Microsoft Multi-Factor Authentication (MFA)

User Guide Version 4.1

northern health
the northern way of caring

WHAT IS A MULTI-FACTOR AUTHENTICATION (MFA)?

Multi-Factor Authentication is a method of confirming a user's claimed identity by utilizing a combination of two different factors:
1. Something you know (your computer login username and password)
2. Something you have (a one-time passcode configured to be received on your mobile phone)

WHAT IS A MICROSOFT AUTHENTICATOR?

Microsoft Authenticator is an app that provides a second layer of security after your password. When logging in, you'll enter your NH password, and then you'll be asked for an additional way to prove it's really you. Either approve the notification sent to the Microsoft Authenticator, or enter the verification code generated by the app.

You enroll with in Microsoft MFA through the Microsoft Authenticator app and add your work account. This will let Northern Health know that the sign-in request is coming from a trusted device and help you seamlessly and securely access additional Microsoft apps and services without needing to log into each. Because Microsoft Authenticator supports single sign-on, once you have proven your identity once, you will not need to log in again to other Microsoft apps on your device.

BEFORE ENROLLING IN MFA

- You must be at a computer (desktop/laptop) connected to the Northern Health network.
    - *Note: If you cannot access the Northern Health network, contact the service desk at 1-888-558-4357*

ENROLLING IN MICROSOFT MFA

Enrolling in Microsoft MFA can be completed in multiple ways. Please select **one** of the following methods that's applicable to your situation and follow the set by set instructions.
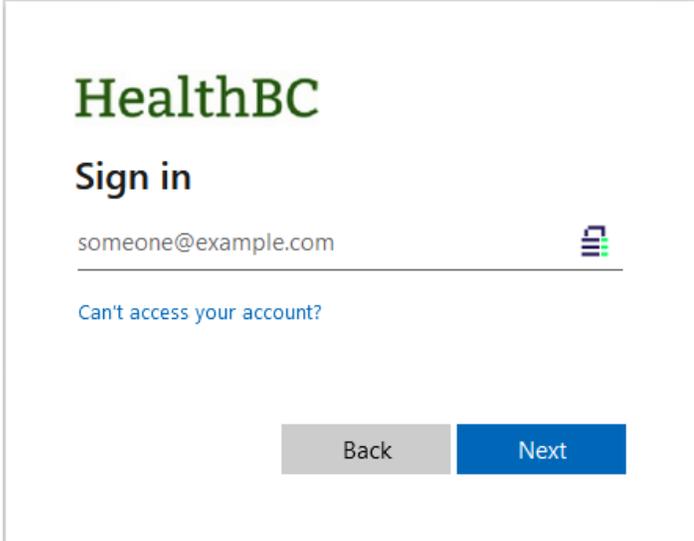
- [You have a computer and mobile device (best option)](#)
- [You only have a mobile device](#)

ENROLLING IN MICROSOFT MFA USING A COMPUTER AND A MOBILE DEVICE

On your computer

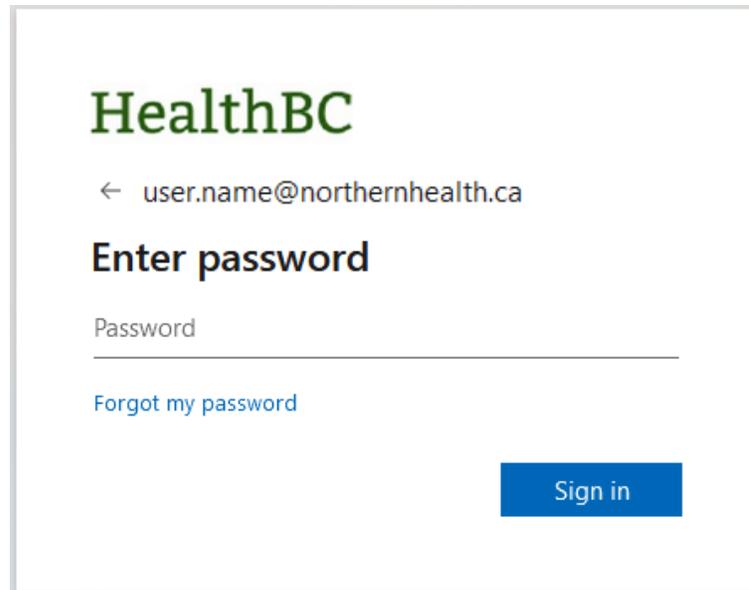*NOTE: For best results consider using Microsoft Edge, Google Chrome or Firefox web browsers.*

1. Please copy and paste this link you're your browser: (**https://account.activedirectory.windowsazure.com/proofup.aspx?whr=healthbc.onmicrosoft.com**) to be greeted with this sign in page:

2. Enter your Northern Health email address (i.e. user.name@northernhealth.ca)

3. Click **Next.**
    a. If prompted, enter your password and click **Sign In**.

4. You'll see this pop-up. Click **Next.**
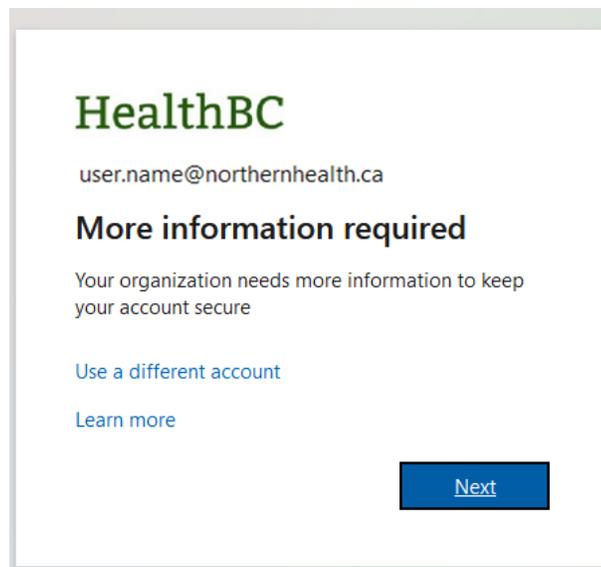
5. Next you may see a screen with the HealthBC Terms of Use, click **Accept.**

6. Now you will be prompted to download the Microsoft Authenticator app on your phone. Once it is downloaded click **Next** on your computer.

NOTE: Go to Google Play (for Android devices) or the App Store (for iOS devices) on your mobile device to download the app.

7. In the app, select the **+** sign at the top to add an account. When prompted select **Work or School** in the app and then click **Next** on your computer.
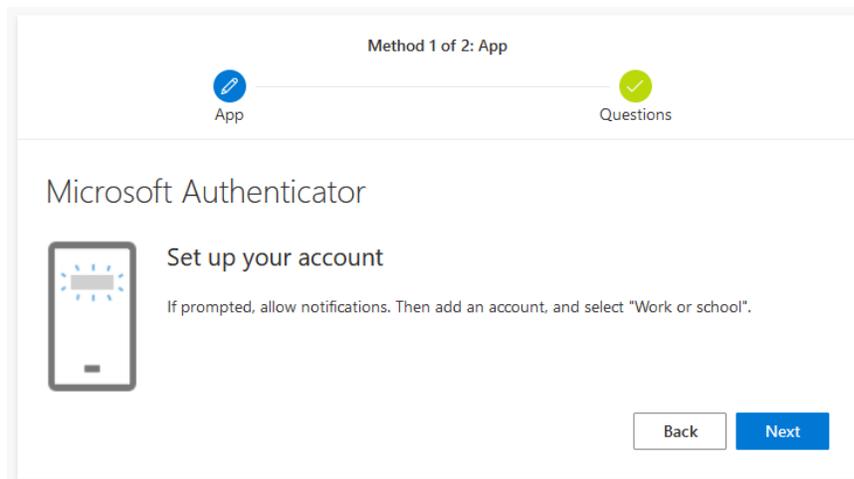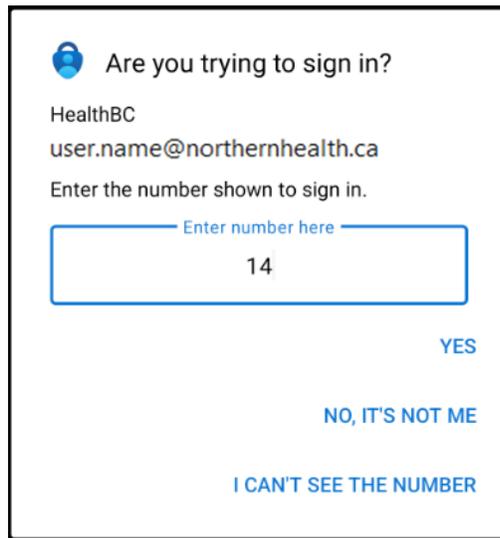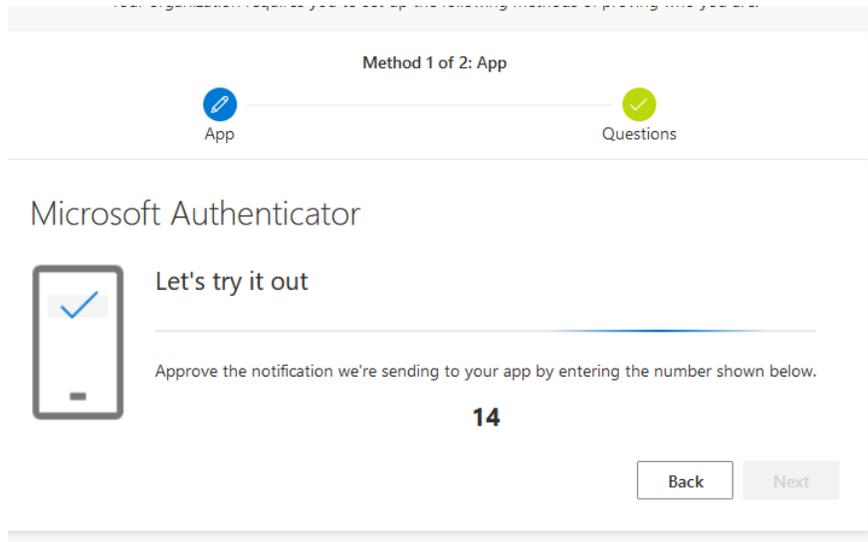

8. **Using your mobile device**, scan the QR code displayed on the computer. **Note:** Upon successful scanning, your account will be added.
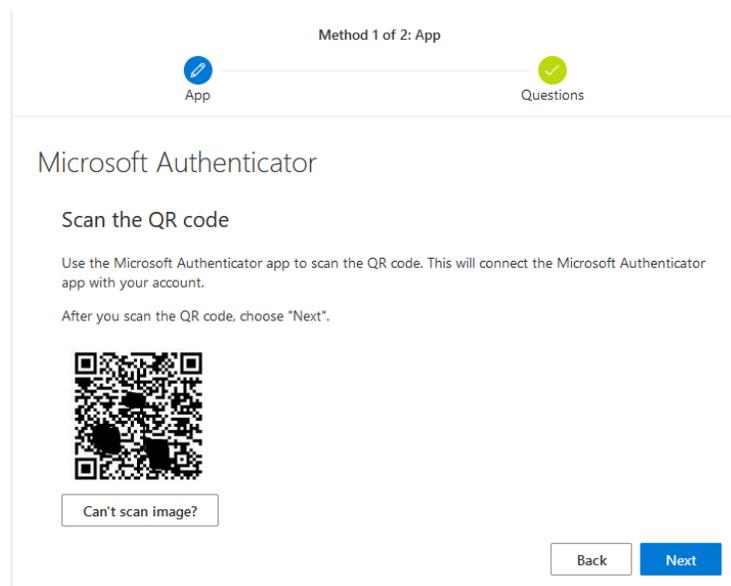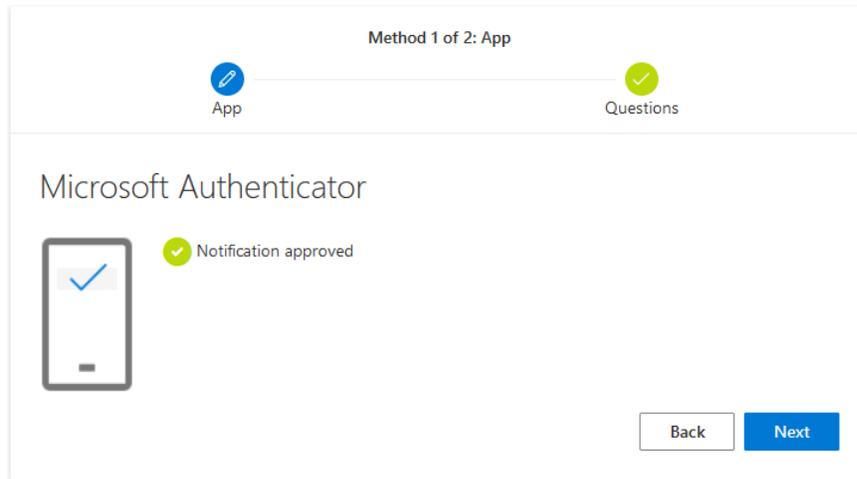

9. Click **Next** on your computer.

10. Respond to the notification on your mobile device by entering the number shown on your computer screen and then selecting **YES.**
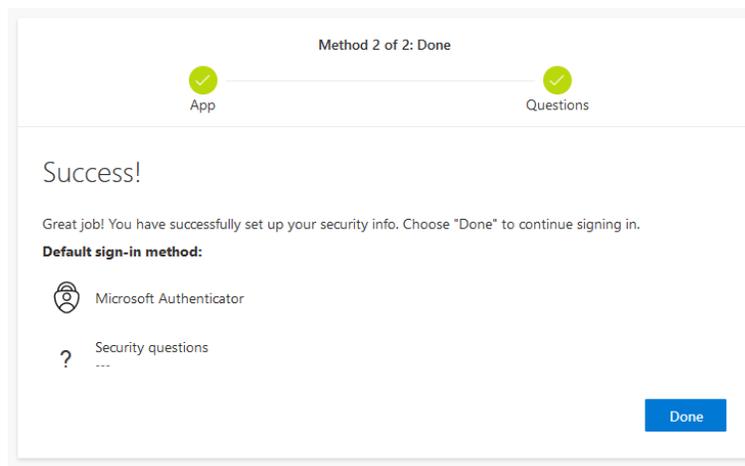
11. Your computer will display Notification Approved. Click **Next.**

12. If you have not yet done so, you will be asked to complete your security questions. Fill in five (5) of the available twenty (20) Security questions and click on the **Done**.

Note: Your Microsoft MFA has been enabled and is now ready to use.

Note: *You can modify your Microsoft account security settings anytime by visiting:*
https://mysignins.microsoft.com/security-info

Upon completing your Microsoft multi-factor authentication registration, take time to visit your My Apps portal located here. You can access and use the My Apps portal on your computer, or from the mobile version of the Edge browser on an iOS or Android mobile device. Learn more here.
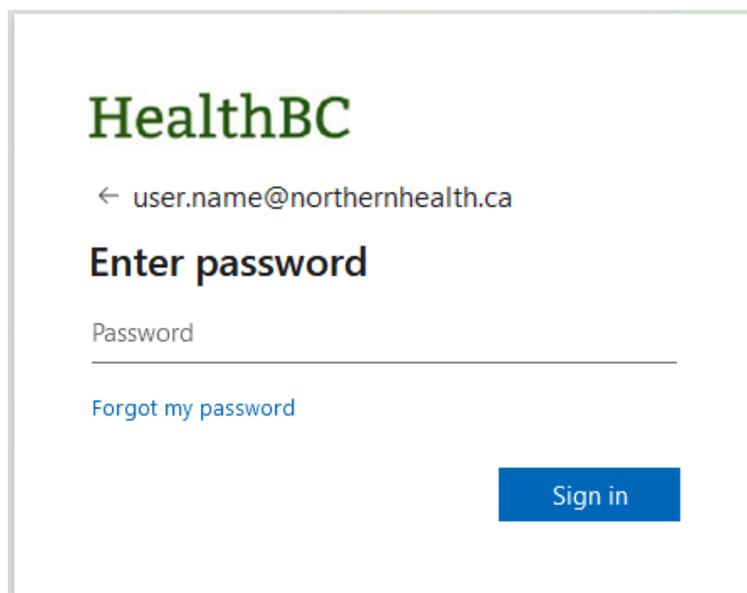
ENROLLING IN MICROSOFT MFA USING ONLY A MOBILE DEVICE

On your mobile device

NOTE: For best results consider using Microsoft Edge, Google Chrome or Firefox mobile web browsers.

1. Please copy and paste this link you're your mobile web browser: (**https://account.activedirectory.windowsazure.com/proofup.aspx?whr=healthbc.onmicrosoft.com**) to be greeted with this sign in:

2. Enter your Northern Health email address (i.e. user.name@northernhealth.ca)

3. Click **Next.**
   a. If prompted, enter your password and click **Sign In.**
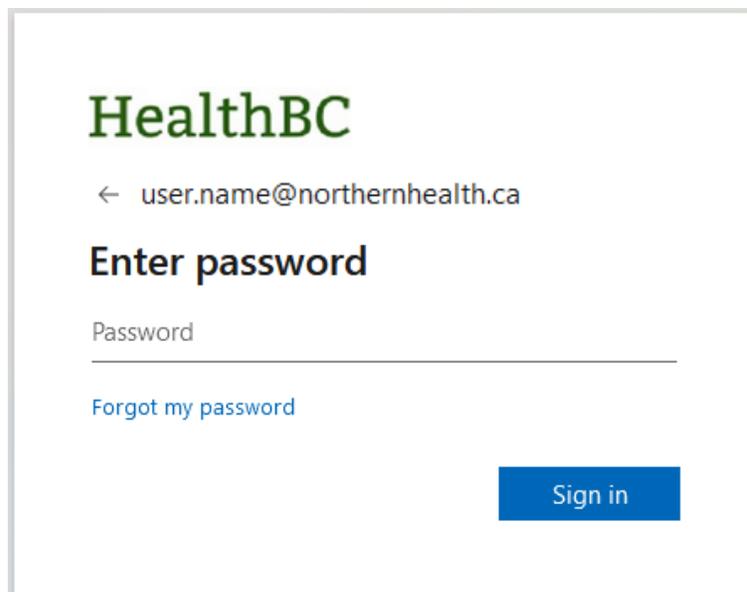
4. Next you may see a screen with the HealthBC Terms of Use, click **Accept.**
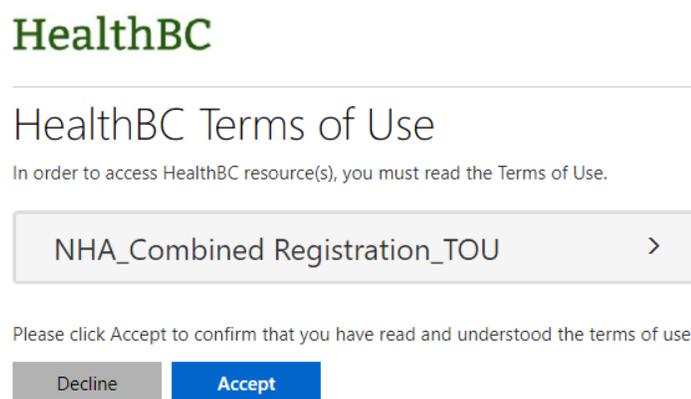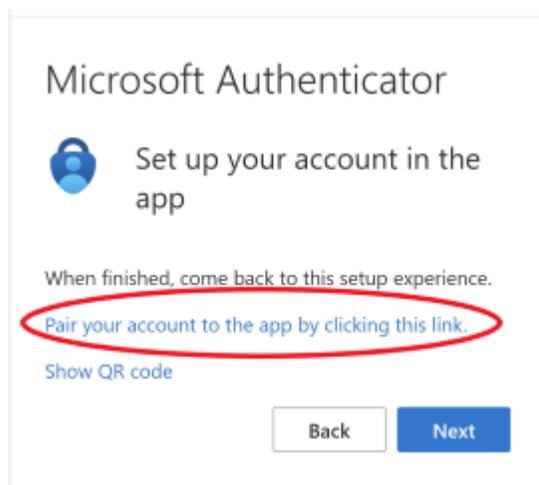
5. Download the Microsoft Authenticator app   to your mobile device.

NOTE: Go to Google Play (for Android devices) or the App Store (for iOS devices) on your mobile device to download the app.

6. After the app is downloaded, return to your mobile web browser and click **Next.**

7. In your mobile web browser select **Pair your account to the app by clicking this link.**
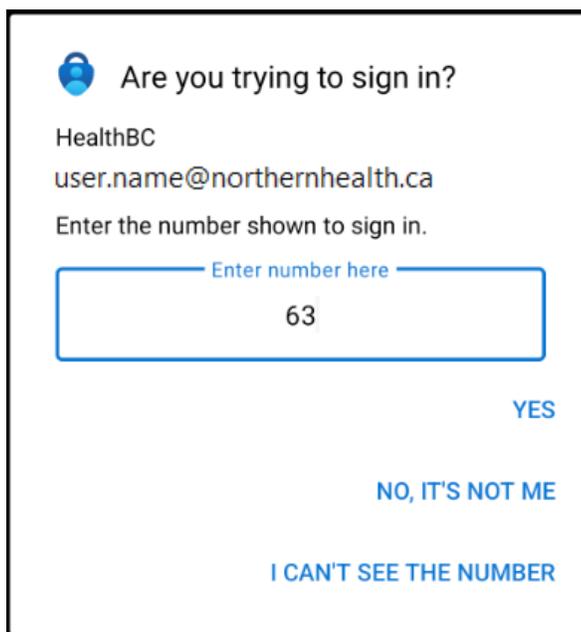
8. This link will open the Microsoft Authenticator app. Click **Finish** to add your Northern Health account.

9. Return to your mobile web browser and click **Next.**
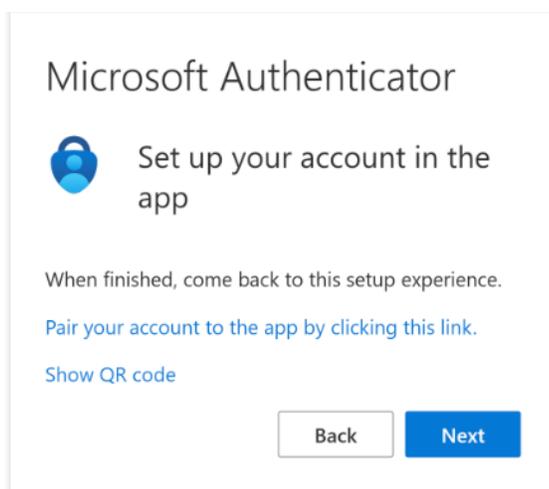
10. You will receive a notification on your phone. Remember the number shown on your screen and select the notification to complete the process by entering the number and selecting **YES.**

11. If you have not yet done so, you will be asked to complete your security questions. Fill in five (5) of the available twenty (20) Security questions and click on the **Done.**

Note: Your Microsoft MFA has been enabled and is now ready to use.

__Note__: You can modify your Microsoft account security settings anytime by visiting: **https://mysignins.microsoft.com/security-info**

Upon completing your Microsoft multi-factor authentication registration, take time to visit your My Apps portal located here. You can access and use the My Apps portal on your computer, or from the mobile version of the Edge browser on an iOS or Android mobile device. Learn more here.

Appendix

Multifactor Authentication

Multifactor Authentication (MFA) is an important security control for preventing unauthorized access to Northern Health (NH) systems and information. At NH, MFA is typically used when you attempt to access NH applications, websites, or systems from outside the NH network. MFA helps to assure your identity, when combined with your NH username and password (credentials).

MFA Fatigue

Cyber criminals are using a social engineering technique called "MFA fatigue" to bypass multifactor authentication. This involves repeated attempts to log in with stolen credentials, flooding the user's mobile device with endless MFA push notifications, hoping to trick the user into inadvertently clicking the "Approve" button to stop the notifications.

Apple Watch and Android wearable device support

After MS introduces MFA Number Matching, Apple Watch and Android wearable devices (such as Samsung Galaxy Watch) will no longer work with the Authenticator app's security features. With the release of Authenticator 6.7.3 for iOS, the companion app was removed from the Apple Watch.

Reporting Security Incidents

NH staff are to report security incidents to the NH Service Desk. This will notify the NH Information Security team for further investigation and response.

servicedesk@northernhealth.ca or 1-888-558-4357