What is Microsoft Multi-Factor Authentication?

Shared Health has introduced stronger cyber security protection called **Microsoft Multi Factor Authentication (MFA)**. MFA requests additional verification of your identity when trying to access any application protected by MFA, including *MS Teams*, *Outlook Mobile*, or *applications currently using Imprivata Two-Factor Authentication (2FA)* when you are not connected to our network (VPN or on site). You must download the **Microsoft Authenticator** app onto your *personal* or *Shared Health managed* smartphone. If you do not have a data plan for your mobile device, please connect to Wi-Fi to complete this QRG.

- **Personal Device:** Your personal cell phone, not provided by Shared Health.
- **Shared Health Managed Device:** This is a smartphone provided to you by Shared Health. For this QRG, this only includes Shared Health managed devices that allow use of email (data plans).

MFA software can be installed on a Shared Health managed device or personal mobile device. It uses very little data on a mobile plan, and can also be configured to not use any mobile data. When MFA is needed, the Microsoft Authenticator app sends a push notification to your phone **OR** a One-Time Passcode (OTP) is available if the user does not approve the push notification. The six (6) digit OTP code allows the user to input it into their laptop when requesting service. When registering for MFA, the user can choose either OTP or the push notification as the first prompt. Refer to ***Using the Microsoft Authenticator App*** QRG for more information.

How do I download and self-register with the Microsoft Authenticator app?

You will need both your computer and your smartphone to enroll for MFA and download the Microsoft Authenticator app. If you do not have a Shared Health managed device, you can still use your personal smartphone. This app will not use a lot of data to run. If you do not have a data plan for your smartphone, please connect to your Wi-Fi to complete the next steps.

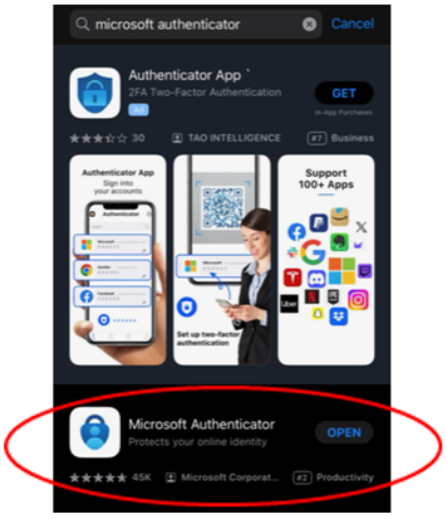
Note: you require an App Store account on your phone in order to download any apps. If you have a corporate issued device please use your work email account to setup the account. Click the link below for your phone:

Iphone - How to create a new Apple ID - Apple Support (CA)
Android - How to add & use accounts in the Google Play Store on your device - Google Play Help

1. If you have a corporate issued smartphone proceed to step 2.

   If you have a personal smartphone a phone passcode, touch ID, face ID or thumbprint is required. If you have not set this up yet please refer to the below links:
   Iphone - Passcode setup: Use a passcode with your iPhone, iPad, or iPod touch - Apple Support
   Iphone - Touch ID setup: Use Touch ID on iPhone and iPad - Apple Support (CA)
   Iphone - Face ID setup: Use Face ID on your iPhone or iPad Pro - Apple Support
   Android - How to set Pattern, Pin or Password for your Lock screen | Samsung SG

2. **On your smartphone**, go to your app or play store and search **Microsoft Authenticator**. Ensure the app you choose says "Microsoft Authenticator" as there are many ads and other similar looking apps in the store. Alternatively, you can scan the below QR codes to find the app if easier.



iPhone

Android

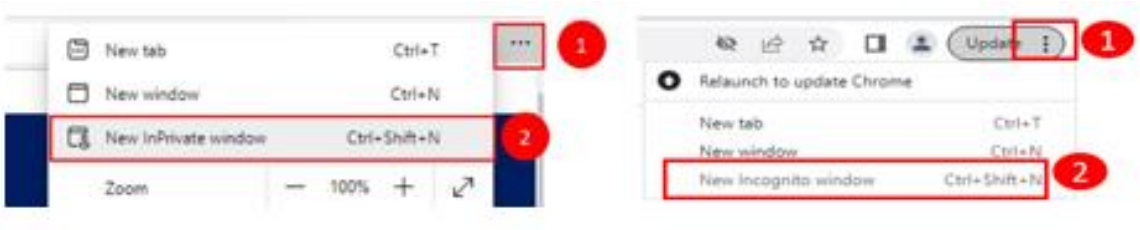
3. **On your smartphone**, tap **Microsoft Authenticator** and then touch **Install**. Continue to step 3 while the app installs on your smartphone.

4. **On your computer**, open **Microsoft Edge, Google Chrome or Apple's Safari.**

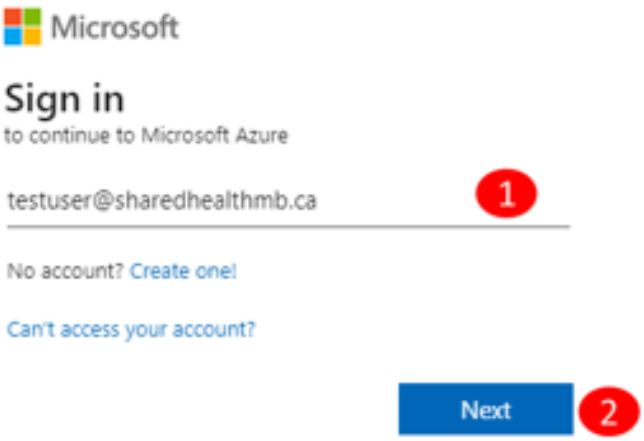
5. **On your computer**, do one of the following:

   a. For users in **NRHA**, **IERHA**, **SH-SS**, and **PMH**, continue to step **6**.

   b. For Shared Health / WRHA users, click the ellipsis at the top right corner of the screen and then choose **New InPrivate Window (Edge) or New Incognito window (Chrome)** from the drop-down menu (Safari not shown below, please see Browse privately in Safari on Mac - Apple Support (CA)).

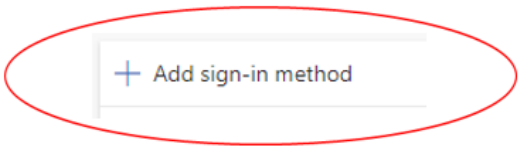


6. **On your computer**, in **Microsoft Edge, Google Chrome or Safari**, go to https://aka.ms/setupsecurityinfo and enter your email address (ex. username@wrha.mb.ca, user@sharedhealthmb.ca, user1@ierha.ca, etc.) then click **Next**.

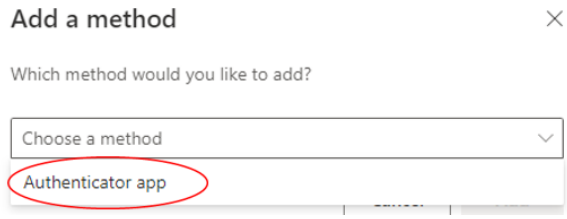


7. **On your computer**, enter your password on the next screen. If Microsoft asks you to stay signed in, choose '**Don't show this again**' and then click **Yes**.

8. **On your computer**, you are directed to the Security info screen. Click **Add sign-in method.**

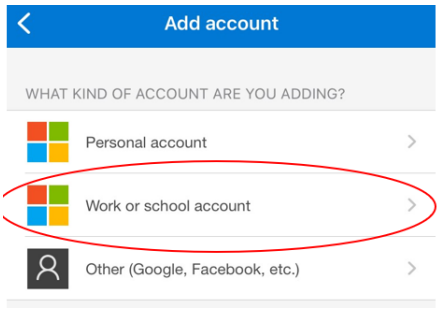


9. **On your computer**, the Add a method screen displays. Select **Authenticator app** from the drop-down menu.

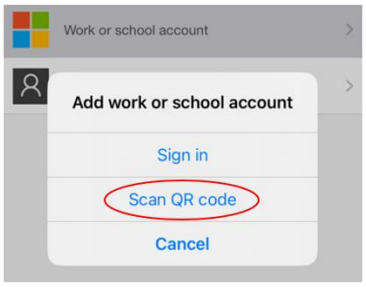


10. **On your computer**, click **Add**.
11. **On your smartphone**, open the Microsoft Authenticator app if it is not already opened.

12. **On your computer**, click **Next**.
13. **On your smartphone**, if the app asks you to accept their policy statement. Touch **I Agree**. You are migrated to the next screen.
14. **On your smartphone**, touch **Work or school account**. (Note: you may need to click the "+" symbol in top right corner of app to get this prompt)



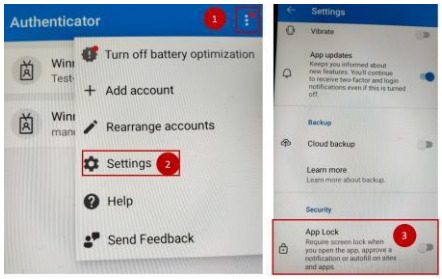
15. **On your computer**, click **Next** and a QR Code will appear.
16. **On your smartphone,** select "Scan QR code"



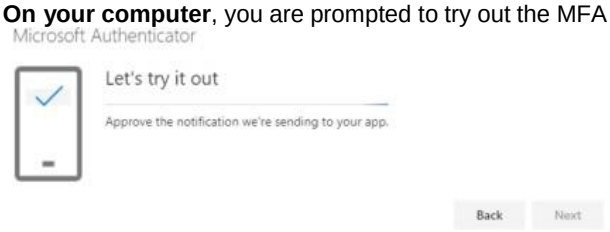
17. **On your smartphone,** scan the code on your computer screen using the Microsoft Authenticator app. Your camera will automatically open up, simply point the camera at the QR code on your computer screen. **Note:** You may switch to the Code / URL Combination.

18. **On your computer**, click **Next**. The **Account added successfully** message appears at the bottom of the screen.

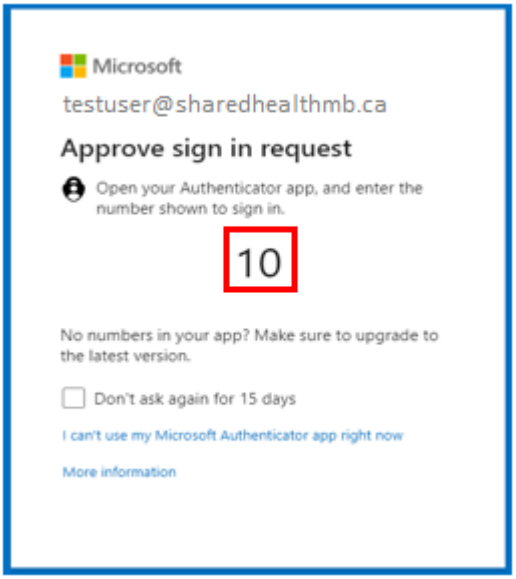
Important: Depending on your smartphone settings, you may receive the message “App Lock enabled. To better protect you, we have enabled App lock by default. To respond to an MFA notification without having to enter your device PIN, go to the Settings inside the **Microsoft Authenticator** app on your smartphone (Menu| Settings), scroll down to the Security section and turn off the ‘App Lock’ setting.



19. **On your computer**, you are prompted to try out the MFA app. Click **Next**.



20. **On your computer**, take note of the number shown on your computer screen.



21. **On your smartphone**, touch **Yes or Approve** within **30 seconds** to approve the sign in request. Your Microsoft Authenticator app will open and you can enter the number shown on your computer screen then click on **Yes.**

22. **On your smartphone**, you may now be prompted to enter your phone’s PIN or thumbprint/touch/face ID. Please follow the prompts to do so. (Note this step will vary depending on how your phone is setup for passcode, thumbprint, touch or face ID)

23. **On your computer**, you are prompted that the sign-in was approved.

24. **On your computer**, click **Next**. You are now registered to use MFA!