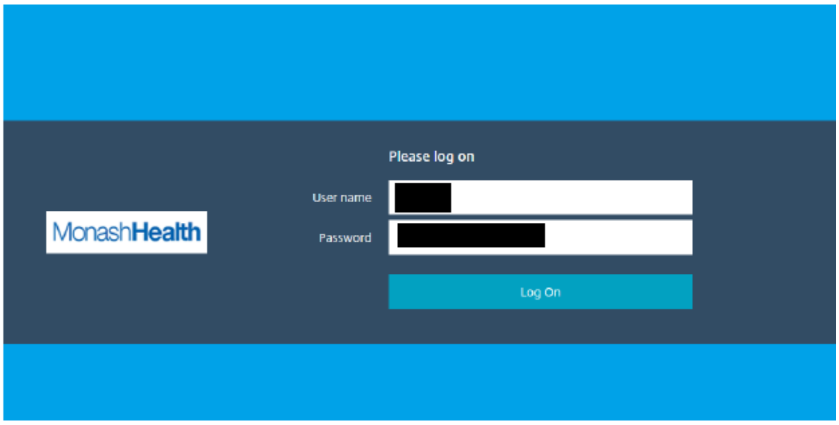
- Your Mobile number is already registered and you can access the Self Service portal. (https://selfservice.monashhealth.org) If not, contact IT Service Desk on 9594 7255 (Option 1)
- The use of the Google Authenticator app is the preferred method for obtaining the 2 Factor Authentication code.
- Citrix receiver is installed. (https://citrix.com/reciever)

What's included in this document:

Section A: Monash Health new Citrix Windows10 Desktop Access Instructions
Section B: Frequently Asked Questions
Section C: Step by Step instructions on enrolling an Authenticator

Section A: Monash Health Remote Citrix Windows 10 Desktop Access Instructions

1. Click on this link: http://portal.monashhealth.org, click on “Allow” to open the link. **You only need to allow this once**.



MonashHealth

Please log on

User name [redacted]

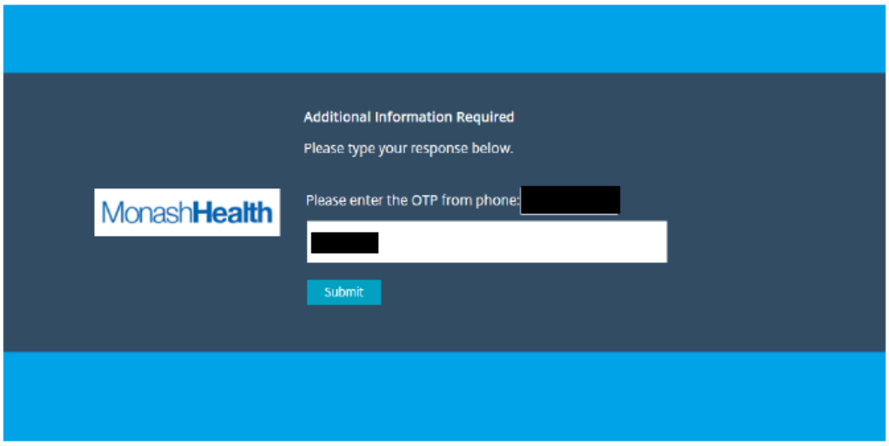
Password [redacted]

2. Enter your Monash Health username and password and click “**Log On**”.

This is the same information used to log into your computer at Monash Health. For example:

User Name: 600001 **Password**: [your password]

3. If you have previously configured your account to utilise Authenticator, enter the token code, alternatively an SMS passcode will be sent to the mobile phone number that has been registered with your account for remote access use. Enter the SMS or Authenticator Passcode you’ve received in the field provided and click on “**Submit”**.



MonashHealth

Additional Information Required

Please type your response below.

Please enter the OTP from phone: [redacted]

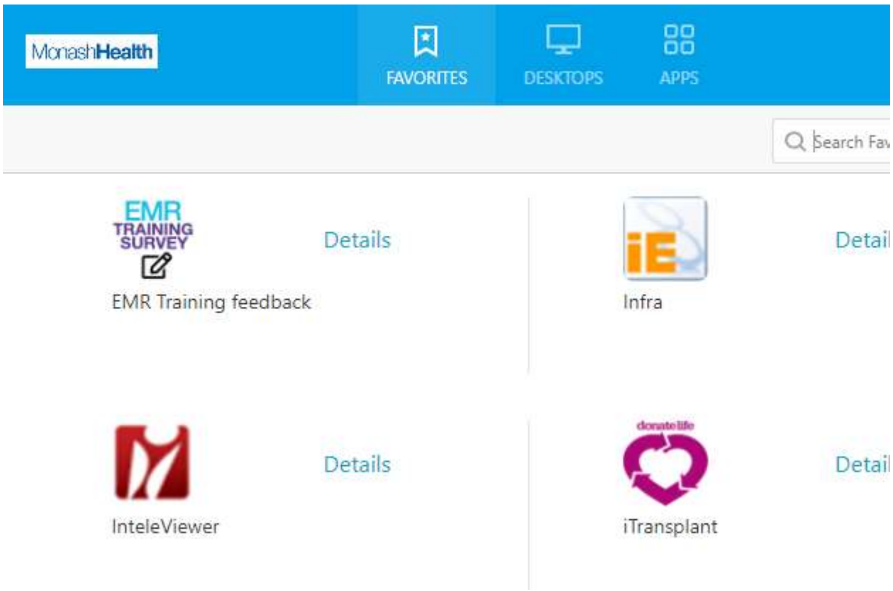
[redacted]

4. To log into the Citrix Access Gateway, you need to have the Citrix Client installed. If this is not installed, you will be prompted to download it. **You only need to install this once**.

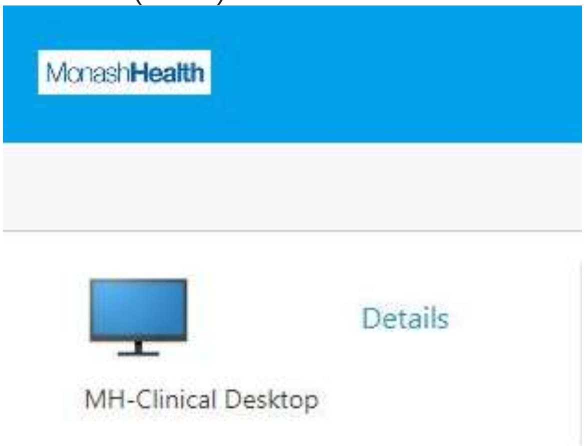
Note: All Monash Health based computers should already have the Citrix Client installed on it.

5. Once the Citrix Client has been installed you will be presented with three options on the top of the page: “**FAVORITES**”, “**DESKTOPS**” and “**APPS**”.

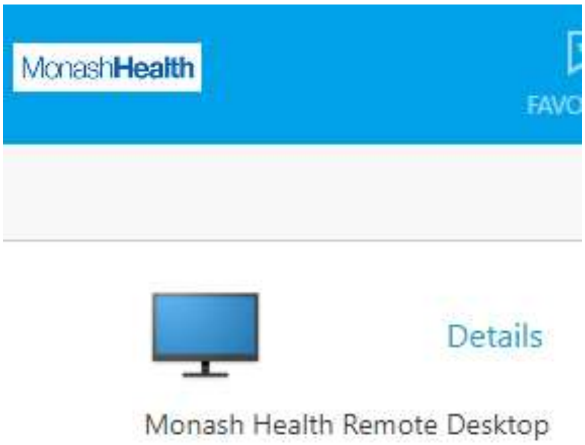
Note: If the “DESKTOPS” option does not appear, please log a ticket via Central.



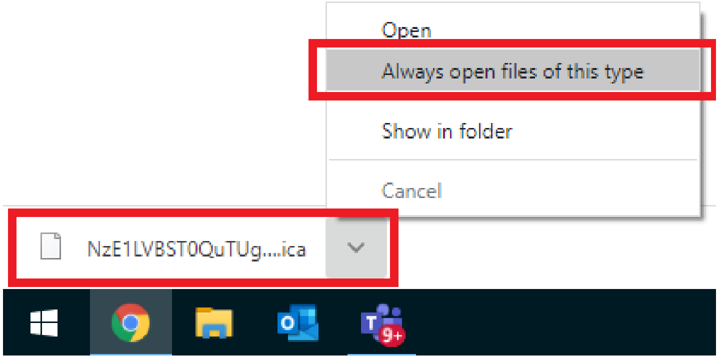
6. Select “**DESKTOPS**”, the Desktop name is dependent on user roles:
   - All Clinical (TOTO) users will have access to: *MH-Clinical Desktop*.



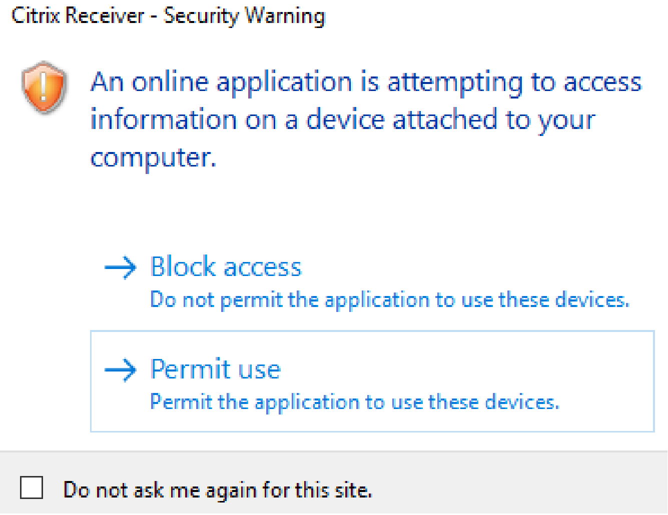
   - All non-clinical (admin) staff will have access to: *Monash Health Remote Desktop*



7. Once you click on the presented Remote Desktop, a Citrix ‘.ica’ file will be shown in the **lower-left** corner with a random name (example: NzE1LVBST0QuTug..ica). Ensure you click the arrow and select ‘Always open files of this type’ if prompted.



If you are presented with below screen, click on “**Permit use**” to continue. Ticking the box of “**Do not ask me again for this site**” will choose this option as default for future.



Citrix Receiver - Security Warning

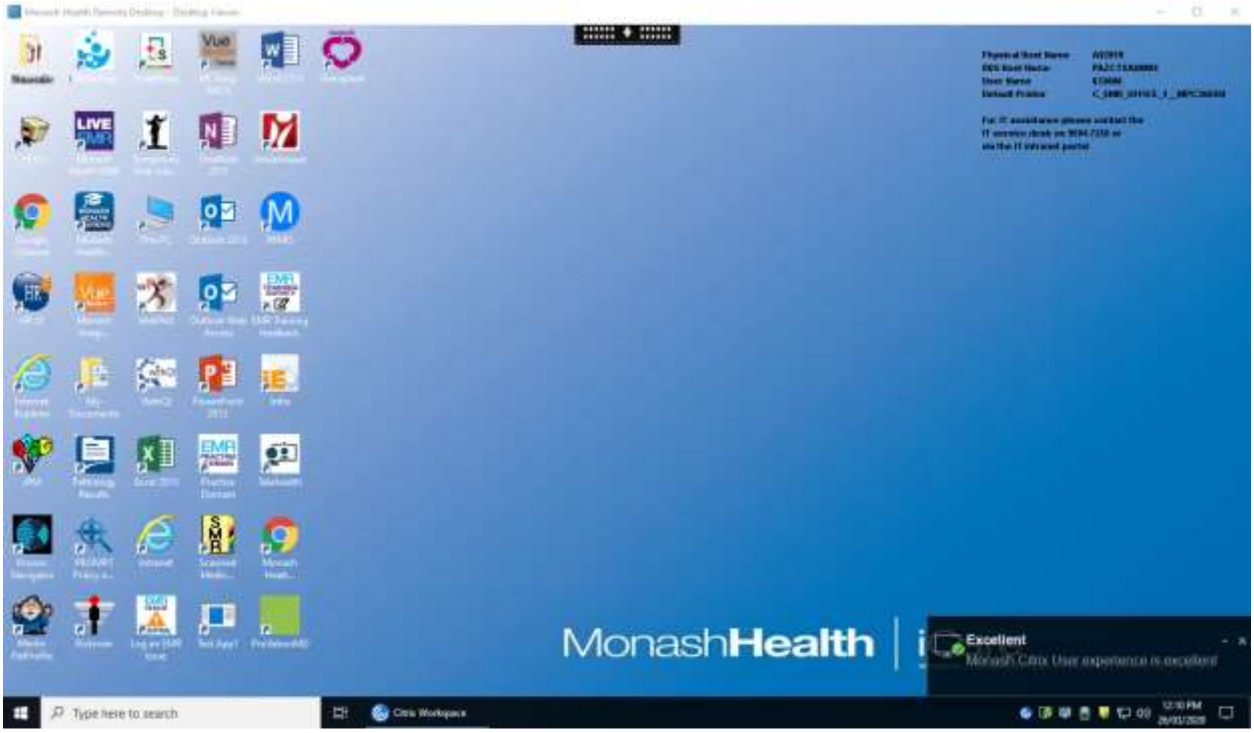
An online application is attempting to access information on a device attached to your computer.

→ Block access
Do not permit the application to use these devices.

→ Permit use
Permit the application to use these devices.

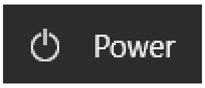
□ Do not ask me again for this site.

8. Once your desktop has launched, it will show all the applications you have access to.

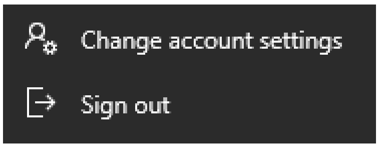


9. To log out of Citrix Desktop,

- Place your cursor on the bottom left hand corner on the windows icon ⊞
- Click on Power icon then “Disconnect” to disconnect from the session.

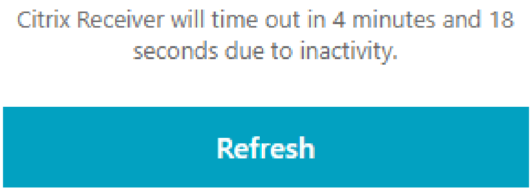


- Alternatively, select your username 👤, then choose “Sign out” to log out your session.



Section B: Frequently Asked Questions

Q: I get the below error; does that mean my Citrix Desktop will be terminated?



Citrix Receiver will time out in 4 minutes and 18 seconds due to inactivity.

A: No, the message is due to inactivity of portal.monashhealth.org website, your Citrix Desktop will not be affected.

Q: Can I use the Citrix Desktop if I am the Monash Health VPN?

A: No, the Citrix Desktop replaces VPN, please disconnect the VPN before proceeding.

Q: I get an error when I try to open i.PM, BOS and some other applications.

A: Please Sign Out (not Disconnect) your session, wait for 5 minutes for your profile to be created then log back in. **Refer to above on how to log out Citrix session.**

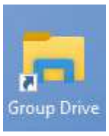
Q: I can't find Webex or Office 365 in the Citrix desktop.

A: it's not enabled within Citrix Desktop, you should run Webex and Office 365 from the desktop of your local computer.

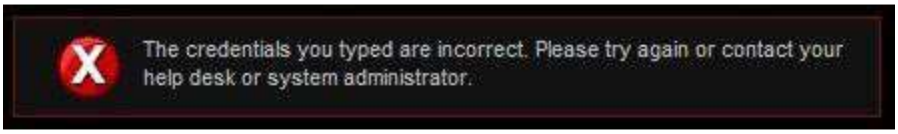
Q: I couldn't find an Application I normally use for my work.

A: Log a call via Central ensure you quote "Citrix remote access application request" is in the heading of the request.

Q: Where can I access my drives?

A: On the desktop, there is Group Drive  has all drives and folders you have access to.

Q. When I log on http://portal.monashhealth.org I get the following error message



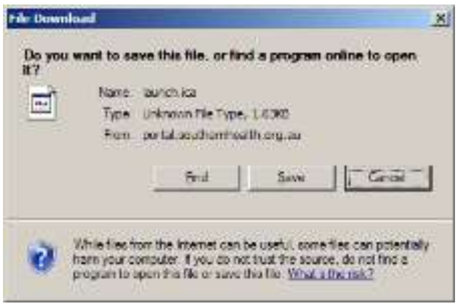
The credentials you typed are incorrect. Please try again or contact your help desk or system administrator.

A: Ensure that you are using the same username and password that you use to log into the computers at Monash Health and you have entered the correct Passcode. You have approximately one minute to enter the SMS passcode when prompted. If you need your password reset, please contact the IT Service Desk.

Q. How do I know what mobile phone is registered with my account for remote access use?

A: Contact IT Service Desk on 9594 7255 (Option 1), they can confirm / update the mobile phone details.

Q. When trying to launch an application I get prompted to download a file:



File Download

Do you want to save this file, or find a program online to open it?

Name: launch.ica
Type: Unknown File Type, 1.63KB
From: portal.southernhealth.org.au

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

A: You will get this message if the Citrix Client has not been installed. Close down all browser Windows and connect to http://citrix.com/receiver this should prompt you again to install the Citrix Client (Refer to step 4 above)

Q: I can't access enrolled authenticator.

A: If for whatever reason you are unable to access your enrolled authenticator (e.g. factory reset on your phone), you can use the 'Problems with the temporary code?' link when logging in to select a different 2FA method.

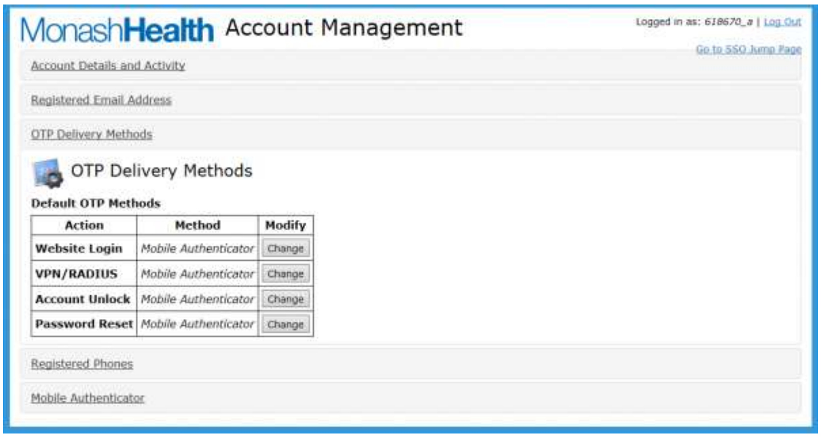
Q: My Google Authenticator codes aren't working (Android)

A:

1. Go to the main menu on the Google Authenticator app.
2. Tap More Settings.
3. Tap Time correction for codes.
4. Tap Sync now.

Q: How can I change authentication defaults?

A. If you wish, you can use a different default method for different activities. You can manage this by logging into https://selfservice.monashhealth.org/ and looking in the 'OTP Delivery Methods' section.



MonashHealth Account Management

Logged in as: 618670_a | Log Out

Go to SSO Jump Page

Account Details and Activity

Registered Email Address

OTP Delivery Methods

OTP Delivery Methods

Default OTP Methods

Action	Method	Modify
Website Login	*Mobile Authenticator*	Change
VPN/RADIUS	*Mobile Authenticator*	Change
Account Unlock	*Mobile Authenticator*	Change
Password Reset	*Mobile Authenticator*	Change

Registered Phones

Mobile Authenticator

Q: Kronos won't display data correctly.

A: The first time you launch Kronos it may take time to install the Java applet (around 5 minutes). Please wait for this to process to complete and 'Run' any pop-ups that appear. If Kronos does not display data after running the two different pop-ups, close and browser window and re-launch Kronos.

For any other issues, please log a call via Central.

Section C: Step by step instructions on setting up an Authenticator

Install Google Authenticator

If you set up 2-Step Verification, you can use the Google Authenticator app to receive codes even if you don't have an Internet connection or mobile service.

iPhone & iPad

To use Google Authenticator on your iPhone, iPod Touch, or iPad, you'll need:

- The latest operating system for your device
- 2-Step Verification turned on
- (optional to set up with QR code) iPhone 3G or later

Download the app from the Apple App Store

INSTALL GOOGLE AUTHENTICATOR

(http://appstore.com/googleauthenticator)

Android

To use Google Authenticator on your Android device, you'll need:

- Android version 2.1 or later
- 2-Step Verification turned on

Download the app from the Google Play Store

INSTALL GOOGLE AUTHENTICATOR

(https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)

Enrolling an Authenticator

As part of Cyber Security improvement, a new 2-factor authentication method is introduced to provide stronger security while accessing external Monash Health sites.

1. Download and Install one of the 2 Authenticator apps on your Smart phone:

- Google Authenticator
- Microsoft Authenticator

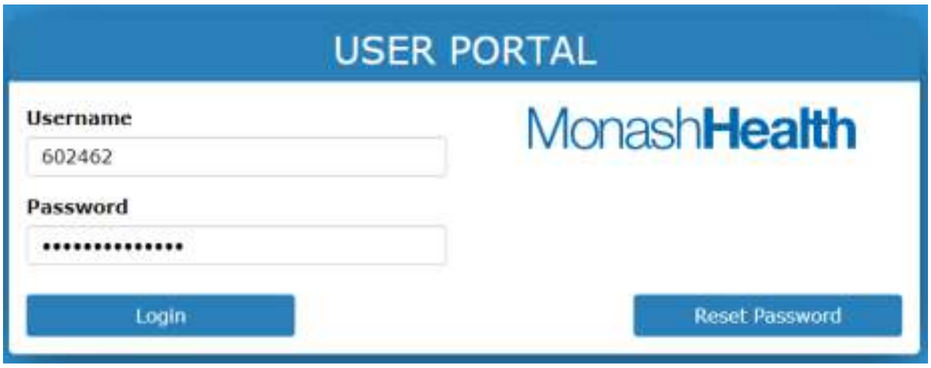
2. Log a call via Central to request Google Authenticator is added to your Active Directory Group

Please note: only move onto step 3 if you have received confirmation step 2 has been processed.

3. Access https://selfservice.monashhealth.org , you will be prompted to enroll the mobile authenticator:

Note: Assumes your Mobile number is already registered as it will send the Temporary code to the registered mobile

4. Enter your Monash Health Username and password and click **Login**

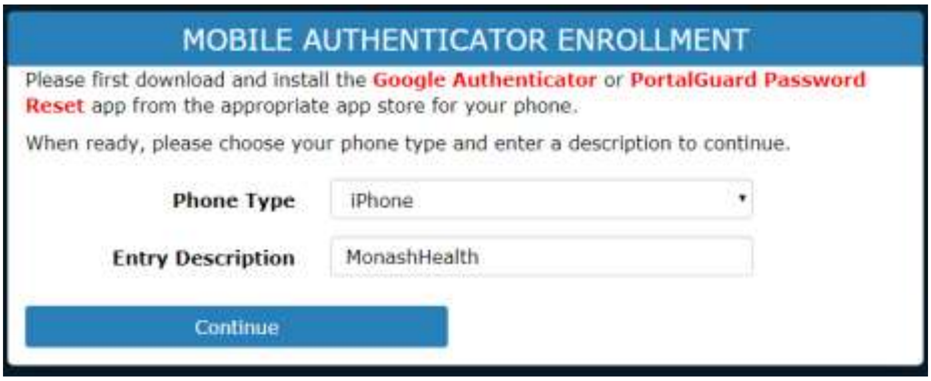


USER PORTAL

Username: 602462

Password: •••••••••••••••

5. If you receive the below screen, please ensure that you read the information carefully.



MOBILE AUTHENTICATOR ENROLLMENT

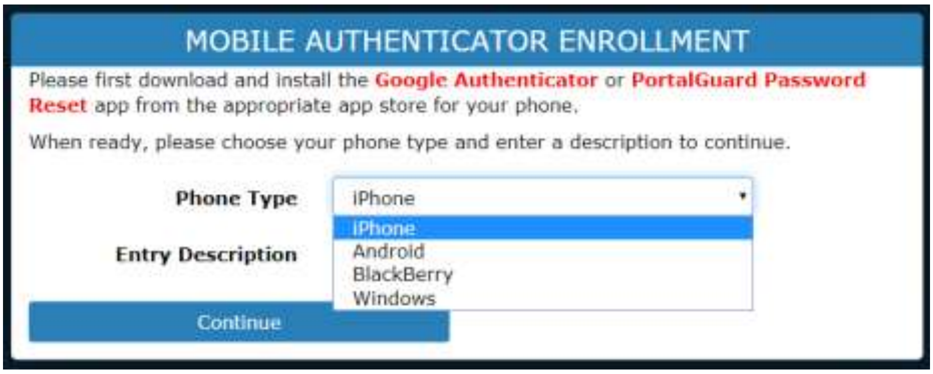
Please first download and install the **Google Authenticator** or **PortalGuard Password Reset** app from the appropriate app store for your phone.

When ready, please choose your phone type and enter a description to continue.

Phone Type: iPhone

Entry Description: MonashHealth

6. Select the type of phone you have. For example Android phone or iPhone.



MOBILE AUTHENTICATOR ENROLLMENT

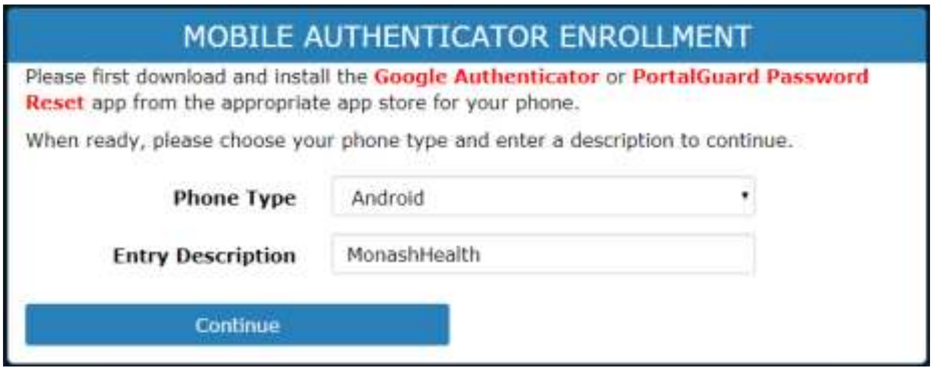
Please first download and install the **Google Authenticator** or **PortalGuard Password Reset** app from the appropriate app store for your phone.

When ready, please choose your phone type and enter a description to continue.

Phone Type iPhone

Entry Description

7. Enter a Description type “MonashHealth” if not already there and click on **Continue**:



MOBILE AUTHENTICATOR ENROLLMENT

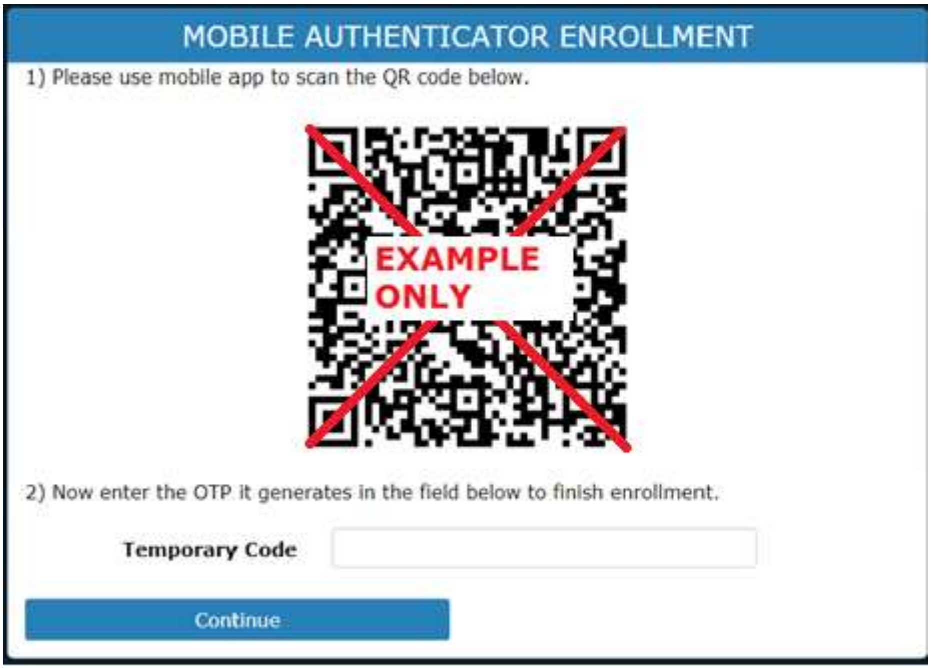
Please first download and install the **Google Authenticator** or **PortalGuard Password Reset** app from the appropriate app store for your phone.

When ready, please choose your phone type and enter a description to continue.

Phone Type Android

Entry Description MonashHealth

8. You will be presented with the Mobile Authenticator Enrolment dialogue box on your computer screen as per example below.



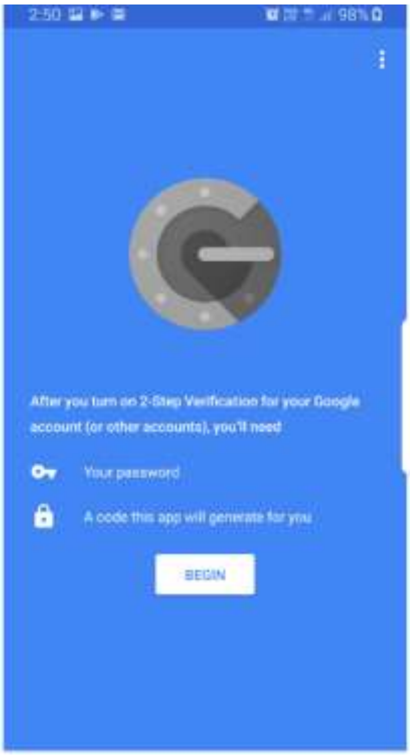
MOBILE AUTHENTICATOR ENROLLMENT

1) Please use mobile app to scan the QR code below.

2) Now enter the OTP it generates in the field below to finish enrollment.

Temporary Code

9. Open the Google Authenticator Application located on your mobile device and Tap Begin.

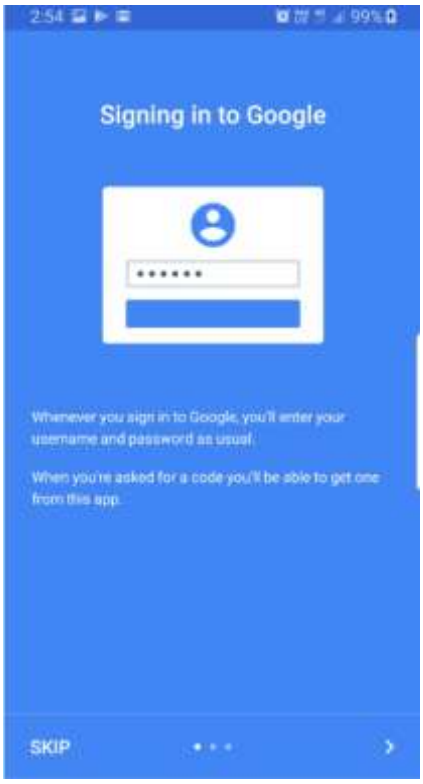


After you turn on 2-Step Verification for your Google account (or other accounts), you'll need

Your password

A code this app will generate for you

10. Tap on **SKIP** to continue (if prompted)

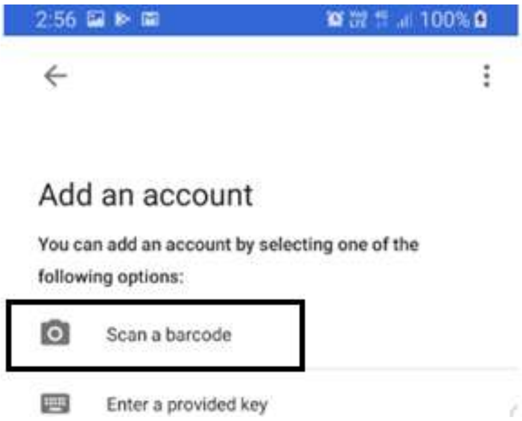


Signing in to Google

Whenever you sign in to Google, you'll enter your username and password as usual.

When you're asked for a code you'll be able to get one from this app.

11.Tap on **Scan a Barcode** on the screen.



2:56 100%

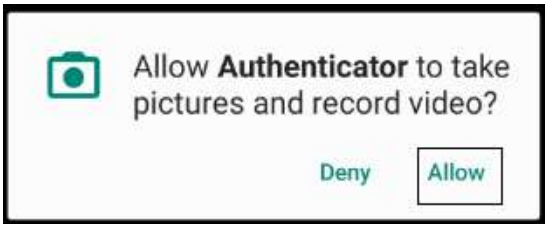
Add an account

You can add an account by selecting one of the following options:

Scan a barcode

Enter a provided key

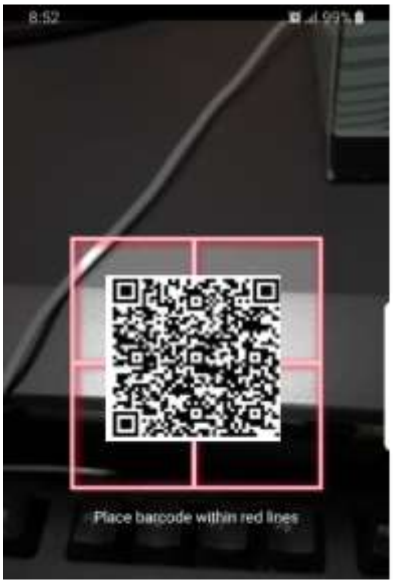
12. Tap **Allow** for the Authenticator to access the camera.



Allow **Authenticator** to take pictures and record video?

Deny Allow

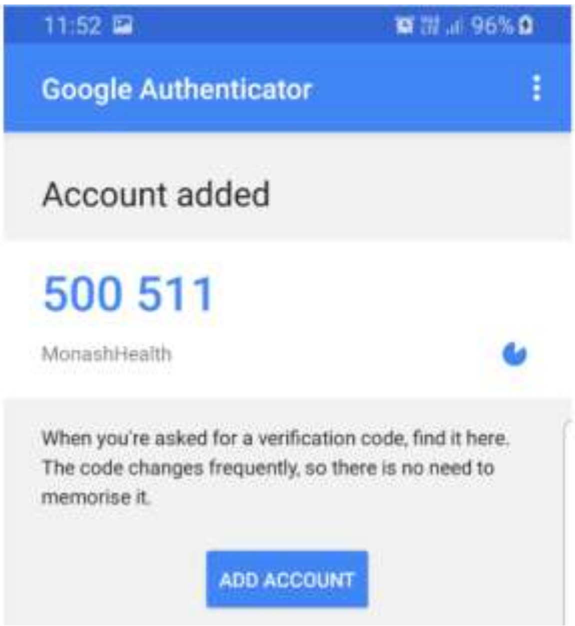
13. Using your Mobile Phone, scan the QR Code displayed on the Computer screen



8:52

Place barcode within red lines

14. A temporary code will appear on your mobile Device under the Google Authenticator program. Please Note: A new temporary code is generated every 60 seconds



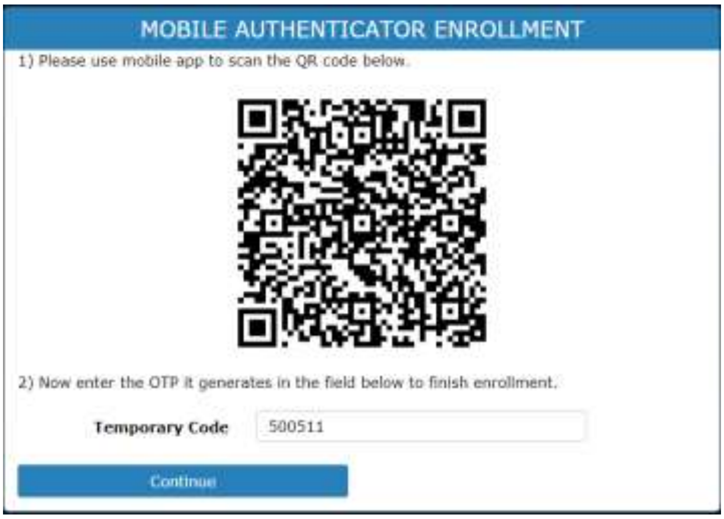
Account added

500 511

MonashHealth

When you're asked for a verification code, find it here. The code changes frequently, so there is no need to memorise it.

15. Enter the Google Authenticator code displayed on your device in the temporary Code Field and press Continue.



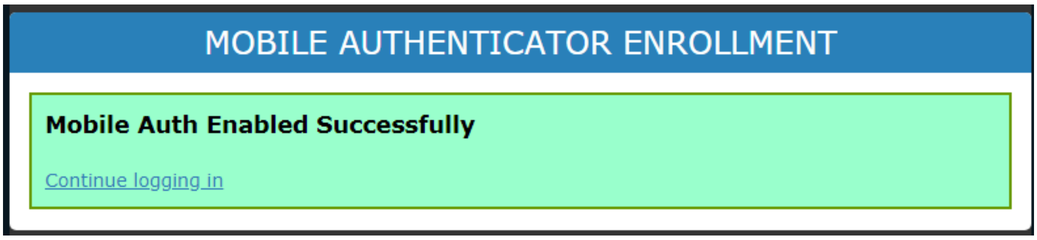
MOBILE AUTHENTICATOR ENROLLMENT

1) Please use mobile app to scan the QR code below.

2) Now enter the OTP it generates in the field below to finish enrollment.

Temporary Code: 500511

16. This will inform you that the Mobile Authenticator enrolment has been successful.



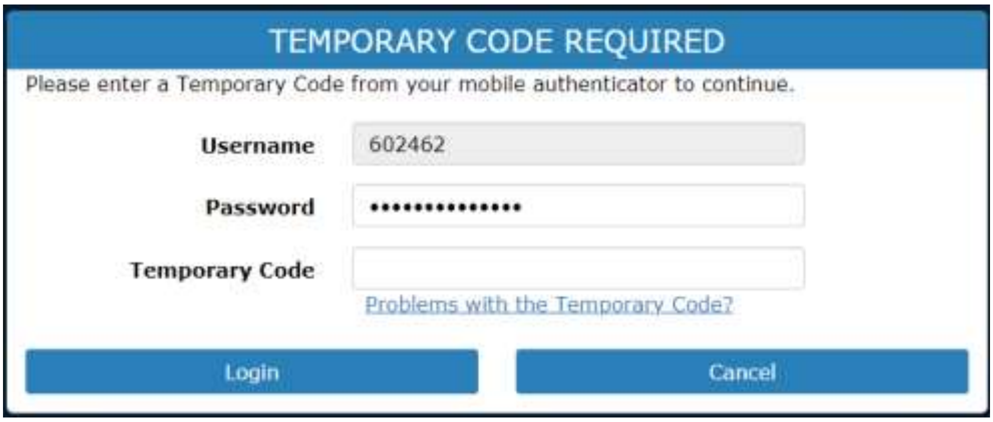
MOBILE AUTHENTICATOR ENROLLMENT

Mobile Auth Enabled Successfully

Continue logging in

17. Select “Continue Logging in”.

18. A Dialog box will appear asking for a temporary password to be entered.



TEMPORARY CODE REQUIRED

Please enter a Temporary Code from your mobile authenticator to continue.

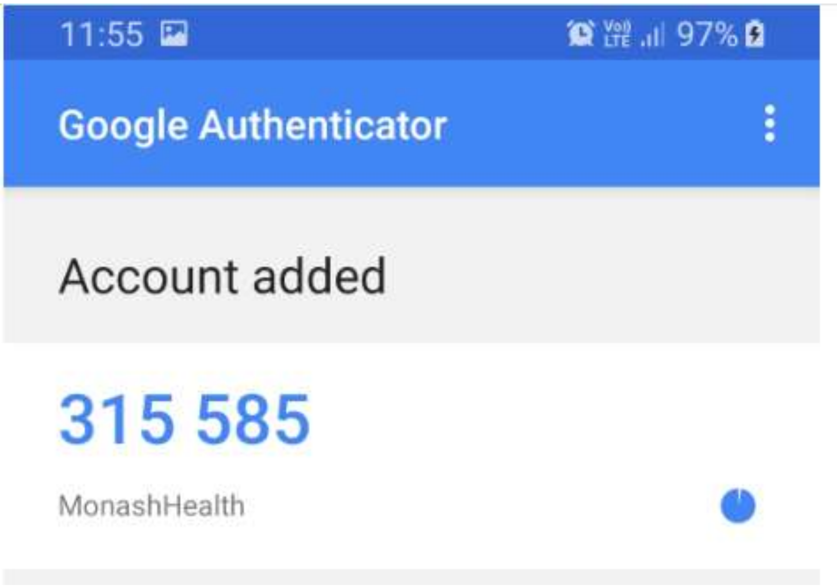
Username 602462

Password ••••••••••••••

Temporary Code

Problems with the Temporary Code?

19. For the temporary code, use the Google Authenticator app on your mobile device.

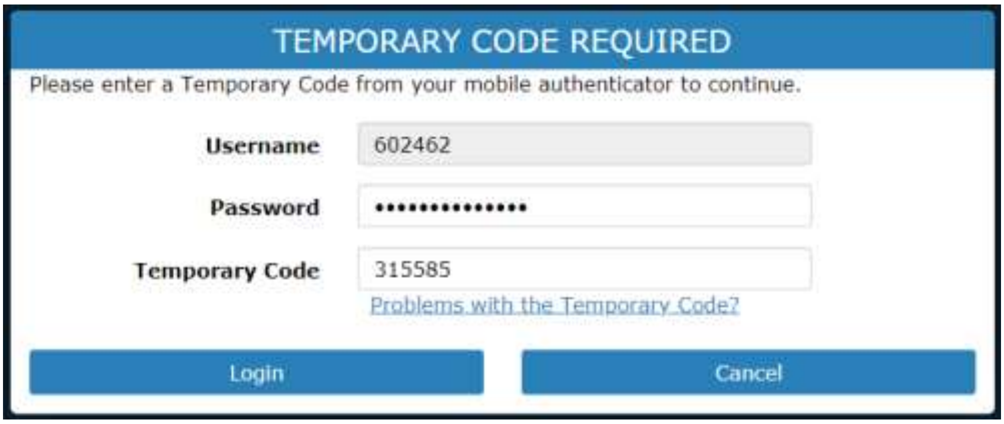


Account added

315 585

MonashHealth

20. Enter the passcode as displayed in the temporary code field and click on Login.



TEMPORARY CODE REQUIRED

Please enter a Temporary Code from your mobile authenticator to continue.

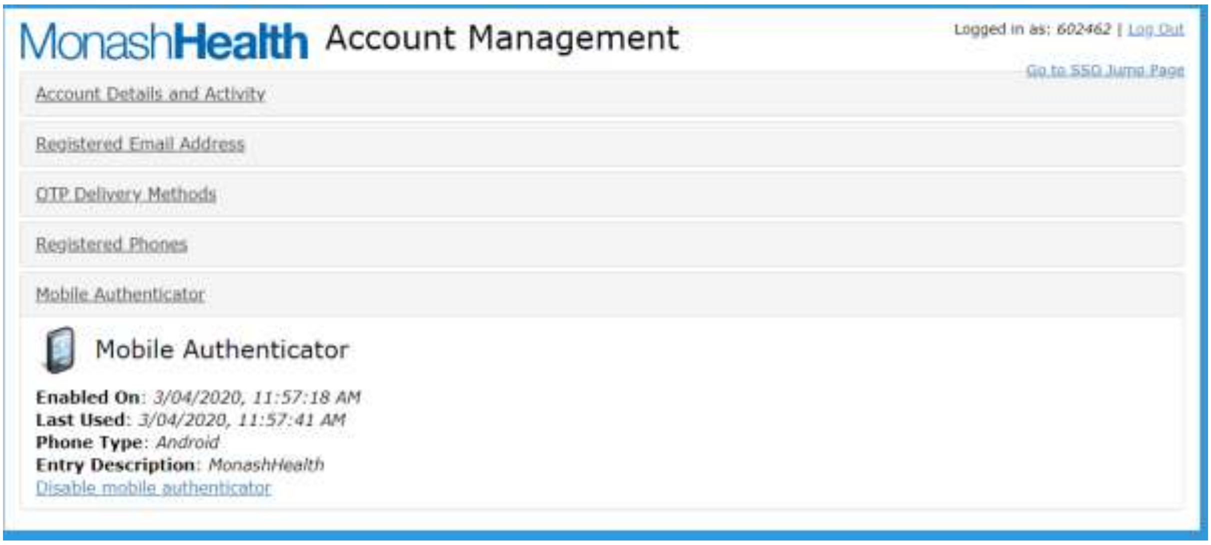
Username 602462

Password ••••••••••••••

Temporary Code 315585

Problems with the Temporary Code?

21. You are now registered in the self-service portal to use Two Factor Authentication (2FA).



Enabled On: *3/04/2020, 11:57:18 AM*
Last Used: *3/04/2020, 11:57:41 AM*
Phone Type: *Android*
Entry Description: *MonashHealth*
Disable mobile authenticator

22. Click on **Log Out** to exit the Self Service Portal.