

# Configuration de l'authentification multifactorielle (AMF) à l'UMoncton

## Pourquoi activer cette mesure?

Activer l'authentification multifactorielle (AMF) est essentiel pour renforcer la sécurité de vos comptes en ligne. En validant et en exigeant plus d'une forme d'authentification, l'AMF protège vos comptes contre les intrusions, la fraude financière et l'hameçonnage. Elle renforce également la protection de vos données personnelles et peut être nécessaire pour se conformer aux normes de sécurité. De plus, l'AMF est devenue plus facile à utiliser grâce à des options conviviales. En résumé, activer l'AMF est une étape cruciale pour protéger votre identité et votre vie numériques. L'authentification multifactorielle est adoptée à l'Université de Moncton afin de mieux sécuriser les données informatiques confidentielles.

Elle est obligatoire pour tous les membres de la communauté universitaire.

## Quelles méthodes dois-je ajouter à mon compte, et son fonctionnement?

Vous devez ajouter les trois (3) méthodes suivantes...

### 1 **L'application « Microsoft Authenticator » pour Apple (iPhone ou iPad) ou appareils Android**

Une notification sera envoyée à votre application et vous devez l'approuver pour compléter la connexion.

- a. Dans le cas que vous n'avez pas de téléphone ou d'appareil mobile, vous pouvez vous rendre à la librairie Édupôle et en échange d'un dépôt de 25\$, vous procurez un jeton de sécurité.

### 2 **Numéro de téléphone secondaire**

Vous recevez un texto automatisé au numéro que vous avez inscrit pour valider votre identité.

### 3 **Adresse de courriel externe pour votre compte**

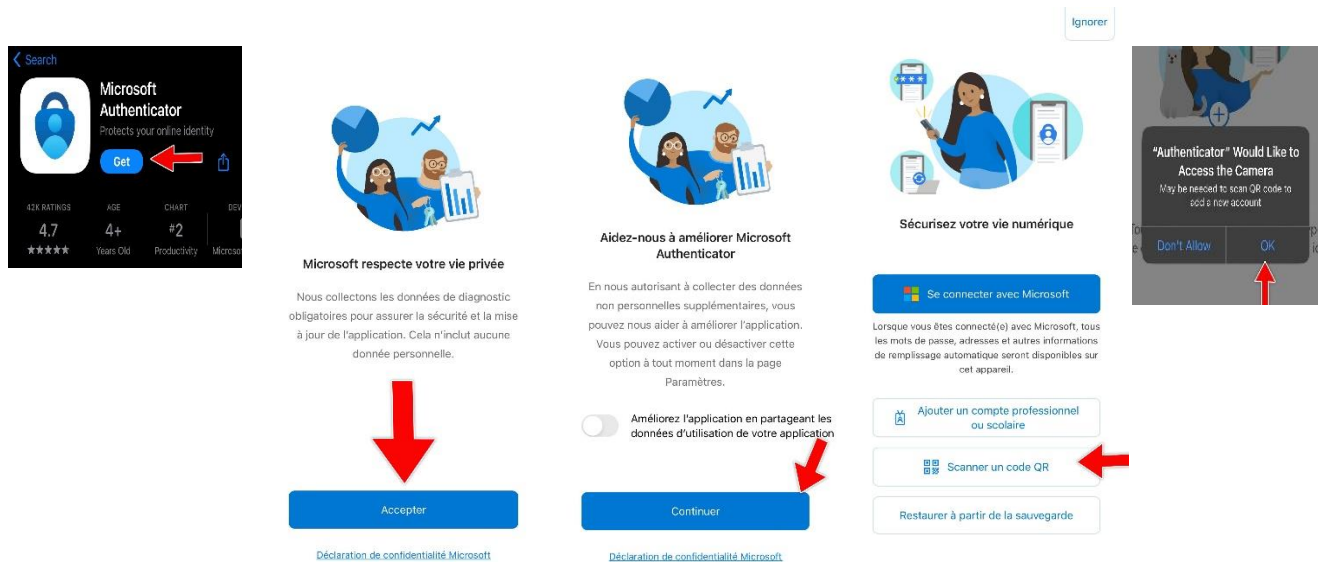
Vous recevez un message automatisé à l'adresse que vous avez inscrite pour valider votre identité.

# Installer Microsoft Authenticator sur votre appareil

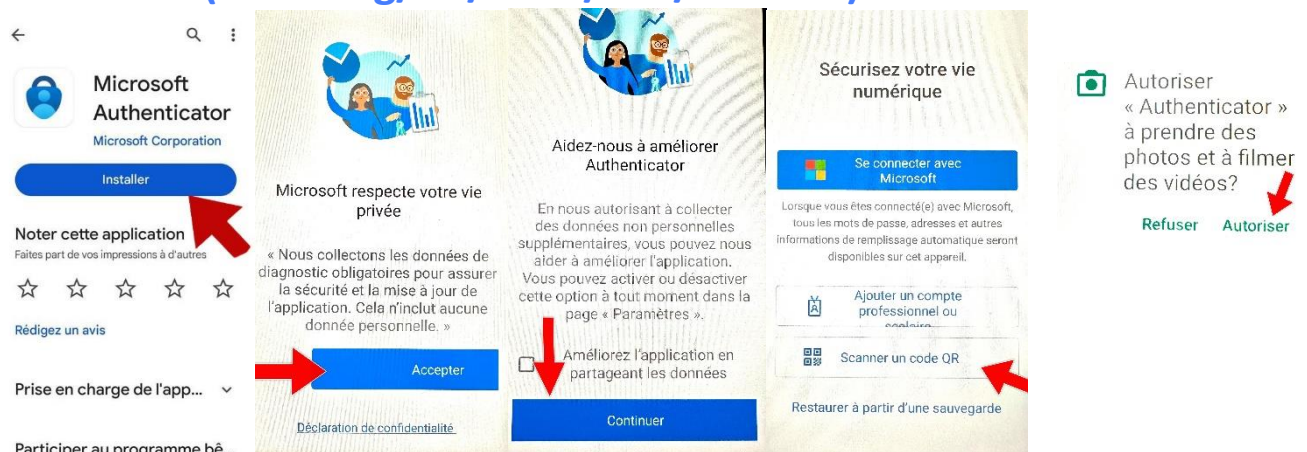
- 1) Scanner le code QR suivant pour choisir quelle version d'Authenticator vous devrez utiliser selon votre appareil.
  - Pour vous faciliter la tâche, à noter que vous avez besoin d'un téléphone intelligent et d'un ordinateur
- 2) Lorsque l'application sera téléchargée, acceptez les notifications et les différentes demandes de confirmation de l'application.



## Apple – (Iphone/Ipad)



## Android – (Samsung/LG/Pixel/TCL/Huawei)

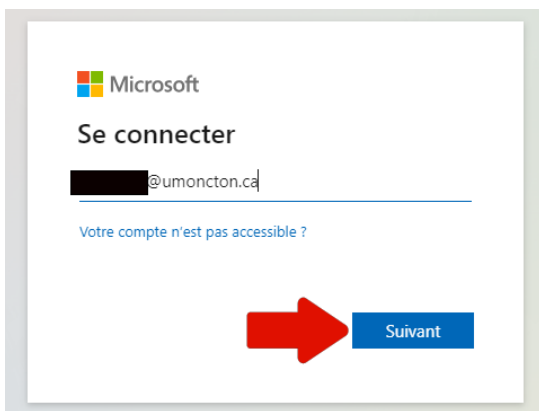


## Comment ajouter des méthodes d'authentification à votre compte avec votre ordinateur?

3) Cliquez sur le lien suivant ou l'ouvrez dans le navigateur de votre choix.

<https://mysignins.microsoft.com/security-info>

4) Entrez votre courriel et votre mot de passe de l'Université  
(votre courriel devrait ressembler à ceci : [eab1234@umoncton.ca](mailto:eab1234@umoncton.ca))




Microsoft

Se connecter

██████████@umoncton.ca

[Votre compte n'est pas accessible ?](#)

 [Suivant](#)



UNIVERSITÉ DE MONCTON  
UNIVERSITY OF MONCTON

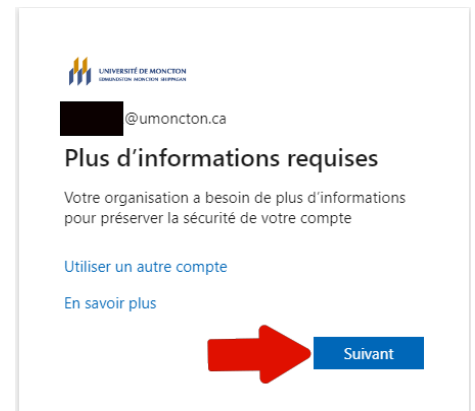
← ██████████@umoncton.ca

Entrez le mot de passe

.....|

[J'ai oublié mon mot de passe](#)

 [Se connecter](#)



UNIVERSITÉ DE MONCTON  
UNIVERSITY OF MONCTON


██████████@umoncton.ca

Plus d'informations requises

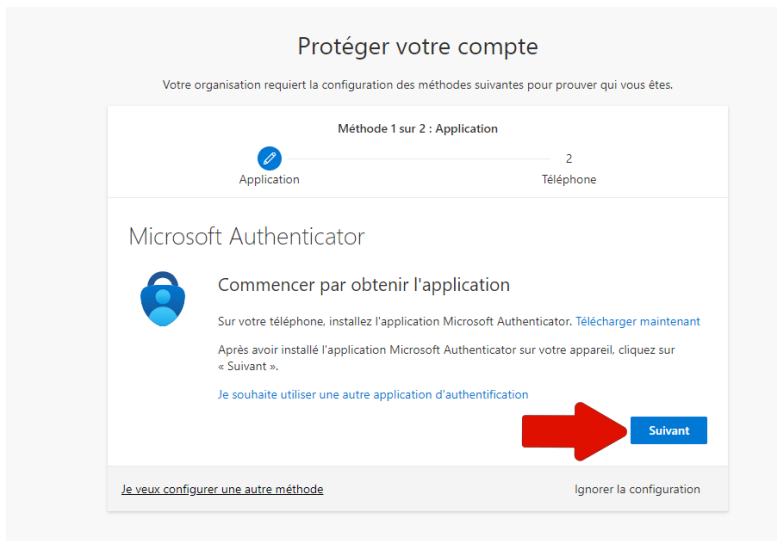
Votre organisation a besoin de plus d'informations pour préserver la sécurité de votre compte

[Utiliser un autre compte](#)

[En savoir plus](#)

 [Suivant](#)

5) Suivre les étapes pour configurer l'AMF avec l'application téléchargée précédemment



Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Méthode 1 sur 2 : Application

Application 2 Téléphone


Microsoft Authenticator

Commencer par obtenir l'application

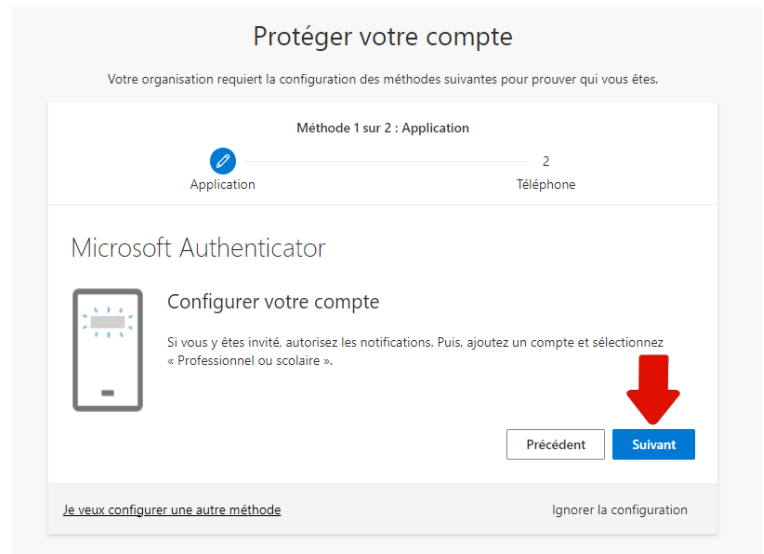
Sur votre téléphone, installez l'application Microsoft Authenticator. [Télécharger maintenant](#)

Après avoir installé l'application Microsoft Authenticator sur votre appareil, cliquez sur « Suivant ».

[Je souhaite utiliser une autre application d'authentification](#)

 [Suivant](#)

[Je veux configurer une autre méthode](#) Ignorer la configuration



Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.


Méthode 1 sur 2 : Application

Application 2 Téléphone

Microsoft Authenticator

Configurer votre compte

Si vous y êtes invité, autorisez les notifications. Puis, ajoutez un compte et sélectionnez « Professionnel ou scolaire ».



[Précédent](#) [Suivant](#)

[Je veux configurer une autre méthode](#) Ignorer la configuration

## Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Méthode 1 sur 2 : Application

Application

2  
Téléphone

### Microsoft Authenticator

#### Scanner le code QR

Utiliser l'application Microsoft Authenticator pour scanner le code QR. Ceci permet de connecter l'application Microsoft Authenticator à votre compte.

Après avoir scanné le code QR, cliquez sur « Suivant ».



Impossible de numériser l'image ?

Scanner le code QR et ensuite

Précédent

Suivant

[Je veux configurer une autre méthode](#)

Ignorer la configuration

## Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Méthode 1 sur 2 : Application

Application

2  
Téléphone

### Microsoft Authenticator



#### Nous allons essayer

Approuvez la notification que nous envoyons à votre application en entrant sur le numéro ci-dessous.

22  
Le code sera aléatoire

Suivant lorsque vous  
aurez entré le code sur  
votre téléphone

Précédent

Suivant

[Je veux configurer une autre méthode](#)

Ignorer la configuration

## Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Méthode 1 sur 2 : Application

Application

2  
Téléphone

### Microsoft Authenticator



✓ Notification approuvée

Précédent

Suivant

[Je veux configurer une autre méthode](#)

Ignorer la configuration

## 6) Configurer l'authentification par numéro de téléphone

Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Méthode 2 sur 2 : Téléphone

Application Téléphone

Téléphone

Vous pouvez prouver qui vous êtes en répondant à un appel sur votre téléphone ou en envoyant un code par SMS à votre téléphone.

Quel numéro de téléphone voulez-vous utiliser ?

United States (+1) Entrez un numéro de téléphone

☒ M'envoyer un code par SMS

☐ Appelez-moi

Le numéro de votre téléphone cellulaire

Des frais relatifs aux messages et aux données peuvent s'appliquer. Si vous choisissez Suivant, cela signifie que vous acceptez Conditions d'utilisation du service et Déclaration sur la confidentialité et les cookies.

Lorsque les options ci-dessus seront complétées, cliquez sur Suivant

Suivant

Ignorer la configuration

Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Méthode 2 sur 2 : Téléphone

Application Téléphone

Téléphone

Vérifié par SMS. Votre téléphone a été inscrit.

Suivant

Ignorer la configuration

Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Méthode 2 sur 2 : Terminé

Application Téléphone

Opération réussie

Bravo ! Vous avez correctement configuré vos informations de sécurité. Cliquez sur « Terminé » pour poursuivre la connexion.

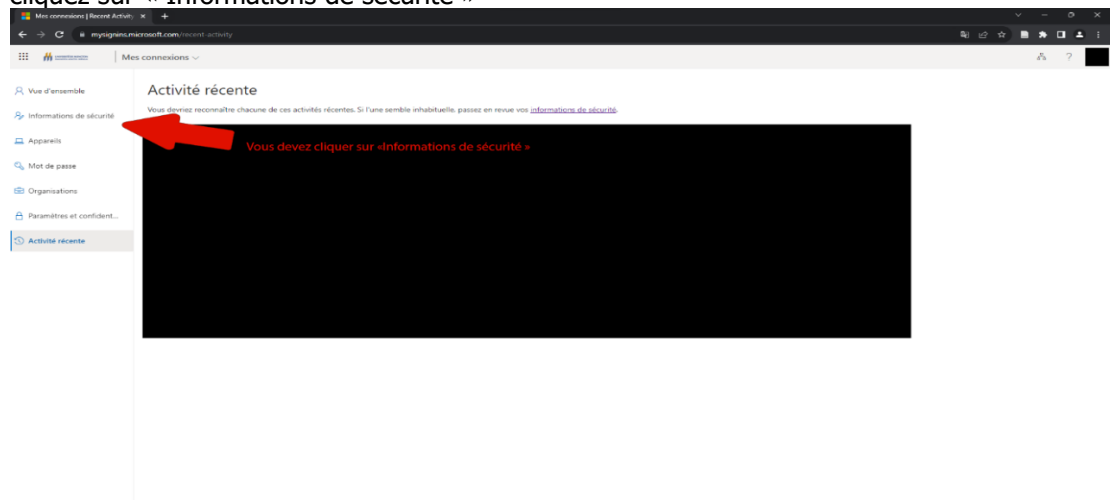
Méthode de connexion par défaut :

Téléphone +1 5619567093

Microsoft Authenticator

Terminé

## 7) Une fois terminée, l'écran d'activité récente apparaît et pour continuer, vous devez donc cliquer sur « Informations de sécurité »



## 8) Ensuite vous cliquez sur « Ajouter une méthode de connexion »

My Sign-Ins | Security Info | Microsoft 365

mysignins.microsoft.com/security-info

Mes connexions

Vue d'ensemble Informations de sécurité Appareils Mot de passe Organisations Paramètres et confident... Activité récente

Informations de sécurité

Voici les méthodes que vous utilisez pour vous connecter à votre compte ou réinitialiser votre mot de passe.

Méthode de connexion par défaut : Microsoft Authenticator - notification [Changer](#)

+ Ajouter une méthode de connexion

Téléphone	<a href="#">Changer</a>	<a href="#">Supprimer</a>
Microsoft Authenticator Authentification multifacteur (MFA) par transmission	<a href="#">Changer</a>	<a href="#">Supprimer</a>

Appareil perdu ? [Se déconnecter partout](#)

**9) Choisir la méthode « E-mail » et entrer votre courriel personnel**

The first screenshot shows a dialog box titled 'Ajouter une méthode' with a list of options: 'Application d'authentification', 'Numéro de téléphone secondaire', 'E-mail', and 'Téléphone (bureau)'. A red arrow points to the 'E-mail' option.

The second screenshot shows a dialog box titled 'E-mail' with the question 'Quelle adresse courriel voulez-vous utiliser?'. It has an input field labeled 'Entrer un courriel' and a 'Suivant' button. A red arrow points to the input field, and another red arrow points to the 'Suivant' button. The text 'Votre courriel personnel' is written next to the input field.

The third screenshot shows a dialog box titled 'E-mail' with the text 'Nous venons d'envoyer un code à [redacted]'. It has an input field labeled 'Entrer le code' and a 'Suivant' button. A red arrow points to the input field, and another red arrow points to the 'Suivant' button.

**10) Lorsque vous voyez les 3 méthodes s'afficher, votre AMF est prête pour l'utilisation**

The screenshot shows a page titled 'Informations de sécurité' with the subtitle 'Voici les méthodes que vous utilisez pour vous connecter à votre compte ou réinitialiser votre mot de passe.' Below this, it says 'Méthode de connexion par défaut : Microsoft Authenticator - notification [Changer](#)'. There is a table with three rows, each representing a connection method. Red arrows point to each row.

+ Ajouter une méthode de connexion			
Téléphone	[redacted]	<a href="#">Changer</a>	<a href="#">Supprimer</a>
Microsoft Authenticator Authentification multifacteur (MFA) par transmissior	[redacted]		<a href="#">Supprimer</a>
E-mail	[redacted]		<a href="#">Supprimer</a>

Appareil perdu ? [Se déconnecter partout](#)