

## BCProvider AD 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 [OneHealthID@gov.bc.ca](mailto:OneHealthID@gov.bc.ca).

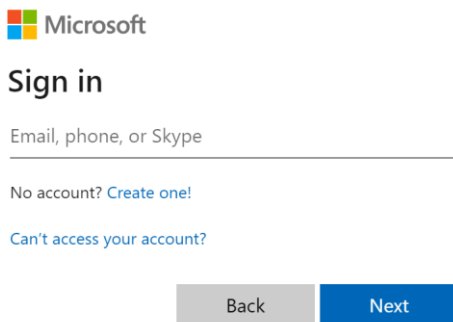
The BCProvider uses Multi-Factor Authentication (MFA) is an additional layer of security that helps protect your online accounts and sensitive information. It enhances the traditional username and password login process by requiring at least two or more forms of verification. This guide aims to explain 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

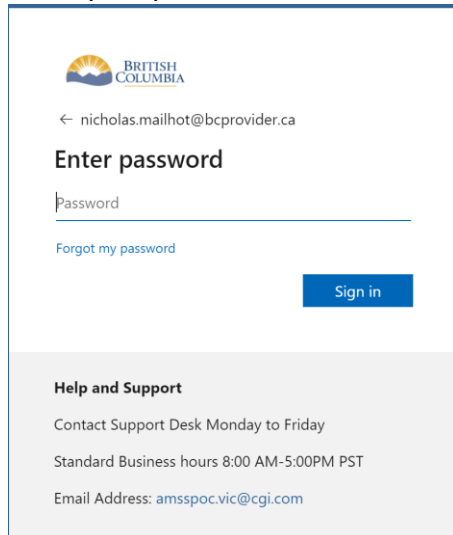
### Setting up the Microsoft Authenticator

1. Go to [bchealthprovider.ca](https://bchealthprovider.ca)
2. Enter your [bcprovider.ca](https://bcprovider.ca) login information



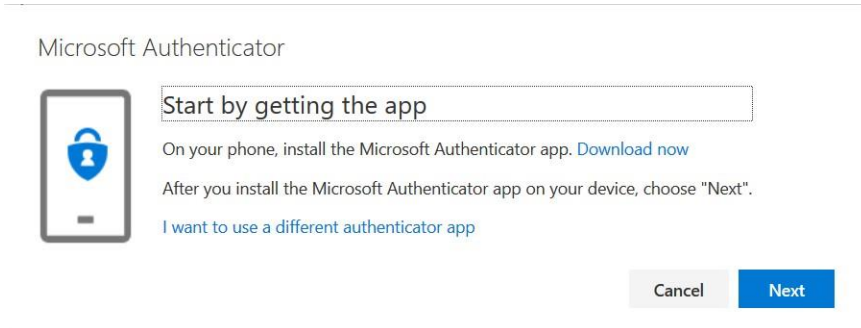
The screenshot shows the Microsoft Sign in page. At the top is the Microsoft logo. Below it is the text "Sign in". There is a text input field labeled "Email, phone, or Skype". Below the input field are two links: "No account? Create one!" and "Can't access your account?". At the bottom are two buttons: "Back" and "Next".

3. Enter your password

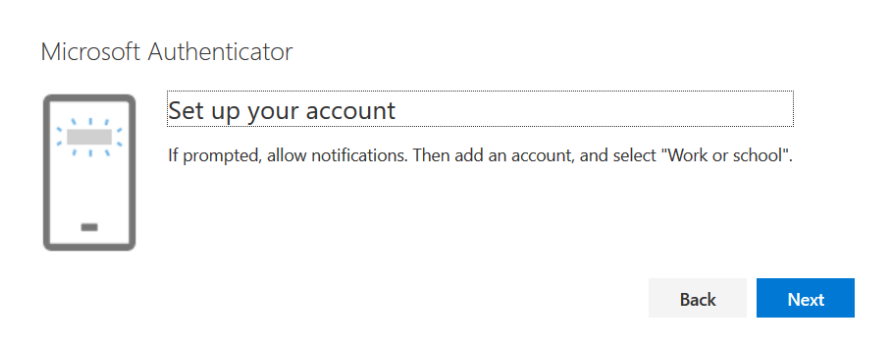


The screenshot shows the BC Provider "Enter password" page. At the top is the British Columbia logo. Below it is the text "Enter password". There is a text input field labeled "Password". Below the input field is a link: "Forgot my password". At the bottom right is a "Sign in" button. At the bottom left is a "Help and Support" section with the following text: "Contact Support Desk Monday to Friday", "Standard Business hours 8:00 AM-5:00PM PST", and "Email Address: [amsspoc.vic@cgi.com](mailto:amsspoc.vic@cgi.com)".

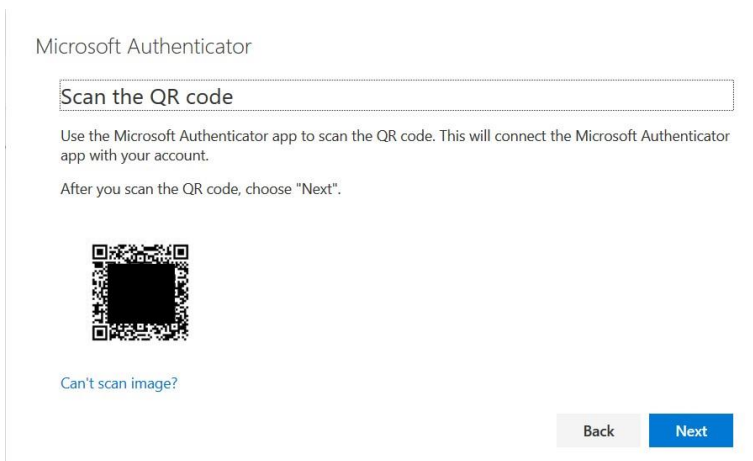
4. You will be prompted for more information on the first login.
5. On your iOS/Android mobile device, you will need to go to the respective app store and install the [Microsoft Authenticator App](#) or Google Authenticator app.
6. If you are using the Google Authenticator App, do not click Next. Click "I want to use a different authenticator app". Go to Appendix A in this document and skip steps 7-15



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

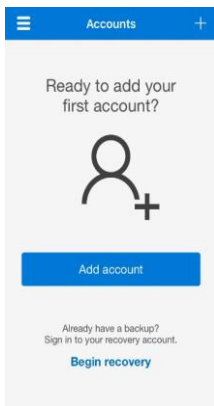


8. Click **Next**



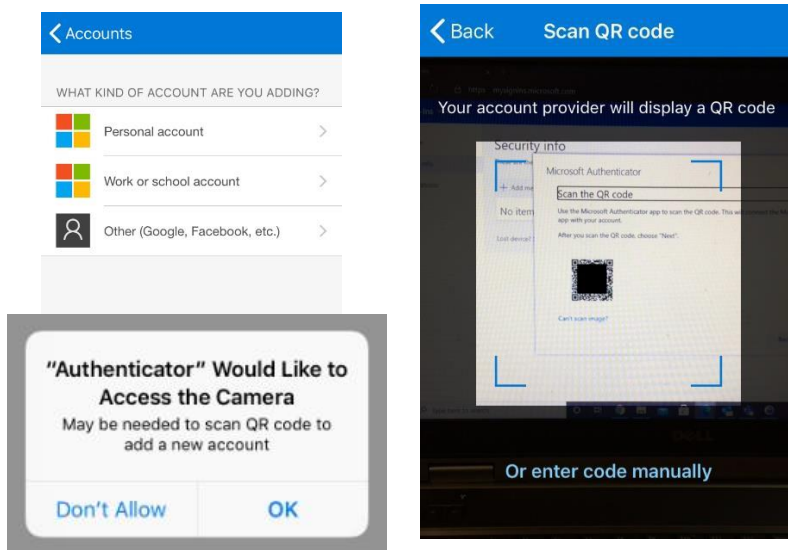
Do not take a picture with your photo app, use the authenticator app.

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



10. Click **Add account**.

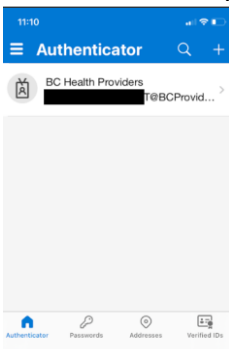
11. Click on **Work or school account**

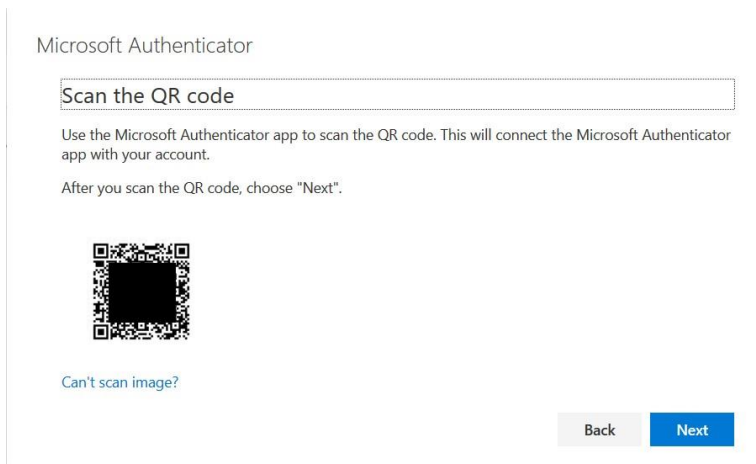


12. If prompted to allow the Authenticator access to the camera, click OK.

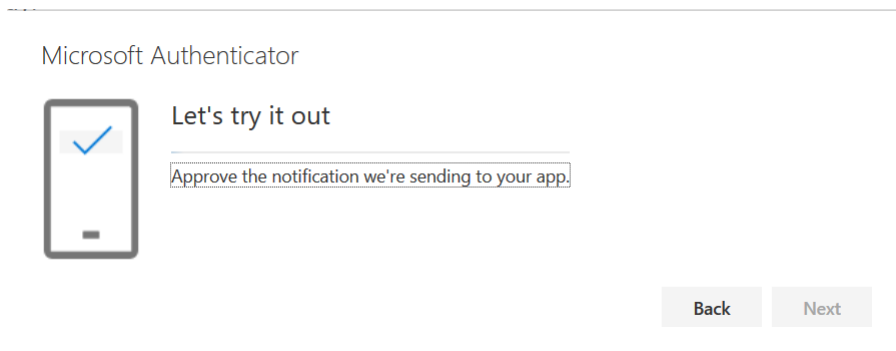
13. Scan the QR code that is presented to you with your mobile device. Do not scan using your photo application. You must scan the QR code in the Microsoft Authenticator app.

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

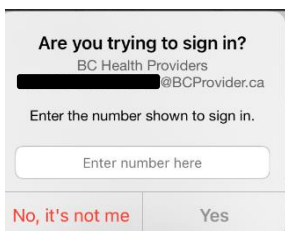




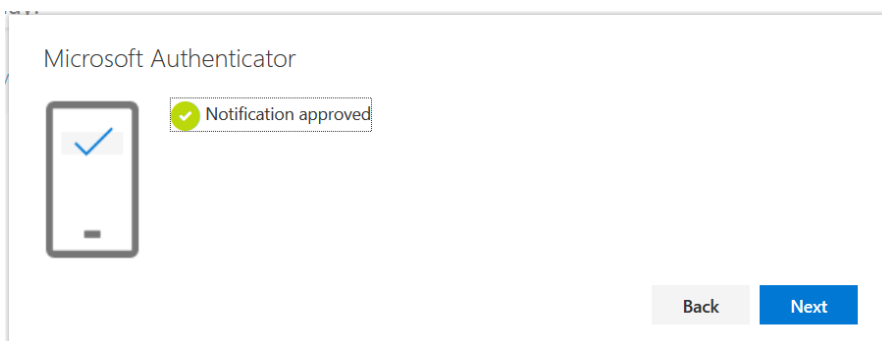
15. Now that the Authenticator app is configured, you can go back to the Authenticator setup page and click **Next**.



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



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



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

17. Click **Next**.

18. You should now be logged into BCHealthProvider

If you have questions during or after the tutorial, please contact us at [OneHealthID@gov.bc.ca](mailto:OneHealthID@gov.bc.ca)

## Appendix A

### Set up Google Authenticator on your smartphone

1. Download the Google Authenticator app from the Play Store or App Store and click Install.
2. Install the Google Authenticator app on your smartphone.
3. Launch the app and select Scan a QR code in the dialog window. To scan, the app needs access to your smartphones camera.
4. You will then be presented with a QR code and a 32-digit code (also known as a security key).  
To proceed, tap the “+” icon in the bottom right of the Google Authenticator app and select “Scan a QR code” to use with your mobile camera. Alternatively, you can manually enter your 2FA codes by choosing to “Enter a setup key”.
5. With your 2-factor authentication now successfully set up, you can begin to use your Google Authenticator codes.
6. Return to step 15 in the guide.

