

BCProvider Active Directory Multifactor Authentication (MFA) Setup

If you are reading this document, it is assumed you have successfully logged into OneHealthID services and created a BCProvider. If you have not yet created a BCProvider, please do so first. <https://healthprovideridentityportal.gov.bc.ca/>

After you have created your BCProvider, you have to link it to your phone using Multi-factor authentication.

If you have questions during or after the tutorial, please contact us at amsspoc.vic@cgi.com

The BCprovider uses Multi-Factor Authentication (MFA) is an additional layer of security that helps protect your online accounts and sensitive information. It enhances the traditional username and password login process by requiring at least two or more forms of verification. This guide aims to explain the significance of MFA and provide instructions on how to set it up for the first time.

- MFA significantly reduces the risk of unauthorized access to your accounts by adding an extra layer of verification.
- Even if someone manages to obtain your password, they won't be able to access your account without the second factor of authentication

The first time you login to Bchealthprovider.ca you may be asked to setup MFA. If you are requested, please follow the steps below

Setting up the Microsoft Authenticator

1. Goto bchealthprovider.ca
2. Enter your bcprovider.ca login information



Sign in

Email, phone, or Skype

No account? [Create one!](#)

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

Back

Next

3. Enter your password



← nicholas.mailhot@bcprovider.ca

Enter password

Password

[Forgot my password](#)

Sign in

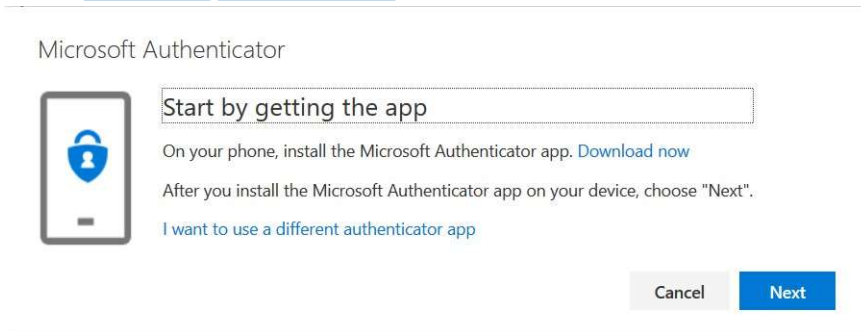
Help and Support

Contact Support Desk Monday to Friday

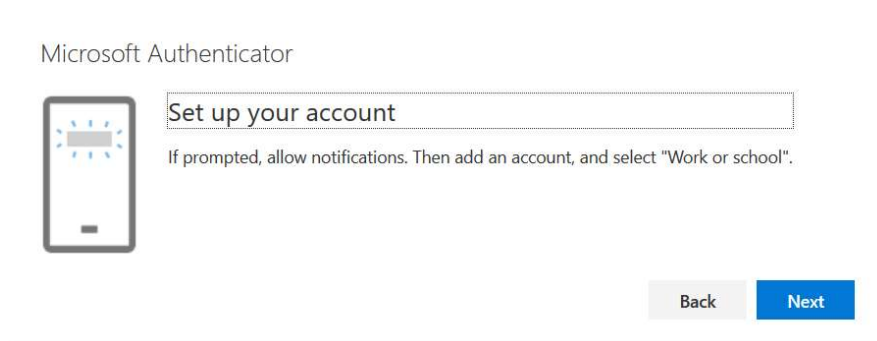
Standard Business hours 8:00 AM-5:00PM PST

Email Address: amsspoc.vic@cgi.com

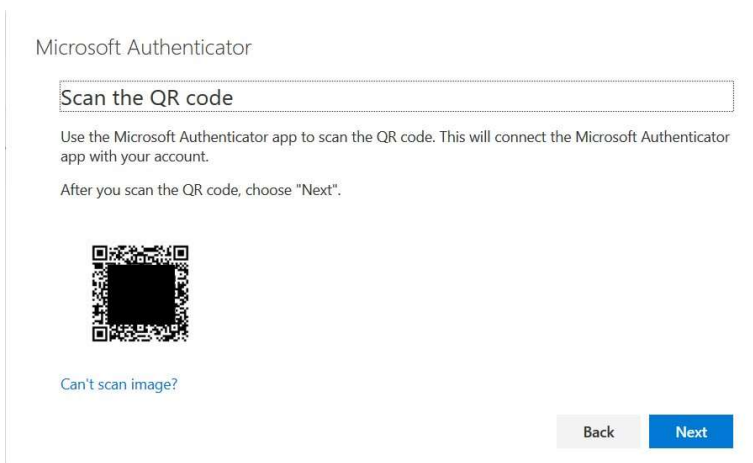
4. You will be prompted for more information on the first login.
5. On your iOS/Android mobile device, you will need to go to the respective app store and install the [Microsoft Authenticator](#).



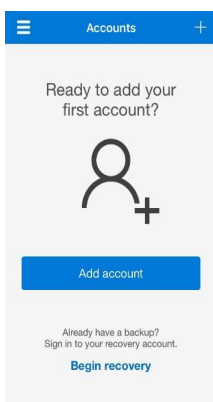
6. Once you have the app installed, click **Next**.



7. Click **Next**

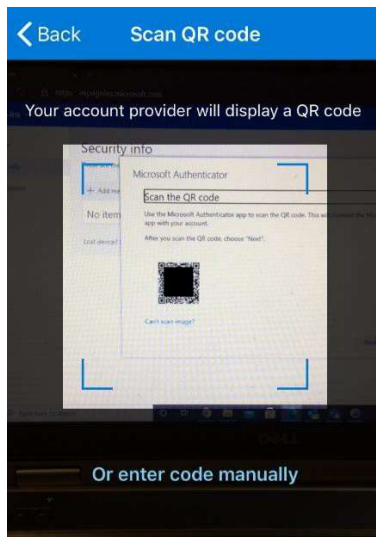
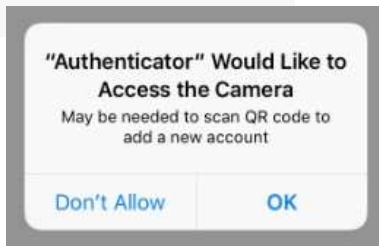
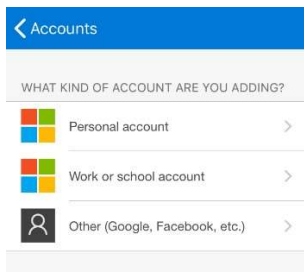


8. On your mobile device, launch the Microsoft Authenticator app.



9. Click **Add account**.

10. Click on **Work or school account**



11. If prompted to allow the Authenticator access to the camera, click OK.

12. Scan the QR code that is presented to you with your mobile device.

13. If successful, your account should now be listed in the Authenticator app.




Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".



[Can't scan image?](#)

[Back](#) [Next](#)

14. Now that the Authenticator app is configured, you can go back to the Authenticator setup page and click **Next**.

Microsoft Authenticator

Let's try it out

Approve the notification we're sending to your app.

[Back](#) [Next](#)

A push notification will be sent to your mobile device...

Are you trying to sign in?

BC Health Providers
[redacted]@BCProvider.ca


Enter the number shown to sign in.

Enter number here

[No, it's not me](#) [Yes](#)

15. On your mobile device, you should receive a notification. Approve it.

Microsoft Authenticator

 Notification approved

[Back](#) [Next](#)

If the push notification worked, it should report the notification was approved.

16. Click **Next**.

17. You should now be logged into BCHealthProvider

If you have questions during or after the tutorial, please contact us at amsspoc.vic@cgi.com