





! Note:

- Ce guide traite de l'inscription à l'authentification multifacteur (AMF) en utilisant principalement un téléphone mobile personnel ou émis par le GNB.
- L'accès au téléphone mobile est fortement recommandé (éventuellement requis) en fonction des sélections d'inscription.
- Le programme d'installation nécessite l'accès à un ordinateur connecté au réseau du GNB (directement ou via le réseau protégé virtuel - RPV).
 - Les étapes impliquant votre ordinateur seront précédées de l'icône suivante : 
 - Les étapes impliquant votre téléphone mobile seront précédées de l'icône suivante : 
- Votre expérience variera en fonction de votre modèle d'appareil mobile.
- Si vous avez l'intention d'utiliser plusieurs téléphones comme forme secondaire d'authentification, vous devez enregistrer chacun d'entre eux à l'aide de ce processus.

Étape 1: Accéder à la page d'inscription


-  À partir du navigateur de votre ordinateur, ouvrez le lien suivant :
<https://mysignins.microsoft.com/security-info>

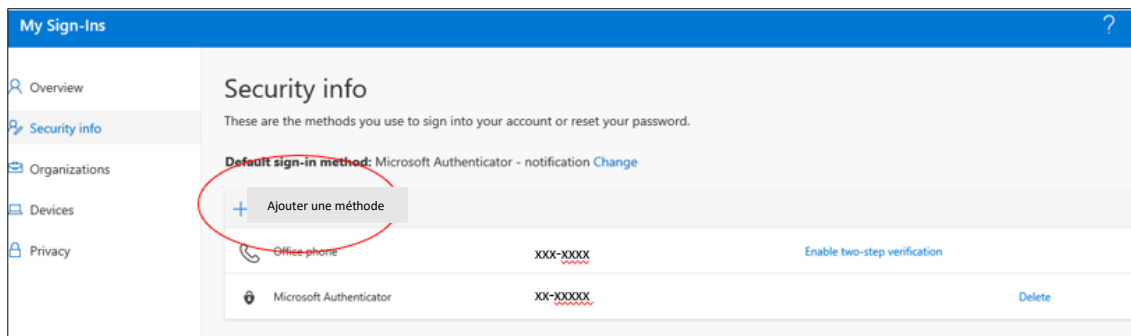
Étape 2: Se connecter

-  Connectez-vous avec votre adresse de courriel (ex. John.Smith@gnb.ca) et le même mot de passe que vous utilisez pour accéder à votre compte courriel et réseau.

Étape 3: Choisir « Ajouter une méthode » pour ajouter une méthode d'authentification multifacteur

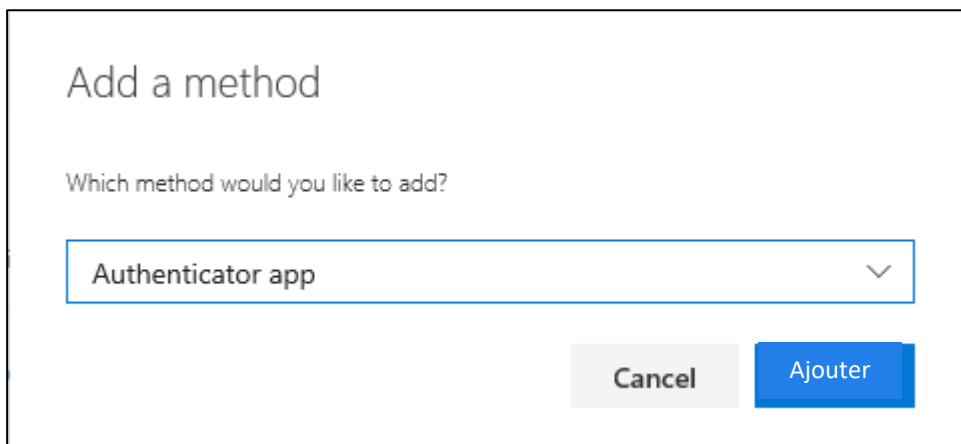
 Sélectionnez l'onglet **Informations de sécurité** situé sur le côté gauche de l'écran, sauf s'il est déjà sélectionné.

 Cliquez sur **Ajouter une méthode** pour ajouter une méthode supplémentaire.




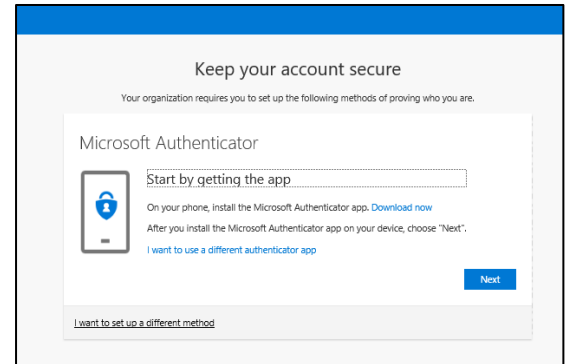
Étape 4: Sélectionner un type de méthode

 Choisissez l'application **Authenticator** dans la liste des méthodes disponibles.

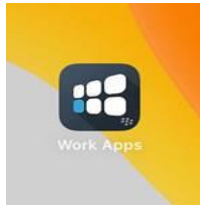


Étape 5: Assistant de sécurisation de votre compte

-  Installez l'application **Microsoft Authenticator**.
 - Sur votre téléphone mobile, accédez à la boutique d'applications.
 - Ou numérisez le code QR approprié montré ci-dessous pour installer



iPhone: Ouvrez (Apple/iOS) **Work Apps**.



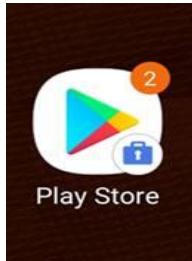
- Recherchez **Microsoft Authenticator**
- Installez l'application



Ou numérisez le code QR et installez l'application (Apple/iOS) **Microsoft Authenticator**.



Android : Ouvrez **Playstore Work Apps** – Il se situe du côté de travail du téléphone et s'affichera avec cadenas sur l'icône.




- Recherchez **Microsoft Authenticator**.
- Installez l'application.



Ou numérisez le code QR et installez l'application (Android) Microsoft *Authenticator*.



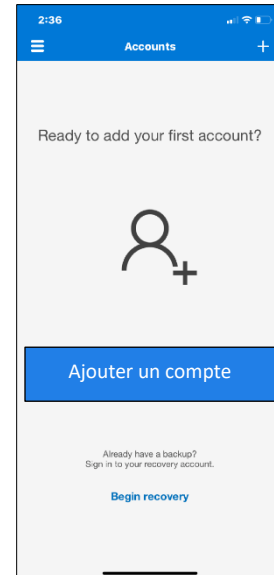
-  Une fois l'installation terminée sur votre téléphone, sélectionnez **Suivant** sur le navigateur de votre ordinateur.

! Note:

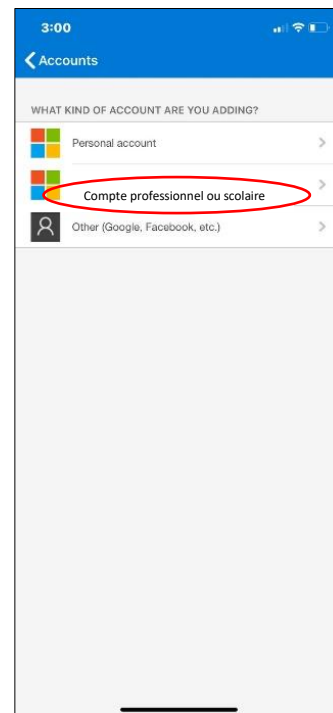
- Si vous ne pouvez pas ou ne souhaitez pas utiliser l'application Microsoft Authenticator (qui est recommandée à toute personne disposant d'un appareil compatible), sélectionnez **Je souhaite configurer un lien de méthode différente**. L'annexe 1 de ce document traite de la configuration de méthodes d'authentification secondaires ou alternatives, qui sont fortement recommandées à tous les utilisateurs.


Étape 6: Configurer *Microsoft Authenticator*

- Ouvrez l'application **Microsoft Authenticator** sur votre téléphone mobile.
- Approuvez les notifications sur votre téléphone mobile, si vous y êtes invité.
- Appuyez sur **Ajouter un compte** sur votre téléphone mobile.




- Appuyez sur **Compte professionnel ou scolaire** sur votre téléphone mobile.





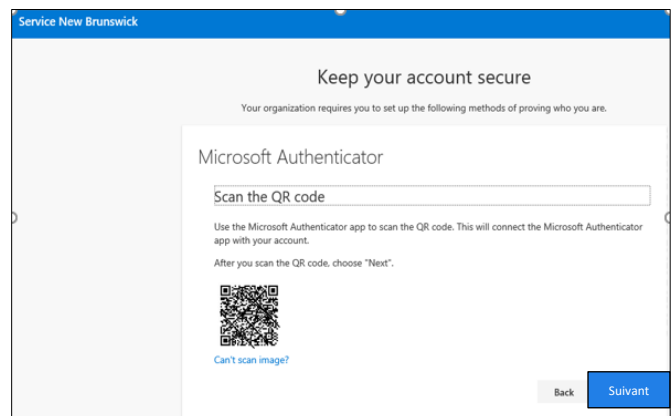
-  La caméra de votre téléphone mobile attendra pour prendre une photo.





-  Sélectionnez **Suivant** sur le navigateur de votre ordinateur.

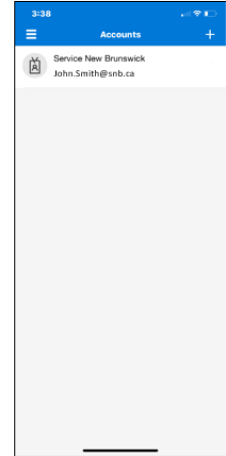
Étape 7: Scanner le code QR

-  Sur le navigateur de votre ordinateur, vous serez invité à numériser quelque chose avec votre appareil photo.
-  Dirigez l'appareil photo de votre téléphone mobile pour scanner le **code QR** affiché sur le navigateur de votre ordinateur.





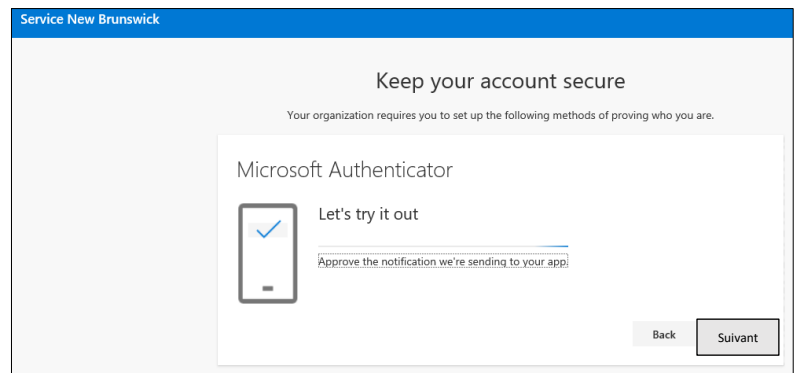
Étape 8: Tester l'application

-  Sélectionnez **Suivant** sur le navigateur de votre ordinateur.
-  Une notification est envoyée à l'application Microsoft *Authenticator* sur votre téléphone mobile, pour tester votre compte.





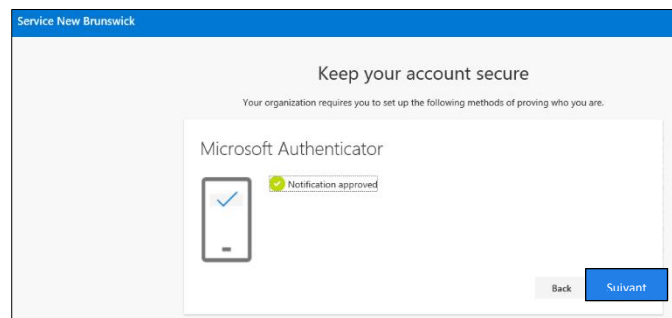
Étape 9: Approuver la notification


-  Sélectionnez **Approuver** sur votre téléphone mobile.
-  Sélectionnez **Suivant** dans le navigateur de votre ordinateur.

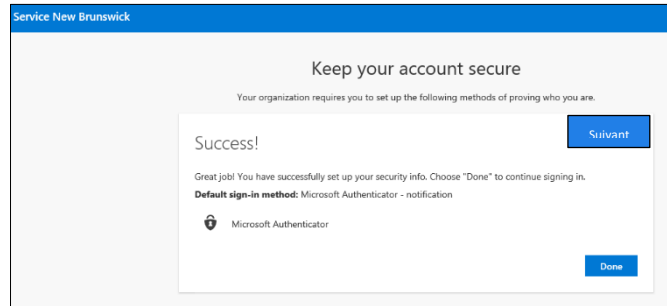


Étape 10: Succès confirmé


-  En cas de succès, vous verrez que la notification a été approuvée sur le navigateur de votre ordinateur.
-  Sélectionnez **Suivant** sur le navigateur de votre ordinateur.

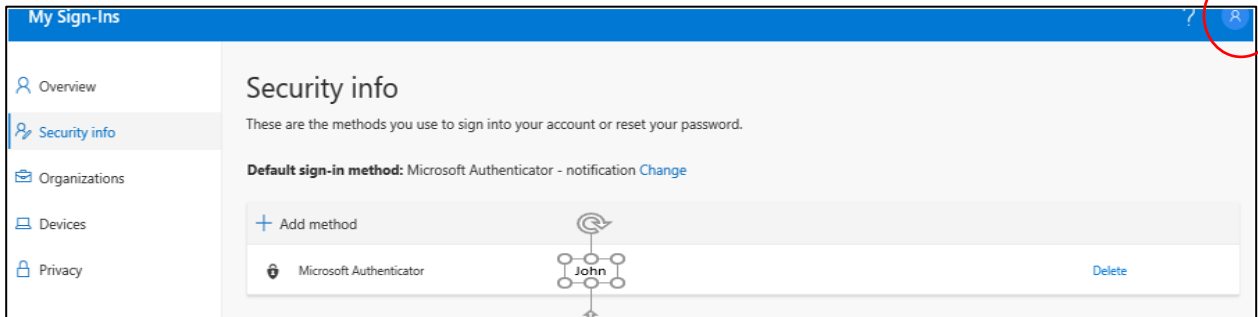


-  Si vous êtes invité à vous reconnecter, vous pouvez le faire. Vous pouvez profiter de cette occasion pour configurer d'autres options d'authentification, tel qu'un appareil téléphonique vers un autre appareil, en tant que sauvegarde de l'application Microsoft *Authenticator* (recommandé) (voir l'annexe 1).



Étape 11: Déconnexion

-  Une fois que vous avez terminé la configuration des options d'authentification, vous pouvez vous déconnecter de la page d'informations sur le compte en sélectionnant l'icône de l'avatar dans le coin supérieur droit, puis **Déconnecter**.



Besoin de soutien technique?

Utilisateurs des ministères (Partie I)

Contactez votre Centre d'assistance informatique à SoutienenTI@snb.ca ou en composant le 1-888-487-5050.


Utilisateurs des régions régionales de la santé (Partie III)

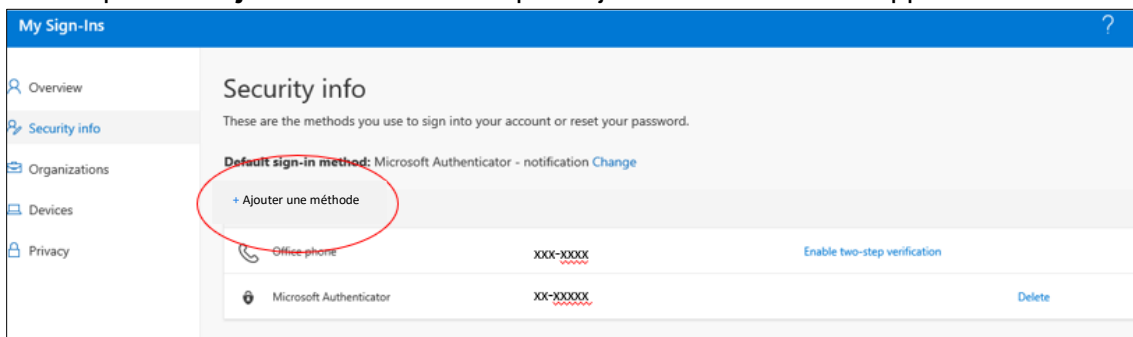
Contactez votre Centre d'assistance informatique à Service@snb.ca ou en composant le 1-844-354-4357.


Configuration d'une option de vérification secondaire

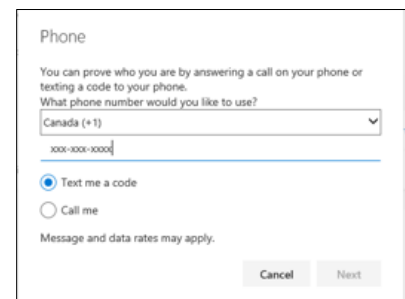
La configuration d'une option de vérification secondaire est fortement recommandée. Cela vous protégera si l'option de vérification AMF principale n'est pas disponible (par exemple, si vous n'avez pas votre téléphone avec vous, si la batterie de votre téléphone est morte, etc.).

Vous pouvez créer des options de vérification secondaires en suivant les étapes ci-dessous :



1.  Connectez-vous à <https://mysignins.microsoft.com/security-info>.
2.  Cliquez sur **Ajouter une méthode** pour ajouter une méthode supplémentaire.



3.  Sélectionnez et configurez la méthode supplémentaire en suivant les instructions à l'écran (recevoir un appel téléphonique ou un SMS / message texte sont les deux possibilités.).



The screenshot shows the 'Phone' configuration screen. It includes the text 'You can prove who you are by answering a call on your phone or texting a code to your phone.' Below this is a dropdown menu for 'What phone number would you like to use?' with 'Canada (+1)' selected. A text input field contains a masked phone number 'xxx-xxx-xxxx'. There are two radio button options: 'Text me a code' (which is selected) and 'Call me'. At the bottom, there is a note 'Message and data rates may apply.' and two buttons: 'Cancel' and 'Next'.

4.  Testez l'option choisie pour vérifier qu'elle fonctionne (cela se produit automatiquement une fois configurée – si vous ajoutez l'option SMS ou appel téléphonique, assurez-vous que l'appareil ou le téléphone que vous ajoutez est disponible.).
5.  Vous pouvez également modifier votre méthode de connexion par défaut à partir de ces menus. Par exemple, vous pouvez retourner sur cette page pour mettre à jour votre méthode de connexion par défaut, si vous recevez un nouveau téléphone ou un nouveau numéro de téléphone.