





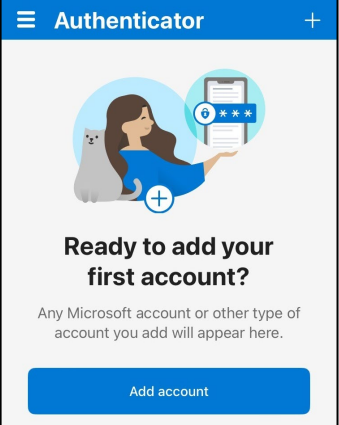
Remote Multi-Factor Authentication Setup using Temporary Access Pass

To remotely access internal Island Health services such as the Intranet, Employee Self-Service, MySchedule, etc., from home or on a personal device, you must first set up **Multi-Factor Authentication (MFA)** on a mobile device. The following instructions will guide you on how to REMOTELY set up MFA using the **Temporary Access Pass (TAP)**.

Before you begin, ensure you have access to a computer with a browser and a mobile device that can access the app store and install the Microsoft Authenticator App.

If you are on-site at an Island Health facility using an Island Health desktop device, you will NOT need to request for a TAP.

Step 1: Preparing your mobile device and App	
1. Close all other applications before you begin.	
2. Is the Microsoft Authenticator app installed on your mobile device?	
No - and you're using a personally owned device, go to the app store and install the Microsoft Authenticator App	
No - and you're using a <i>corporate iOS device</i> , call the Service Desk at 1.877.563.3152 Local 18777 and request IM/IT push the app to the device	
3. Open the Microsoft Authenticator App and accept the following if prompted: <ol style="list-style-type: none"> a. Privacy message b. Update message 	
4. Click on the "Skip" in the top right corner of the screen to continue	

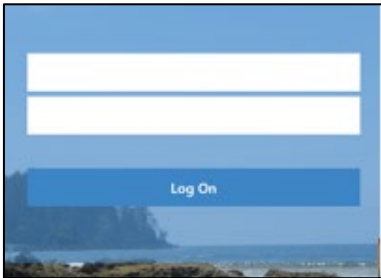
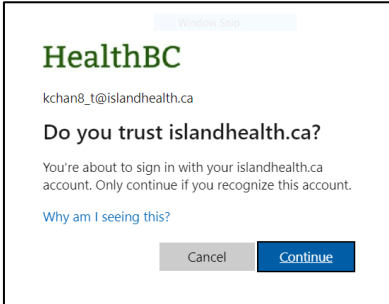
<p>5. You should now see this screen</p> <div style="border: 2px solid red; padding: 5px; text-align: center; margin: 10px 0;"> DO NOT click on Add account! </div> <p><i>If you don't see this screen, close the app then re-open the app until you see this screen before you continue</i></p>	
<p>6. You have now prepared your mobile device and app for MFA setup.</p> <p>STOP HERE and call the Island Health IMIT Service Desk to request a Temporary Access Pass before you continue.</p>	

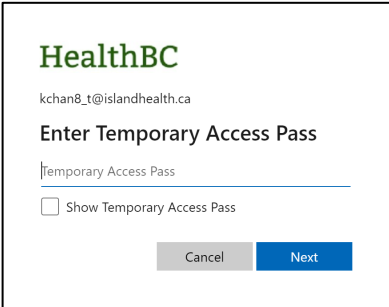
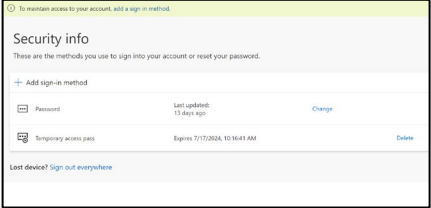
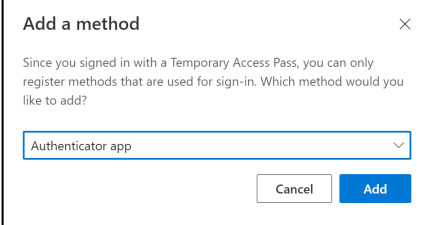
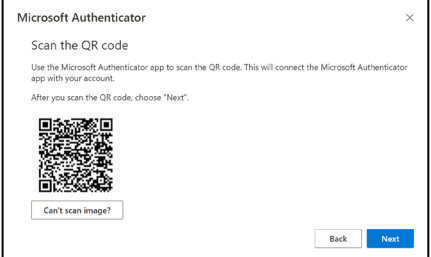
The Island Health IMIT Service Desk will provide a **Temporary Access Password (TAP)** for you to proceed through steps 8-21.

Do not start these steps until you call for a TAP, you will not be able to the complete MFA setup.

NOTE: an issued TAP will **expire** after **60 minutes**. If MFA setup is not completed within the 60-minute timeframe, you will need to call the Service Desk to issue **another TAP** before continuing to step 8-21.

Step 2: Adding a MFA device to your Security Info Profile

<p>7. Call the Island Health IMIT Service Desk at 1.877.563.3152 Local 18777 to request a Temporary Access Pass (TAP).</p>	<p>It is recommended that you write down your TAP value due to its complexity; you will need to enter in this value in Step 12.</p>
<p>8. Once the Service Desk has provided you with a TAP, on a computer, open a web browser (Chrome, Safari, etc.) and go to: https://mfasetup.islandhealth.ca</p>	<p>It is required to use a computer and mobile device for this process; the Service Desk agent may stay on the line with you to ensure successful MFA setup.</p>
<p>9. This will take you to the Island Health Log On prompt</p> <p>Enter in your Island Health username and password given from your manager</p> <p>Note: the process may require you to create a new password at this point</p>	
<p>10. Once you have successfully entered in your username and password, the following window will appear:</p> <p>Click “Continue” to trust Island Health as an Organization</p>	

<p>11. Enter in the TAP provided by the Service Desk, and click on “Next”</p>	
<p>12. You should now be logged into your Security Info Profile:</p> <p>Click on the Add sign-in method button</p>	
<p>13. Select the Authenticator App option from the drop down menu</p> <p>14. Click on Add</p>	
<p>15. The Microsoft Authenticator QR code will appear</p>	

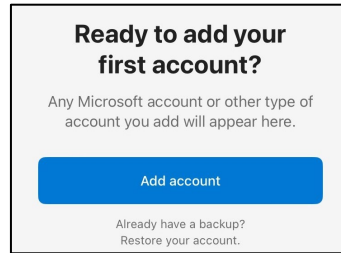
16. Go to your **mobile device** you plan to use as your MFA device (prepared in **Part 1**).

- Click on **“Add account”**
- Click **“Continue”** to bypass the backup prompt
- Select **“Work or School Account”**
- Select **“Scan QR code”** - if prompted to allow access to camera, click **Yes**
- Use your **mobile device**, which should now be displaying your camera, to scan the **QR code image** currently displayed on your **computer browser**.

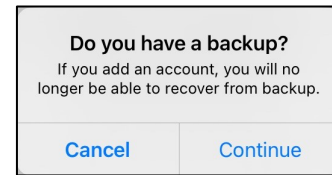
NOTE: the camera will pick up the QR code very quickly even if it is not pointed directly at it.

- Your mobile device should now show your account has been added.

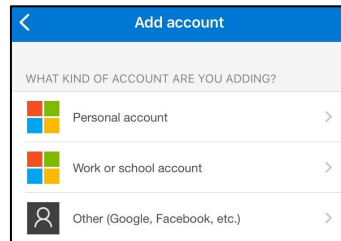
A:



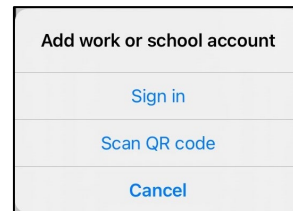
B:



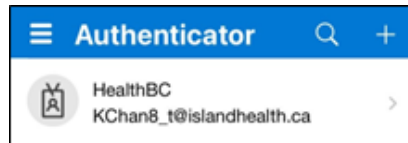
C:



D:

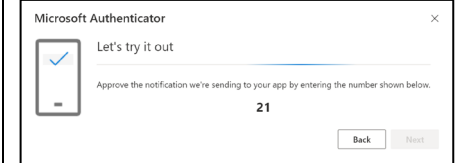
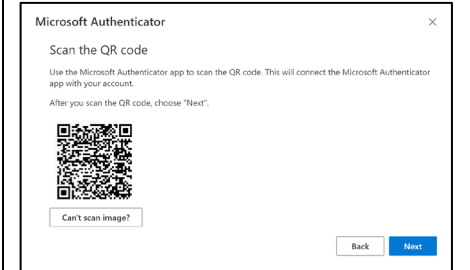


F:



17. Back on your **computer**, click on **“Next”** to activate this **MFA mobile device**.

You should now see a test notification with a two-digit code.



18. On your **mobile device**, a new screen should have opened in the **Authenticator App** where you can enter in the two-digit code shown on the computer screen

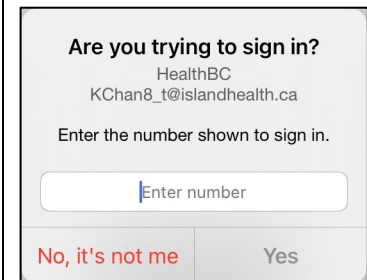
NOTE: If your phone screen lock is triggered, open your phone, and ensure the **Authenticator App** is open to see this window. You may also be required to pull the app down (iPhone) to refresh it to see this window.

19. Click **“Yes”** once you have entered in the two-digit code

Look to your computer screen to see if it was successful

20. On your **computer screen**, you should now see that your Notification was approved:

Click **“Next”**



21. This will return you to your Security Info Profile, where you can add an additional MFA device now by returning to **Step 13**.

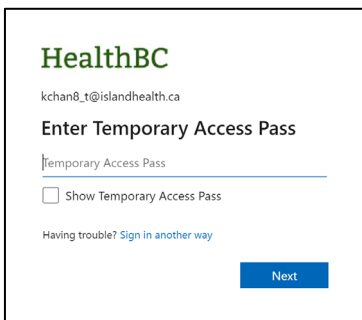
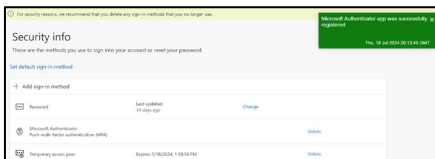
If you are not adding another device you have now finished setting up your MFA devices and are ready to login remotely using your username and password plus:

- Temporary Access Pass until the 60 minutes has expired
- Your MFA device with a two-digit code once the Temporary Access Pass expires.

NOTE: You will be continued to be prompted for Temporary Access Pass at your next login until it's expired, or manually deleted from your Security Info Profile.

At your next login you can also click the "Sign in another way" option to avoid using Temporary Access Pass.

Your MFA setup is now complete!



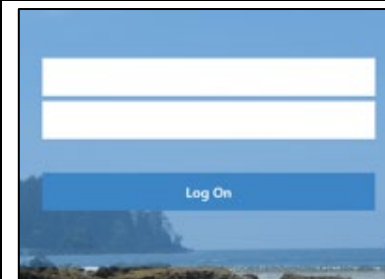
Register for Self-Serve Password Reset (SSPR) (Optional; can be completed later)

You **MUST** successfully set up an MFA device before you can complete Self-Serve Password Reset (SSPR).

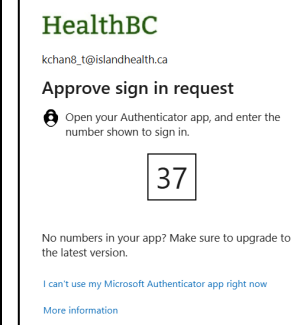
These instructions detail how to add security questions into your Security Info Profile using a desktop and your MFA device

1. On your computer, launch any browser (Chrome, Safari, etc.) and navigate to:
<https://ssprsetup.islandhealth.ca/>

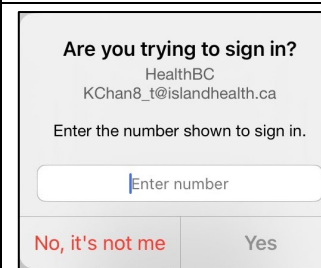
2. This will take you to the **Island Health Log On** prompt. Enter in your Island Health **username and password** and click **Log on**

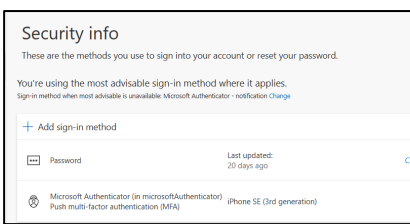
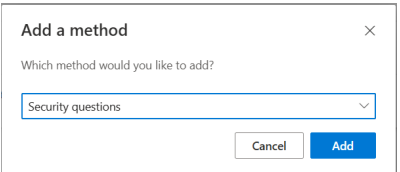
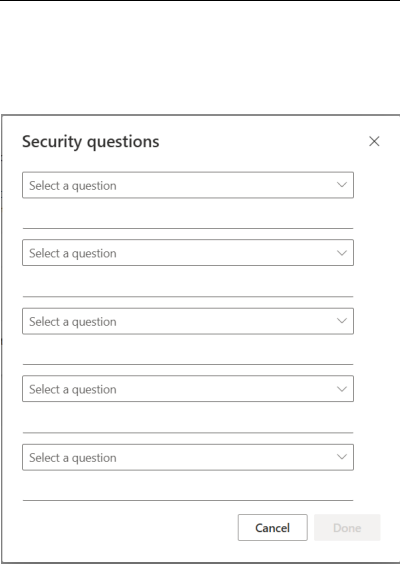
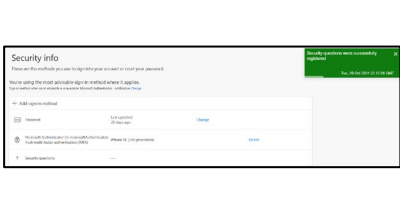


3. Once you have entered in your credentials successfully, you should see an **Approve sign in request** prompt on your computer screen with a **2-digit number**.



4. On your MFA device, open the **Authenticator App** and enter in the **2-digit number** shown on your computer screen and click **Yes**.



<p>5. You should now be logged into your Security Info Profile on your computer:</p> <p>Click on the “Add sign-in method” button to add Security Questions to your Security Info Profile</p>	
<p>6. Select Security Questions.</p> <p>7. Click on Add.</p>	
<p>8. Select one of the 18 questions from the drop-down list, and enter in your answers</p> <p>You will need to repeat this until you have five different questions completed.</p> <p>9. When you have completed all five, click Done</p> <p>Recommendation: try to pick questions that only YOU know the answer to, preferably with a single-word answer for ease of recall.</p> <p>NOTE: answers are not case sensitive; i.e even if you use capital letters in your answer, you will not need to use them when challenged.</p>	
<p>10. You have now completed your SSPR setup!</p> <p>You should now see a successful registration notification on the top right corner of your web browser and be looking at your MFA Security Info Profile</p>	

<h2 style="text-align: center; background-color: #4a86e8; color: white; padding: 5px;">Troubleshooting</h2>	
Issue	Solution
<p>Your sign-in was blocked.</p>	<p>Call the Service Desk and request a TAP to be able to register your mobile device for MFA remotely.</p>
<p>I don't seem to get notifications; or the camera does not appear to scan the QR code.</p>	<p>Go into your phone settings to ensure the Authenticator App has notifications turned on and allows the camera access.</p>
<p>I received one of the following errors:</p> <ul style="list-style-type: none"> Activation error Can't add Account at this time 	<p>Check your Network speed and availability – ensure your mobile MFA device has more than 1 Bar of cellular service. If it doesn't:</p> <ul style="list-style-type: none"> Connect your mobile device to WiFi if available Try later when cellular service has improved