ⓘ **Note:**

- This guide covers enrolling in multifactor authentication (MFA), primarily by using a GNB-issued or personal smartphone.

- Access to the smartphone is strongly recommended (potentially required) depending on enrollment selections.

- Setup requires access to a computer that is connected to the GNB network (either directly or via the virtual protected network - VPN).
    - Steps involving your computer will be preceded with the following icon 🖥
    - Steps involving your smartphone will be preceded with the following icon 📱

- Your experience will vary depending on your mobile device.

- If you intend to use more than one phone as a secondary form of authentication, you must register each one using this process.

Step 1: Navigate to enrollment page

🖥 From your computer's browser, open the following link:
https://mysignins.microsoft.com/security-info

Step 2: Sign in

- 🖥 Login with your e-mail address (e.g. John.Smith@gnb.ca) and the same password you use to access your email and network account.

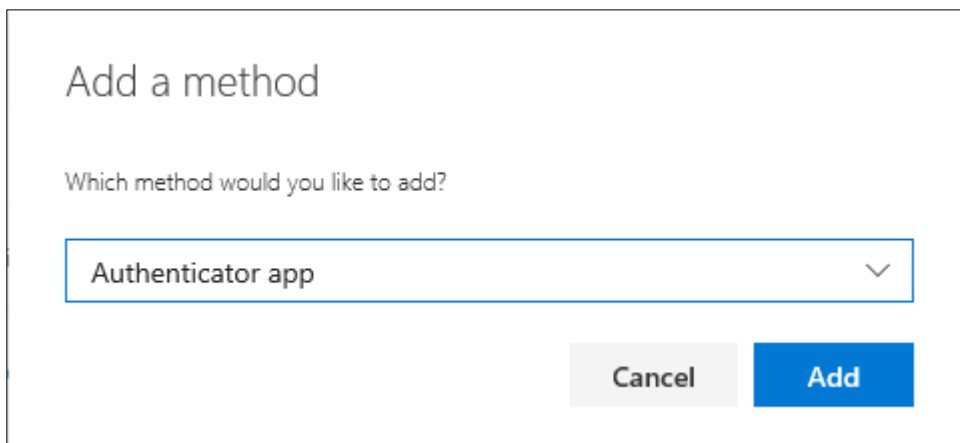## Step 3: Choose "Add method" to add a Multifactor Authentication Method

⬚ Select the **Security Info** tab on the left side of the screen unless it is already selected.
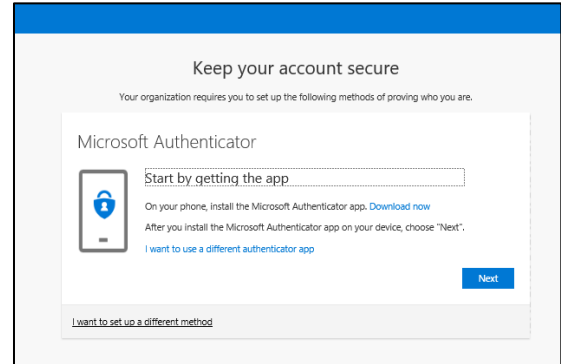
⬚ Click **Add method** to add an additional method.
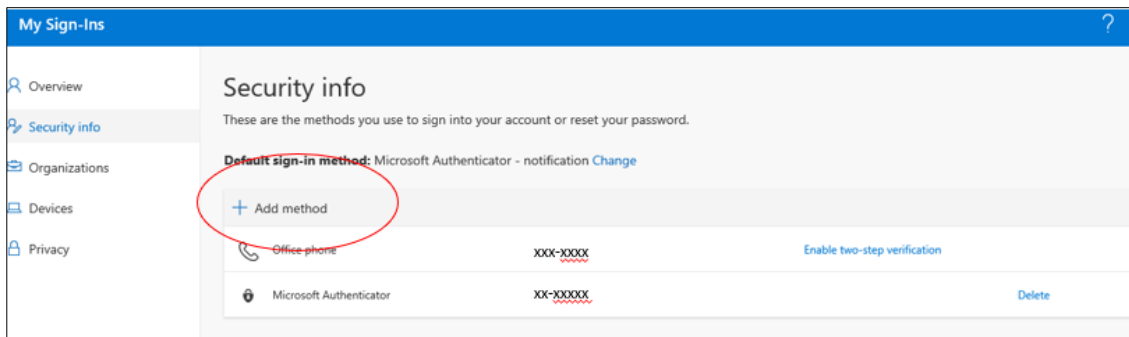
Step 4: Select a Method Type

⬚ Choose the **Authenticator** App from the list of available methods

Step 5:   Keep Your Account Secure Wizard

- ☐ Install the **Microsoft Authenticator** application.
  - o <u>On your mobile phone</u> navigate to the application App Store
  - o Or scan the appropriate QR code shown below to install
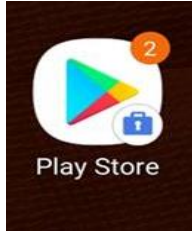
iPhone: Open (Apple/IOS) **Work Apps**

- o Search for **Microsoft Authenticator**
- o Install the application

Or scan the QR code and install the (Apple/IOS) Microsoft Authenticator application.

Android: Open **Playstore Work Apps** – This is on the work side of the phone and will have a lock in the icon.

- o Search for Microsoft Authenticator.
- o Install the application.

Or scan the QR code and install the (Android) Microsoft Authenticator application.

- 🖥️ Once installation on your phone is complete, select **Next** on your computer browser.

⚠️ **Note:**

- If you cannot or do not want to use the Microsoft Authenticator application (which is recommended for anyone with a compatible device) select **I want to set up a different method** link. Appendix I of this document speaks to setting up secondary or alternative authentication methods, which are strongly recommend for all users.

Step 6: Configure Microsoft Authenticator

- 📱 Open the **Microsoft Authenticator** App on your <u>mobile phone</u>.

- 📱 Approve notifications on your <u>mobile phone</u>, if prompted.

- 📱 Touch **Add Account** on your <u>mobile phone</u>.
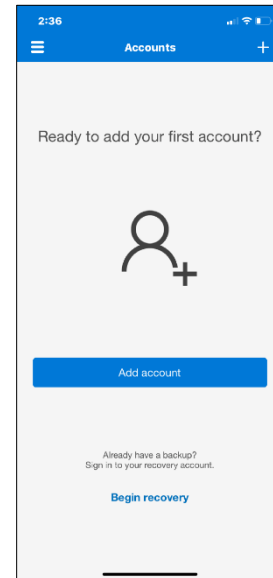
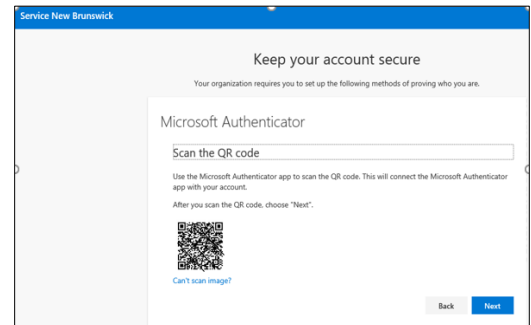- 📱 Touch **Work or School Account** on your <u>mobile phone</u>.
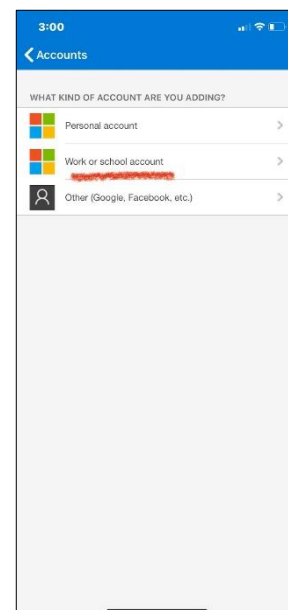
- 📱 Your <u>mobile phone</u> camera will be waiting to take a picture.

- 🖥 Select **Next** on your **<u>computer browser</u>**.

Step 7: Scan QR Code

- 🖥 On your <u>computer browser</u>, you will be prompted to scan something with your camera.

- 📱 Direct your <u>mobile phone</u> camera to scan the **QR code** displayed on your <u>computer browser</u>.
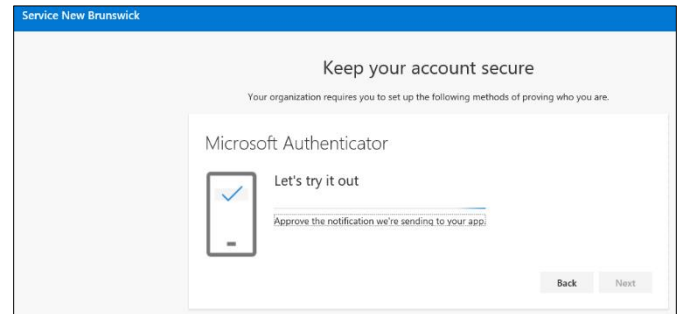
Step 8: Test the App

- 🖥 Select **Next** on your <u>computer browser.</u>

- 📱 A notification is sent to the Microsoft Authenticator app on your <u>mobile phone</u>, to test your account.

Step 9: Approve Notification

- 📱 Select **Approve** on your <u>mobile</u> <u>phone</u>.

- 🌐 Select **Next** on your <u>computer</u>
<u>browser.</u>

Step 10: Success Acknowledged

- 🖥 If successful, you will see that the notification was approved on your <u>computer browser.</u>

- 🖥 Select **Next** on your <u>computer</u>
<u>browser</u>.

- 🌐 If prompted to log in again, you can do so. You can take this opportunity to configure other MFA options, such as a phone call to another device, as a *backup* to the Microsoft Authenticator Application (recommended) (see Appendix 1).
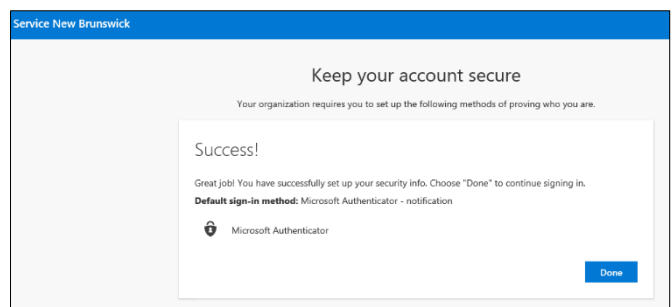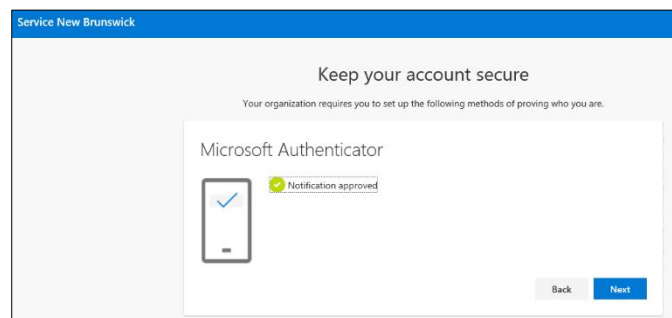
Step 11: Log Out

- 🖥 Once you are done setting up MFA options, you can log out of the account information page by selecting the avatar symbol in the top right-hand corner and choosing **Sign out**.
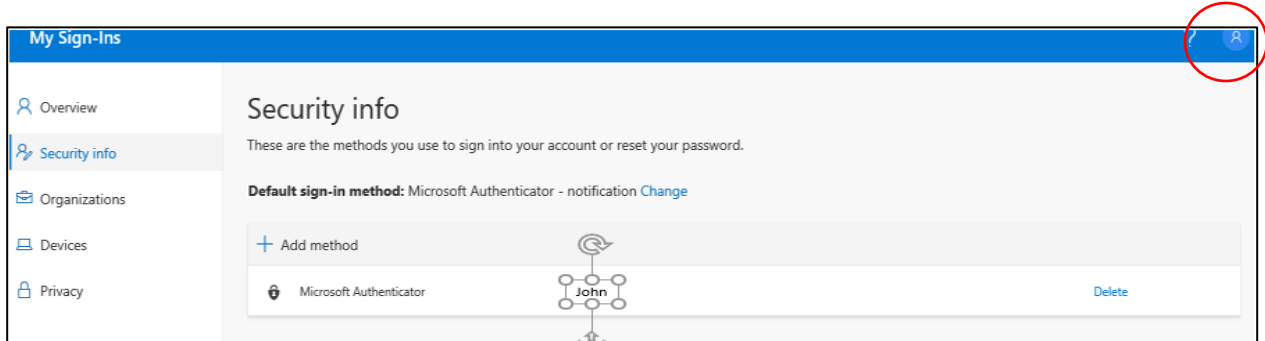
Need technical help?

Department users (Part I)
Contact your IT Service Desk at ITServiceDesk@snb.ca or by calling 1-888-487-5050

Regional Health Authority users (Part III)
Contact your IT service Desk at Service@SNB.ca or by calling 1-844-354-4357
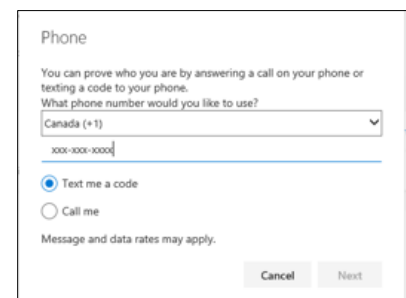
Configuring a secondary verification option

Configuring a secondary verification option is strongly recommended. This will protect you in case the primary MFA verification option is unavailable (e.g. you do not have your phone with you, the battery on your phone has died, etc.).

You can create secondary verification options by following the steps below:

1. Login to https://mysignins.microsoft.com/security-info
2. Click **Add method** to add an additional method.
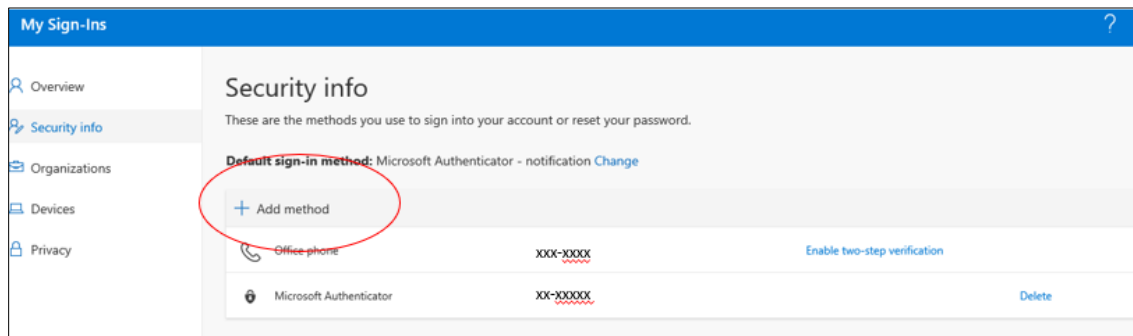
3. Select and configure the additional method by following the on-screen instructions (Receiving a phone call or a SMS / text message).

4. Test the chosen option to verify it works (this automatically occurs once configured – if you are adding the SMS or phone call option, ensure the device or phone you are adding is available.).

5. You can change your default sign-in method from these menus as well – for example, you can revisit this page to update your default sign-in method should you receive a new phone or phone number.