

CONFIGURATION DE L'AUTHENTIFICATION MULTIFACTEUR (**MFA**) POUR OMNIVOX ET CLARA



Table des matières

| | |
|---|----|
| Introduction | 3 |
| Prérequis | 3 |
| 1. Connexion à Omnivox | 4 |
| 2. Choix de la méthode d'authentification MFA..... | 5 |
| 3. Configuration du MFA pour Omnivox/Clara avec Microsoft Authenticator | 6 |
| 4. Configuration du MFA pour Omnivox/Clara avec une adresse courriel | 10 |
| Annexe 1 - Appareils de confiance | 13 |
| Annexe 2 - Modification aux paramètres MFA | 14 |
| Annexe 3 – En cas de problématique | 15 |
| Annexe 4 : Installation de l'application Microsoft Authenticator | 16 |

Introduction

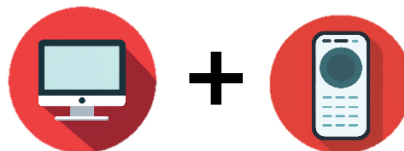
Qu'est-ce que le MFA ?

Le MFA (authentification multifacteur) est une méthode de sécurité qui exige que vous fournissiez deux informations pour accéder à votre compte. En plus de votre mot de passe habituel, vous devrez également fournir une autre forme d'authentification, comme un code unique généré par une application d'authentification ou envoyé par courriel.

Prérequis

Pour pouvoir configurer le MFA sur Omnivox, 2 méthodes d'authentification sont possibles. Vous devez obligatoirement configurer **au moins une des méthodes proposées**.

MÉTHODE #1



Si vous avez accès à un ordinateur ET un appareil intelligent (téléphone ou tablette dotée d'un appareil photo) :

- Authentification à partir de l'application **Microsoft Authenticator** installée sur un appareil intelligent.
- Vous devez **installer l'application** au préalable ([voir procédure d'installation](#)).

MÉTHODE #2



Si vous avez accès à un ordinateur OU un appareil intelligent :

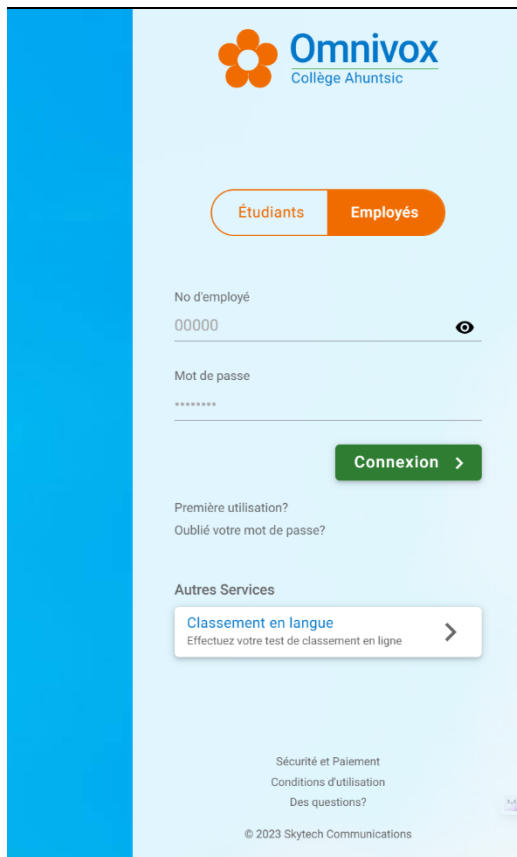
- Authentification à partir d'une **adresse courriel principale** (que ce soit une adresse personnelle ou celle fournie par le Collège).

1. Connexion à Omnivox

Avant tout, il faut vous connecter à Omnivox.

- Accédez à **Omnivox** à partir du lien suivant :

<https://collegeahuntsic.omnivox.ca/>



- **Employé.e :**
 - Entrez votre # **d'employé.e** et votre **mot de passe**.
- **Étudiant.e :**
 - Entrez votre # **d'étudiant.e** et votre **mot de passe**

- La configuration de l'authentification multifacteur (MFA) débutera ensuite.

2. Choix de la méthode d'authentification MFA

Dans la section suivante, nous allons voir comment configurer les deux méthodes d'authentification MFA.

Validation en 2 étapes

Vous devez mettre en place la validation d'identité en 2 étapes pour votre compte utilisateur.

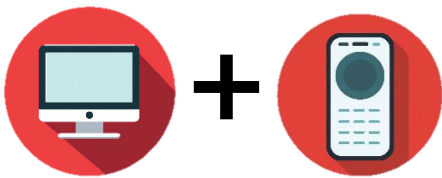
La validation en 2 étapes consiste à fournir deux types d'informations pour confirmer votre identité. Après avoir entré votre identifiant et votre mot de passe, un code de sécurité à usage unique vous sera envoyé. Vous devrez entrer ensuite ce code pour vous connecter à votre compte.

Cette validation d'identité en 2 étapes a pour but de rendre la connexion à votre compte encore plus sécuritaire.

COMMENCER

- En vous connectant sur Omnivox/Clara, cette fenêtre s'affiche.
- Cliquez sur « **COMMENCER** ».

Ensuite...



Si vous configurez le MFA avec un ordinateur et un appareil intelligent avec **Microsoft Authenticator** :

[Cliquez ICI](#)



Si vous avez un ordinateur OU un appareil intelligent et que vous voulez configurer le MFA avec une **adresse courriel principale** :

[Cliquez ICI](#)

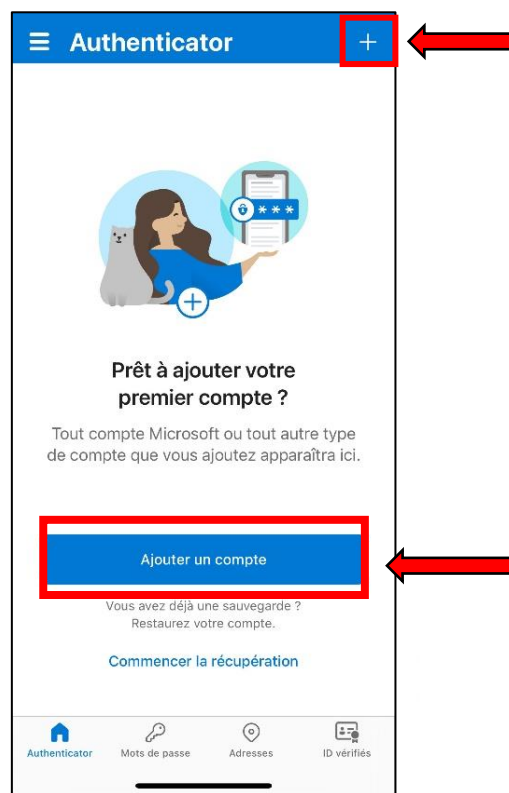
3. Configuration du MFA pour Omnivox/Clara avec Microsoft Authenticator

Si ce n'est pas déjà fait, vous devez installer au préalable l'application sur votre appareil intelligent : [cliquer ICI](#)

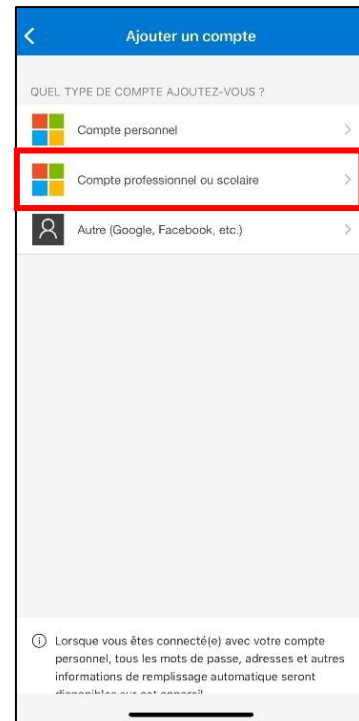
- La fenêtre suivante s'affiche sur Omnivox avec un **code QR** :



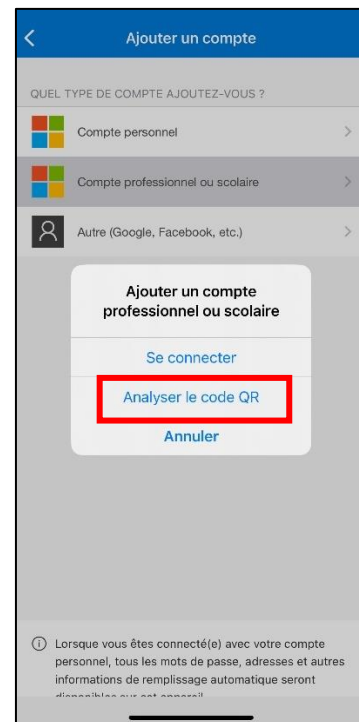
- Lancez l'application **Microsoft Authenticator** sur votre appareil mobile.
- Cliquer sur **ajouter un compte** ou **+**.



- Choisissez « **Compte professionnel ou scolaire** » :



- Choisissez « **Analyser le code QR** » :



Ajout d'une application d'authentification

1. Si vous ne possédez pas d'application d'authentification sur votre appareil mobile, nous vous suggérons d'installer Microsoft Authenticator ou Google Authenticator disponible sur le App Store ou le Google Play Store.
2. Par la suite, veuillez scanner le code QR ci-dessous avec votre application d'authentification en utilisant votre appareil mobile.
3. Une fois le compte ajouté à votre application d'authentification, appuyez sur le bouton **Suivant** afin de tester un des codes générés par votre application et de valider le processus.

Attention: Ne pas utiliser votre application appareil photo.



[Je ne suis pas en mesure de scanner ce code](#)

[Mettre en place une autre méthode de validation d'identité](#)

SUIVANT

- Scannez le **code QR** généré par Omnivox.

Validation de l'application d'authentification

Un code de sécurité à 6 chiffres devrait être généré par votre application. Assurez-vous d'appuyer sur le bouton valider avant que le code expire dans votre application.

Code de sécurité (6 chiffres) *

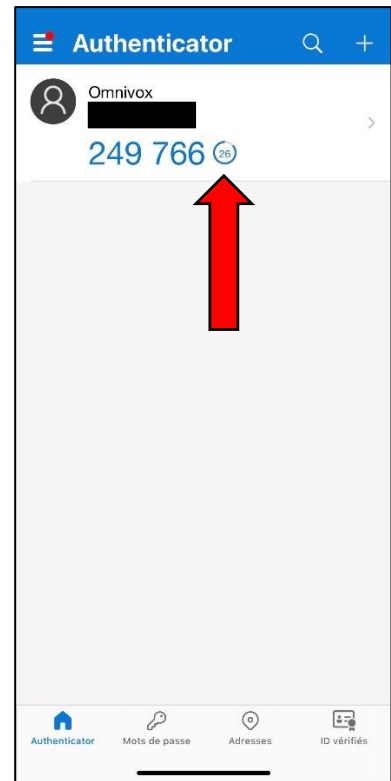
RETOUR

VALIDER

- Sur la page suivante, un **code à 6 chiffres** vous sera demandé.

- Rendez-vous dans l'application **Microsoft Authenticator** (sur votre appareil mobile) afin de saisir le code* fourni pour Omnivox.

****ATTENTION :** le code n'est valable que 30 secondes. Une fois le délai dépassé, un nouveau code vous sera fourni.*



4. Configuration du MFA pour Omnivox/Clara avec une adresse courriel

- Pour configurer une **adresse courriel** comme méthode d'authentification :
 - Une fois sur la page avec le code QR, cliquez sur « **Mettre en place une autre méthode de validation d'identité** ».

Ajout d'une application d'authentification

1. Si vous ne possédez pas d'application d'authentification sur votre appareil mobile, nous vous suggérons d'installer Microsoft Authenticator ou Google Authenticator disponible sur le App Store ou le Google Play Store.
2. Par la suite, veuillez scanner le code QR ci-dessous avec votre application d'authentification en utilisant votre appareil mobile.
3. Une fois le compte ajouté à votre application d'authentification, appuyez sur le bouton **Suivant** afin de tester un des codes générés par votre application et de valider le processus.

Attention: Ne pas utiliser votre application appareil photo.



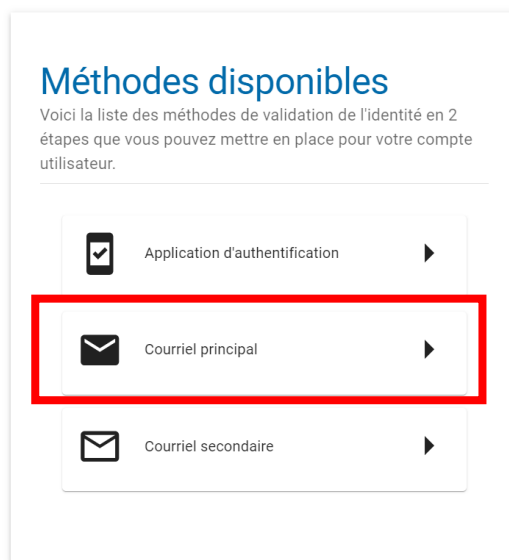
[Je ne suis pas en mesure de scanner ce code](#)

Mettre en place une autre méthode de validation d'identité

[Remettre à plus tard](#)

SUIVANT

- Cliquez sur « **Courriel principal** » :



- Vous allez devoir entrer une **adresse courriel** (personnelle ou professionnelle). **Nous vous conseillons de mettre votre courriel du Collège pour des raisons de sécurité.**

Ajout d'un courriel

La configuration d'un courriel principal comme méthode de validation d'identité est très importante afin d'activer la validation en 2 étapes pour votre compte utilisateur. Un code de sécurité sera envoyé à ce courriel afin de confirmer votre identité.

Courriel *

Mettre en place une autre méthode de validation d'identité

Remettre à plus tard **SUIVANT**

- Vous recevrez par courriel des informations à chaque tentative de connexion sur votre compte, ce qui vous permet de savoir si quelqu'un tente de se connecter à votre insu.

- Sur la page suivante, un **code à 6 chiffres** vous sera demandé.

Validation du courriel

Un code de sécurité à 6 chiffres a été envoyé à l'adresse de courriel [REDACTED]@collegeahuntsic.qc.ca. Vous devriez recevoir ce code dans votre boîte de réception sous peu.

Veillez saisir le code de sécurité reçu et appuyer sur 'Valider'.

Code de sécurité (6 chiffres) *

[Demander un nouveau code](#)

- Récupérez le code fourni par Omnivox dans votre **Boîte courriel** afin de le saisir.



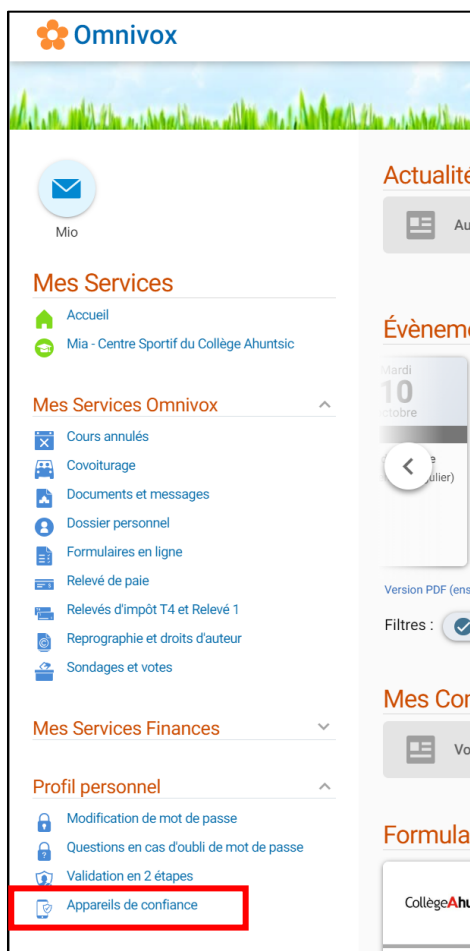
Afin de confirmer le courriel à ajouter comme méthode de validation d'identité en 2 étapes, veuillez utiliser le code de sécurité ci-dessous.

Votre code de sécurité:

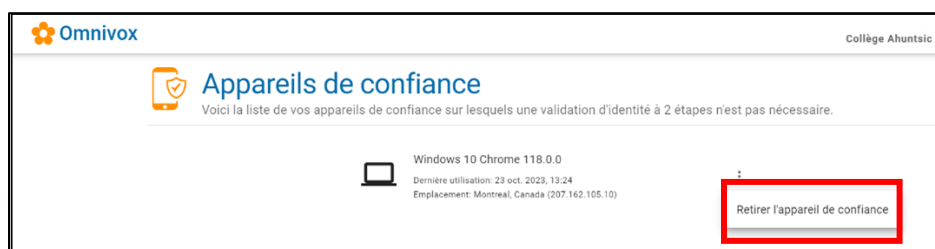
636044

Annexe 1 : Appareils de confiance

Afin de gérer vos appareils de confiance, il suffit de vous rendre sur votre page Omnivox et d'aller dans la section « **Profil Personnel** » et cliquer sur « **Appareils de confiance** »



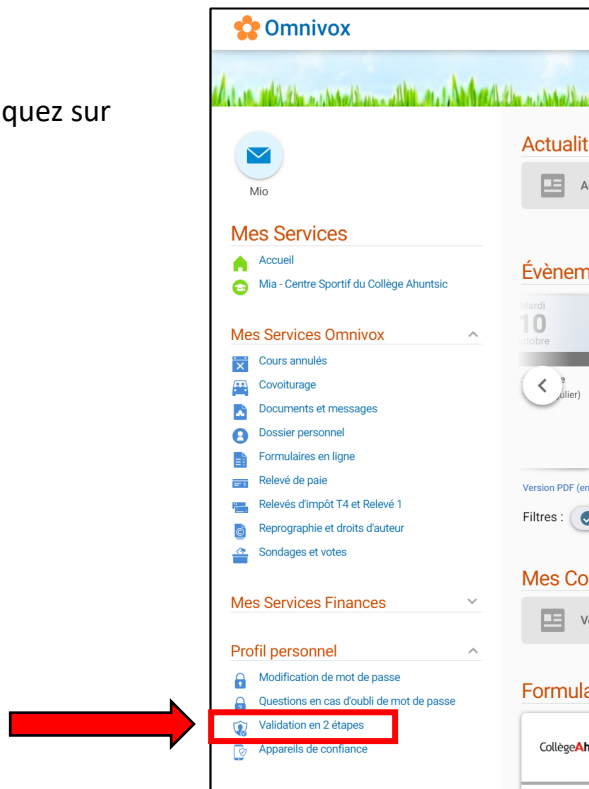
Dans cet espace, vous pouvez gérer vos appareils de confiance. En cas de changement, perte ou vol d'un appareil, le retrait de celui-ci comme appareil de confiance est possible.



Annexe 2 : Modification aux paramètres MFA

Pour modifier vos paramètres MFA :

- Rendez-vous dans la section « **Profil personnel** » et cliquez sur « **Validation en 2 étapes** » :



- À partir de cette page, vous pouvez gérer vos méthodes MFA pour :



| | |
|------------------|--|
| Ajouter | Pour ajouter une autre méthode (Application, courriel principal, courriel secondaire) d'authentification pour le MFA |
| Modifier | Vous ramène sur la page afin de scanner le code QR en cas de nouvel appareil |
| Tester | Vous demande le code MFA à 6 chiffres afin de tester si le tout est synchronisé et correct |
| Supprimer | Pour supprimer la méthode d'authentification |

Annexe 3 : En cas de problématique

Si vous rencontrez un problème avec le MFA, voici **les personnes ressources** à contacter :

Étudiants, accès Omnivox : Comptoir blanc du SOE

Employés, accès Clara/Omnivox Pédagogie : Comptoir blanc de SOE poste 2223

Employés, accès Clara/Omnivox Finances : Service de la comptabilité poste 2141

Employés, accès Clara/Omnivox RH/Paie : Service de la comptabilité poste 2139

En cas de **perte ou de vol** de votre appareil, il sera possible pour la personne ressource de retirer l'appareil des **appareils de confiance** de votre profil. Un code temporaire valide pour 12 heures pourra également être généré pour remplacer celui fourni par l'application **Microsoft Authenticator**.

Annexe 4 : Installation de l'application Microsoft Authenticator

- Scannez l'un des deux codes QR suivants pour télécharger l'application **Microsoft Authenticator** à partir de Google Play ou de l'App Store. *



Téléchargez l'application sur votre téléphone*

Scannez le code QR avec votre appareil mobile Android ou iOS.



Google Play



App Store

*Vous pouvez également utiliser les liens suivants si nécessaire:

- Google Play: <https://go.microsoft.com/fwlink/p/?linkid=2168850&clid=0xc0c&culture=fr-ca&country=ca>
- App Store: <https://go.microsoft.com/fwlink/p/?linkid=2168643&clid=0xc0c&culture=fr-ca&country=ca>