

# Using NHEverywhere (VDI) with the Microsoft My Apps portal



User Guide Version 1.2



**northern health**  
*the northern way of caring*

---

## WHAT IS NHEVERYWHERE?

NHEverywhere is a virtual desktop solution that allows physicians, clinicians and staff to reliable and secure access to the Northern Health applications you need to care for patients (eg.Cerner, CMOIS, PACS) or business (eg. Access for Call Centre Staff)

**Note:** *When accessing NHEverywhere from outside a Northern Health facility you must always access it via the Microsoft My Apps portal at:*

*<https://myapplications.microsoft.com/>*

---

## WHAT IS THE MICROSOFT MY APPS PORTAL?

The Microsoft My Apps portal is a website used to group and launch your applications. It's also used to launch and load NHEverywhere.

You can get to the My Apps portal from any of the following web browsers:

- Microsoft Edge
  - Google Chrome
  - Mozilla Firefox, version 26.0 or later
- 

## 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)

Multi-Factor Authentication (MFA) helps keep data secure by validating your access when working from home, at work and on the go.

---

## WHAT IS A MICROSOFT AUTHENTICATOR?

Microsoft Authenticator is an app that provides a second layer of security (like the RSA SecurID app) 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.

# LAUNCHING NHEVERYWHERE VIA THE MICROSOFT MY APPS PORTAL.

## On your computer (Windows or Mac)

1. Open your web browser of choice (e.g., Microsoft Edge, Google Chrome, Mozilla Firefox, version 26.0 or later) and load the following web site:  
<https://myapplications.microsoft.com/>
2. Enter your **Northern Health** email address (i.e. user.name@northernhealth.ca).

HealthBC

Sign in

someone@northernhealth.ca

[Can't access your account?](#)

[Sign-in options](#)

Next

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

Sign In

https://sts.healthbc.org/adfs/ls/?client-request-id=f3ca4cbe-bfb3-482a-ae98-f3773a9ca760&wa=wsl...

Network Account Login

Sign in with your organizational account:

first.last@northernhealth.ca

Password

Sign in

© 2013 Microsoft

4. You'll see this pop-up, click **Next**.

HealthBC

username@northernhealth.ca

### More information required

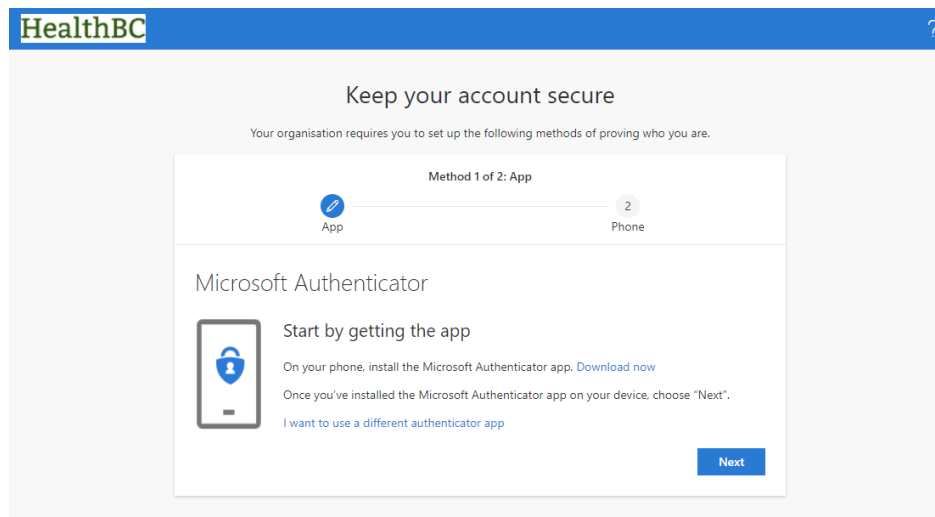
Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

*NOTE: If you don't see the prompt above, but you receive a mobile notification from the Microsoft Authenticator app on your mobile device select "Approve" and jump to step 20 by [clicking here](#).*



## On your mobile device

5. Download the Microsoft Authenticator app  to your mobile device.

***NOTE:** Go to Google Play (for Android devices) or the Apple App Store (for iOS devices) on your mobile device to download the app. On NH corporately managed mobile phones, this step can be completed using the Catalog app (Apple ID not required in corporate store).*



## On your computer

- Next you'll see a screen with the HealthBC Terms of Use, click **Accept**.

### HealthBC

#### HealthBC Terms of Use

In order to access HealthBC resource(s), you must read the Terms of Use.

NHA\_Combined Registration\_TOU



Please click Accept to confirm that you have read and understood the terms of use.

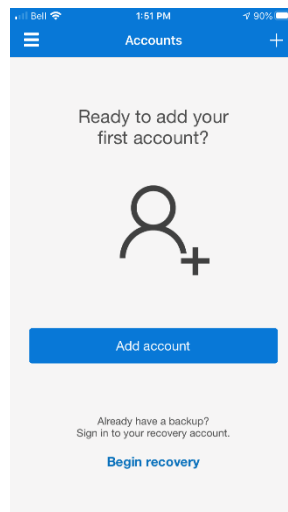
Decline

Accept

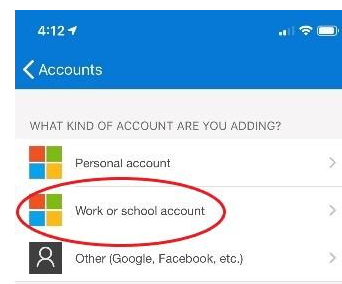
**NOTE:** If you did not download the app in step #1, please do so now.

## On your mobile device

- Open the Microsoft Authenticator app on your mobile device.
- If prompted, tap **Allow** to receive notifications.
- Tap **Add Account**

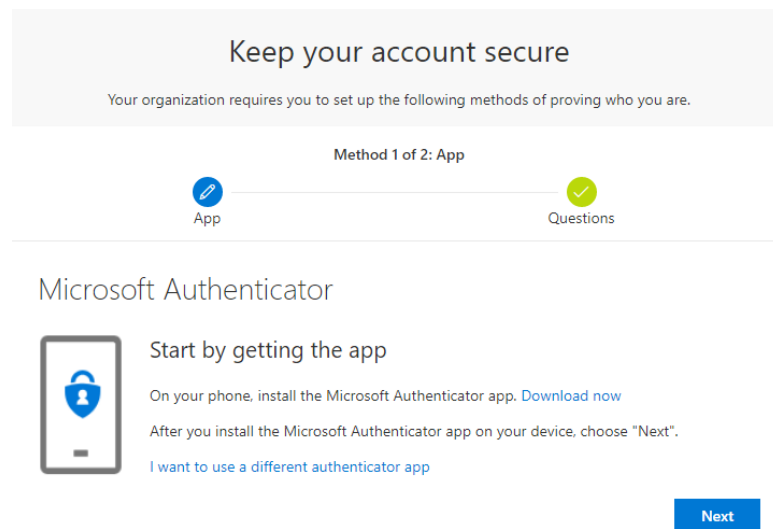


- Tap **Work or school account**
- If prompted, tap **OK** to allow access to camera.  
**You will require camera access to scan the QR code.**



## On your computer

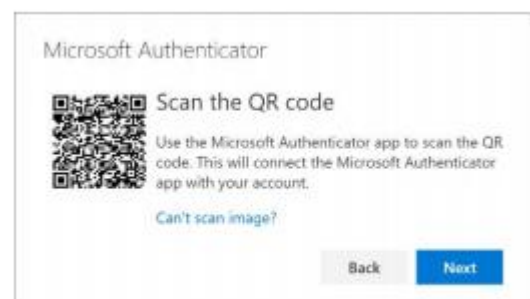
12. Go back to your computer and on the Setup Account page, click **Next**.



13. Using your mobile device, scan the QR code displayed on the computer

**Note:** Upon successful scanning, your account will be added.

14. Click **Next**.

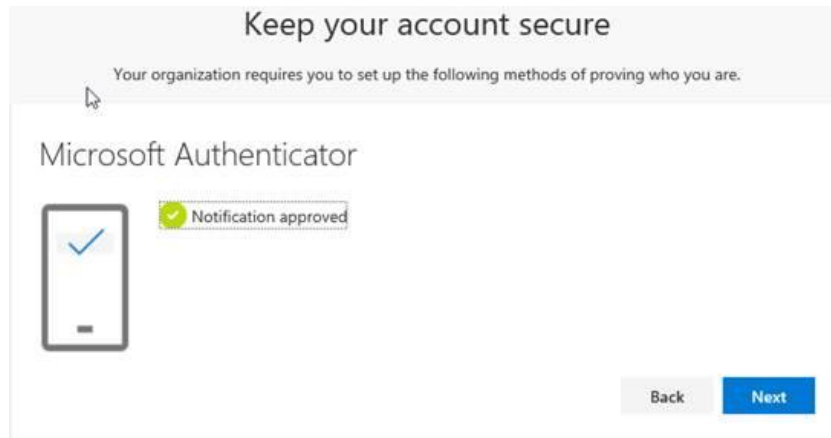


*Do not scan the code above, it is an example only.*

15. Respond to the notification on your mobile device by selecting **Approve**.

**Note:** If you do not see a notification, open the Microsoft Authenticator app and “pull down” (slide your finger down and release) on the screen to refresh and check for notifications

16. Your computer will display Notification Approved. Click **Next**.



17. Now you'll be asked to register a second secure method.

You can choose “Phone” or “Security questions”. If you continue with the Phone method, you'll need to enter your phone number to receive an SMS text code or select the “Call me” method and respond to the touch tone phone call.

A screenshot of a web interface titled "Keep your account secure". Below the title, it says "Your organization requires you to set up the following methods of proving who you are." The main content area is labeled "Method 2 of 2: Phone". It shows two options: "App" (with a green checkmark) and "Phone" (with a blue pencil icon). Below this, the "Phone" section is active, showing the text "You can prove who you are by answering a call on your phone or texting a code to your phone. What phone number would you like to use?". There is a dropdown menu for "United States (+1)". Below the dropdown, there are two radio buttons: "Text me a code" (selected) and "Call me". At the bottom, it says "Message and data rates may apply." and there is a "Next" button.

Phone

You can prove who you are by answering a call on your phone.  
What phone number would you like to use?

United States (+1)

☒ Text me a code  
☐ Call me

Message and data rates may apply.

[I want to set up a different method](#)

To continue with the Security questions, you'll want to click on the "I want to set up a different method" at the bottom left of your screen and select Security questions from the drop down list. Click **Confirm**.

HealthBC

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

App Phone

Choose a different method

Which method would you like to use?

Security questions

Cancel Confirm

Next

18. Fill in five (5) of the available twenty (20) Security questions and click on the **Done**.

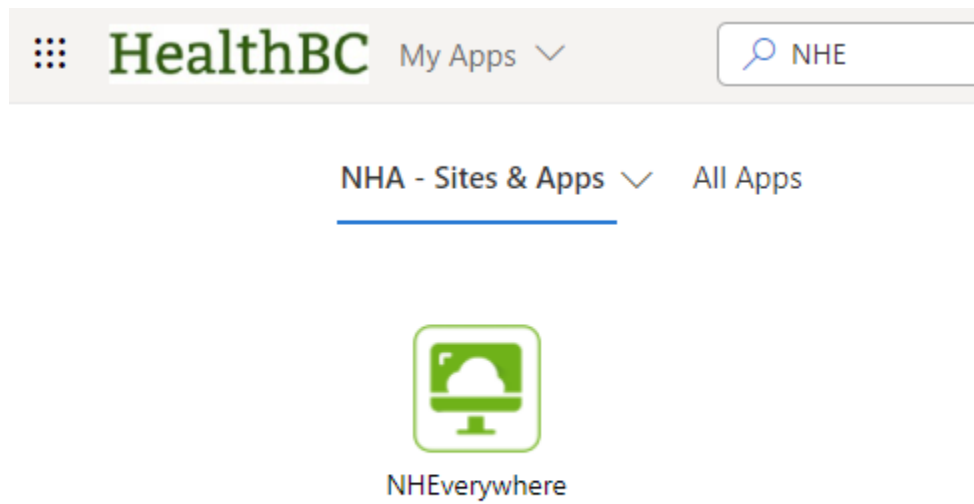


The screenshot shows the 'Security questions' setup page in the HealthBC portal. At the top is a blue header with a hamburger menu icon and the text 'HealthBC'. Below the header, the title 'Security questions' is displayed. There are five identical rows, each containing a dropdown menu with the text 'Select a question' and a downward arrow. At the bottom right of the form area is a grey button labeled 'Done'.

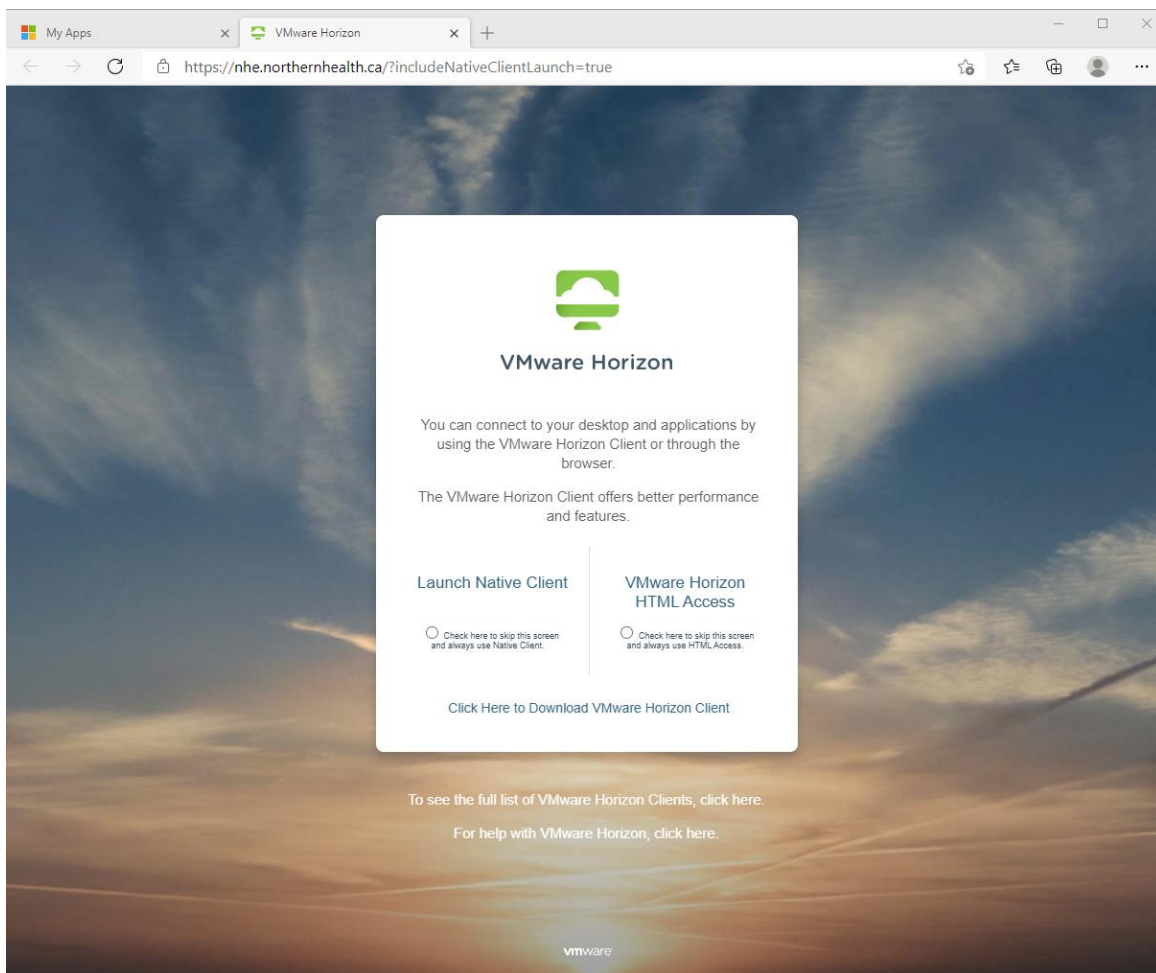
19. Your Microsoft MFA has been enabled and is now ready to use. Click **Done** and be re-direct to the Microsoft My Apps portal website.

The screenshot shows the 'Keep your account secure' success screen in the HealthBC portal. At the top is a blue header with a hamburger menu icon, the text 'HealthBC', and a question mark icon. Below the header, the title 'Keep your account secure' is displayed, followed by the text 'Your organization requires you to set up the following methods of proving who you are.' Below this is a progress bar labeled 'Method 2 of 2: Done'. The progress bar has two steps: 'App' and 'Questions', both marked with green checkmarks. Below the progress bar, the word 'Success!' is displayed, followed by the text 'Great job! You have successfully set up your security info. Choose "Done" to continue signing in.' Below this is the text 'Default sign-in method: Microsoft Authenticator - notification'. There are two items listed: 'Microsoft Authenticator' with a lock icon and 'Security questions' with a question mark icon. At the bottom right is a blue button labeled 'Done'.

20. Click on the **NHEverywhere** tile to launch it.

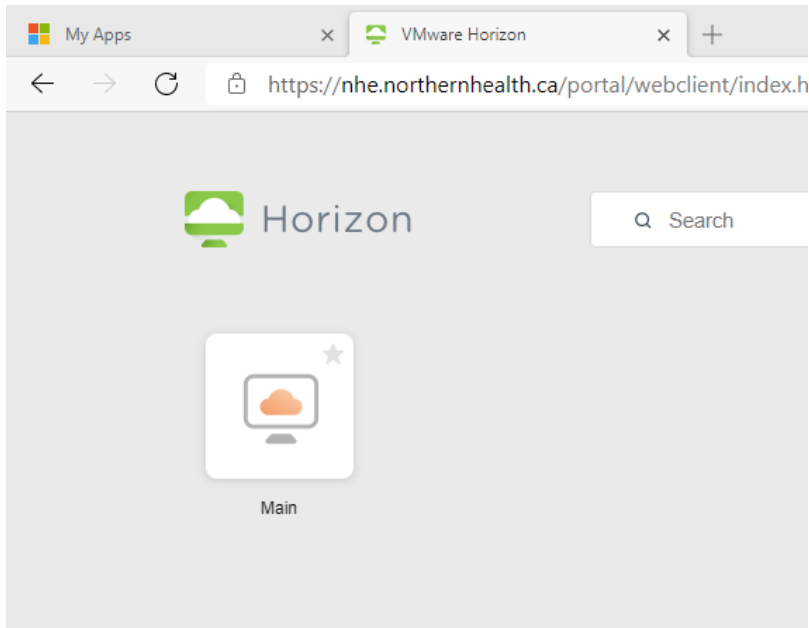


21. This will open a new web browser tab that looks like this:



22. Select one of the two options : **Launch Native Client** or **VMware Horizon HTML Access**

23. Selecting the **VMware Horizon HTML Access** will load a web page that looks like this:



24. Click on **Main** to launch your VMware Horizon Virtual desktop!

25. When prompted enter your Northern Health username and password in the following log on box.

A screenshot of a Windows login dialog box titled 'Login to Windows'. It features the 'northern health' logo and the tagline 'the northern way of caring' along with the 'imprivatix powered by' logo. The form includes fields for 'User Name:', 'Password:', and a 'Log on to:' dropdown menu currently set to 'NHRHB'. There are 'OK' and 'Cancel' buttons. At the bottom, there is a section 'Choose how to authenticate with OneSign' with radio buttons for 'Password' (selected), 'Fingerprint', 'ID Token', and 'Proximity Card'. At the very bottom, there are links for 'Shut down' and 'Restart'.

**Note:** When accessing NHEverywhere from outside a Northern Health facility you must always access it via the Microsoft My Apps portal at: <https://myapplications.microsoft.com/>

---

# FREQUENTLY ASKED QUESTIONS (FAQ)

## Tips to try before calling Service Desk!

- Have your mobile device in hand with Microsoft Authenticator app open before logging on.
  - Clear Internet cache by pressing Ctrl+F5.
  - Try a different Internet browser (Microsoft Edge, Google Chrome or Firefox).
  - Start an in-private or incognito session.
  - If having issues with token registration, do not uninstall the Microsoft Authenticator app. Instead, remove your account on the app and start over.
- 
1. Need help getting your Microsoft MFA profile set up? Call the ITS Service Desk at 250-565-2784 or 1-888-558-4357.
  2. Can I self-register a new phone?
    - a. Yes! You can modify your Microsoft account security settings anytime by visiting: <https://mysignins.microsoft.com/>
  3. What if I don't receive the App notification from MFA or it's delayed?
    - a. Sometimes it takes longer to receive the MFA code. You can re-request the code again if the system times-out at the first attempt
  4. What if I don't have a company phone?
    - a. If you want to use the mobile app you can use any personal device that runs iOS or Android, either a cell phone or a tablet
  5. I'm using the mobile app and there's no cell or data connection
    - a. The mobile app supports the offline mode. There is a one-time passcode generated every 30 seconds in the MS Authenticator App, that can be used to login to the MFA portal
  6. What if I forgot my cell phone or the battery is dead?
    - a. If you have access to your alternate authentication method, you can login to MFA portal and change your default method
  7. My cell phone is forgotten/dead and I can't remember my alternate authentication method?
    - a. Call the ITS Service Desk 24/7 at 250-565-2784 or 1-888-558-4357