Shared health
Soins communs
Manitoba

Using Microsoft Multi-Factor Authentication (MFA)
Quick Reference Guide

Using the Microsoft Authenticator App

Now that you have downloaded the Microsoft Authenticator (MFA) app, you can review this QRG to learn:

- How do I sign into my MFA account?
- How will I receive notifications?
- How do I access an application using MFA?
- How do I change the default verification method?
- How do I delete my security settings?
- How do I sign out of my MFA account everywhere?

How do I sign into my MFA account?

Signing into your account will be experienced differently when outside of the Shared Health network (e.g., at home, coffee shop, working from a hotel or airport):

- **Step 1 – Enter your normal computer login credentials**

  Sign into your Shared Health or Regional account like you usually would (using your username and password)

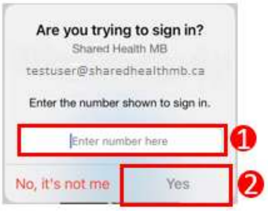
- **Step 2 – Respond to prompt for a second verification**

  Approve the notification from the Microsoft Authenticator app on your smartphone. This will complete the sign-in process

How do I Receive Notifications?

Microsoft Authenticator app has two types of validation methods; a push notification and One-Time Passcode (OTP).

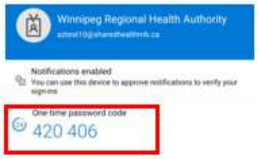
- The push notification requires the user to have either a data plan on their smartphone or a Wi-Fi connection to receive the push notification. The user will receive a prompt on their computer or tablet to Approve sign in request that will list a number to enter in their Microsoft Authenticator app. On their smartphone the user must press Yes to approve the request then open their Microsoft Authenticator app and enter the number.



Are you trying to sign in?
Shared Health MB
testuser@sharedhealthmb.ca
Enter the number shown to sign in.

Example of what you will see if you choose the ***push notification***.

- **OTP does not need a data plan or Wi-Fi connection**. The user will need to open the app and then enter the six (6) digit passcode into the requesting service on their laptop. You will receive notifications from the Microsoft Authenticator app on your smartphone OR be given a one-time user verification code from your smartphone that you must enter in your web browser.



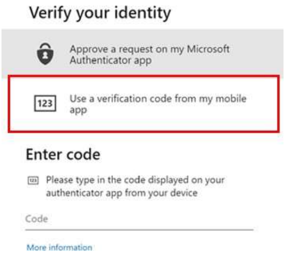
Winnipeg Regional Health Authority

Notifications enabled
You can use this device to approve notifications to verify your sign-ins

One-time password code
420 406

Example of what you will see if you choose the ***One-Time Password***.

- **Important:** When prompted to approve a sign in request, you may want to change your notification to an OTP instead of the push notification. In your MFA app, touch 'Use a verification code from my mobile app'. You are then requested to enter the six-digit code.



Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

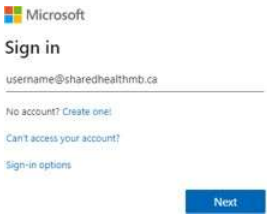
Enter code

Please type in the code displayed on your authenticator app from your device

Should you receive a notification request to Approve sign-in on your device when you have not requested one, press Deny. Report any suspicious activity or verification requests to servicedesk@sharedhealthmb.ca for investigation.

How do I access an application using MFA?

1. When you launch the application you will be directed to a Microsoft page. Enter your email address and click Next.



Microsoft

Sign in

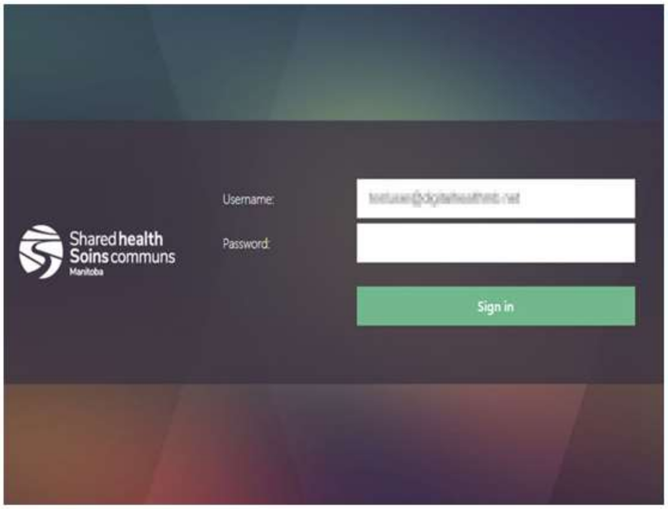
username@sharedhealthmb.ca

No account? Create one!

Can't access your account?

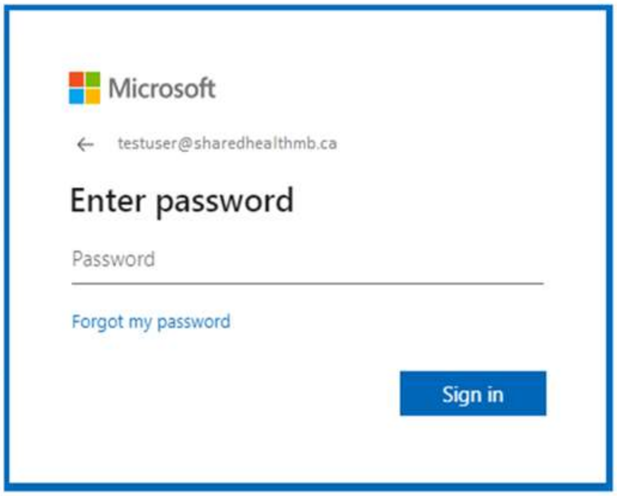
Sign-in options

2. For WRHA, NRHA and Shared Health users the window will look like the picture below on the left. For all other users it will appear like the picture below on the right.



Username: testuser@digitalhealthmb.net

Password:



Microsoft

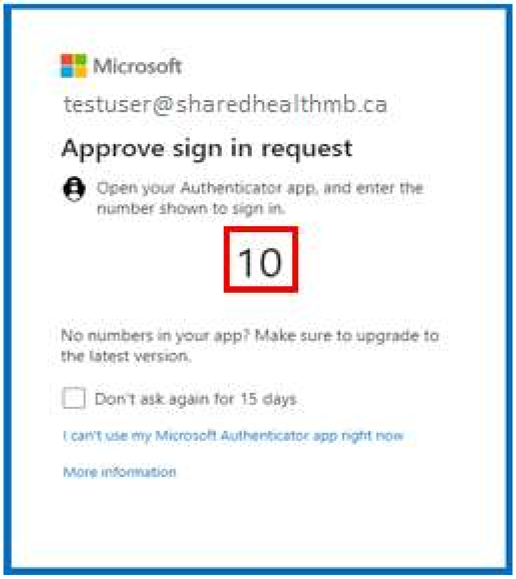
← testuser@sharedhealthmb.ca

Enter password

Password

Forgot my password

3. Enter your usual computer/email password and click Sign In. If you are using push notifications take note of the number provided to enter into your Authenticator application. If you need to use a one-time password click on the "I can't use my Microsoft Authenticator app right now" link.



Microsoft

testuser@sharedhealthmb.ca

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

10

No numbers in your app? Make sure to upgrade to the latest version.

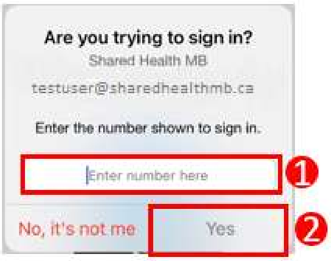
□ Don't ask again for 15 days

I can't use my Microsoft Authenticator app right now

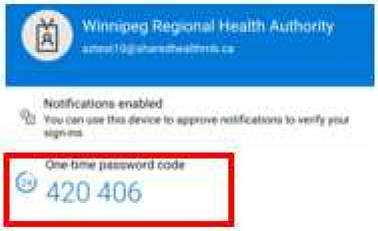
More information

4. MFA will prompt you either on your smartphone or as a one-time password code (when your smartphone is not available).

Authenticator app request **Authenticator app one-time password code**



Are you trying to sign in?
Shared Health MB
testuser@sharedhealthmb.ca
Enter the number shown to sign in.



Winnipeg Regional Health Authority
aztest10@sharedhealthmb.ca

Notifications enabled
You can use this device to approve notifications to verify your sign-ins

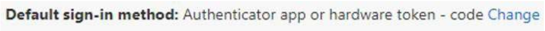
One time password code
420 406

5. Once you verify your identity via the selected choice, you will be granted access to the application you need to use.

How do I change the default verification method?

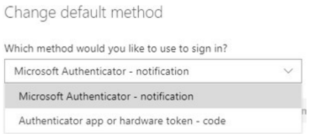
Once you have set up Microsoft Authenticator, you may change your preferred authentication method for your account. Upon signing into an application with your username and password, you will be presented with a security verification alert on your smartphone. This appears as a notification or verification code through the authenticator app.

1. From your web browser, go to https://aka.ms/setupsecurityinfo. Your default sign-in method displays.



Default sign-in method: Authenticator app or hardware token - code Change

2. Click **Change**.
3. Choose the new default from the drop-down menu.



Change default method

Which method would you like to use to sign in?

Microsoft Authenticator - notification
Microsoft Authenticator - notification
Authenticator app or hardware token - code

4. Your new default MFA method applies.

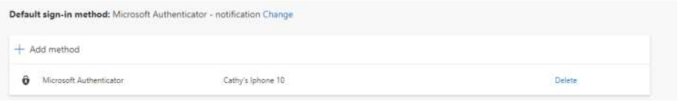
Two options for authentication using the Microsoft Authentication Application:

- Receive notifications for verification – This option sends a notification to the authenticator app on your smartphone or tablet. You must then review the notification and, if it is legitimate, select Approve in the app. You may have to enter your PIN to authenticate
- Use verification code (OTP) – In this mode, the app generates a verification code that updates every 30 seconds. You must enter the most current verification code in the sign-in screen.

How do I delete my security settings?

You may delete any of your configured MFA methods from the Security info page. **If the Microsoft Authenticator method is deleted, you will have to complete the entire registration process on both your smartphone and computer once again**.

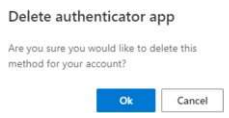
1. In your web browser, go to https://aka.ms/setupsecurityinfo.
2. Click the Delete link next to the MFA method you wish to delete.



Default sign-in method: Microsoft Authenticator - notification Change

Microsoft Authenticator   Cathy's Iphone 10

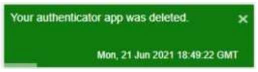
3. The confirmation prompt appears. Click OK.



Delete authenticator app

Are you sure you would like to delete this method for your account?

4. Once confirmed, a notification appears in the upper right corner of the page.



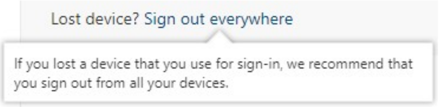
Your authenticator app was deleted.

Mon, 21 Jun 2021 18:49:22 GMT

How do I sign out everywhere?

You must sign out your devices via the Security Info page when your MFA enabled smartphone is lost or stolen. This will sign you out of all endpoints (but will not delete any set up MFA methods). You will have to complete the self-registration for the Microsoft Authenticator app again.

1. From your browser, go to https://aka.ms/setupsecurityinfo



Lost device? Sign out everywhere

If you lost a device that you use for sign-in, we recommend that you sign out from all your devices.

2. Click Sign out everywhere.