CÉGEP DE SAINT-HYACINTHE

Guide de l'authentification à deux facteurs (A2F/MFA) – Omnivox et Clara

Table des matières

Version : 24 août 2023

CÉGEP DE SAINT-HYACINTHE

Comprendre l'authentification à deux facteurs

Clara est un système utilisé uniquement par les employés du Cégep; les étudiants ne sont pas concernés par ce logiciel et peuvent donc ignorer les consignes qui s'y rattachent.

À noter que les employés qui utilisent Omnivox-Test et Clara-Test doivent également enregistrer leurs deuxièmes facteurs dans ces systèmes.

- ✓ Pour Skytech (le fournisseur de Clara et Omnivox), l'authentification à deux facteurs se nomme plutôt la *validation en 2 étapes.* C'est exactement la même chose!

- ✓ L'authentification à deux facteurs d'Omnivox et Clara se configure dans Omnivox seulement. Une fois que vous vous êtes inscrits dans Omnivox, vous le serez également dans votre compte correspondant dans Clara (si vous en avez un). Vous pourrez donc utiliser les mêmes deuxièmes facteurs dans Clara que ceux que vous avez configurés dans Omnivox.

- ✓ Ce deuxième facteur pour Clara et Omnivox est complètement indépendant de celui de Microsoft 365, pour laquelle la procédure diffère passablement. Il sera important d'utiliser les bons deuxièmes facteurs avec les bons logiciels ou systèmes.

- ✓ Il est très simple d'enregistrer un deuxième facteur pour un compte générique (qui n'est pas à votre nom, par exemple *agent_securite*). Il s'agit de choisir l'option pour recevoir le code à 6 chiffres par courriel, et d'indiquer une boîte partagée avec vos collègues qui doivent également accéder au compte générique.

- ✓ L'option de jeton physique n'est pas offerte. Il faut plutôt se rabattre sur l'option de courriel, où vous recevrez le code à 6 chiffres lorsque requis.

CÉGEP DE SAINT-HYACINTHE

Choisir ses deuxièmes facteurs

Il est fortement recommandé de choisir plus d'un 2ème facteur puisqu'en cas de dysfonctionnement de l'un de ceux-ci, vous pourrez recourir à l'autre sans devoir solliciter l'aide du CAT!

✓ **OPTION 1 et 2 – APPAREIL MOBILE (MEILLEURE OPTION – la plus conviviale, sécuritaire, etc.)**
Si vous possédez un téléphone mobile et que vous consentez à l'utiliser comme deuxième facteur, voici les choix qui s'offrent à vous (il est recommandé d'en sélectionner au moins deux):

- 1-Utiliser l'application d'authentification « Microsoft Authenticator » sur son appareil mobile (**méthode recommandée, la plus sécuritaire et ne nécessitant pas de connexion Internet, sauf pour l'installation**). Vous pouvez l'utiliser aussi pour votre authentification Microsoft 365, ce qui centralise et simplifie la gestion de vos deuxièmes facteurs!

Microsoft Authenticator

- 2-Utiliser l'application « Omnivox Mobile » sur son appareil mobile (**aussi sécuritaire que « Microsoft Authenticator », mais nécessite une connexion Internet pour son fonctionnement – à noter également qu'au moment d'écrire ces lignes, le code n'est envoyé que dans les notifications du téléphone et ce n'est donc pas convivial…**).

✓ **OPTION 3 – ADRESSE COURRIEL PRINCIPALE**
POUR LES EMPLOYÉS : Nous vous invitons à utiliser votre adresse courriel institutionnelle (@cegepsth.qc.ca). Cette option est sécuritaire, puisque votre boîte de courriel est protégée par l'authentification à deux facteurs de Microsoft. À noter qu'il est possible d'utiliser une adresse personnelle, bien que ce ne soit pas recommandé.

POUR LES ÉTUDIANTS : Vous pouvez utilisez votre adresse courriel du Cégep(DA@etu.cegepsth.qc.ca) et récupérer le code en vous connectant dans un navigateur Web (exemples : Chrome, Edge, etc.) à https://outlook.com. Il est possible d'utiliser une adresse personnelle, mais assurez-vous de protéger votre courriel personnel en activant l'authentification à deux facteurs pour celle-ci!

CĒGEP DE SAINT-HYACINTHE

Inscription à l'authentification à deux facteurs en libre-service

ATTENTION!

- ✓ **L'authentification à deux facteurs d'Omnivox et Clara se configure dans Omnivox seulement. Une fois que vous vous êtes inscrits dans Omnivox, vous le serez également dans votre compte correspondant dans Clara (si vous en avez un).**
- ✓ **Il est important de configurer au moins deux facteurs pour pouvoir se dépanner en libre-service. Le premier facteur dont vous effectuerez la configuration deviendra votre facteur principal. Si vous en configurez un second, vous pourrez y recourir si votre facteur principal fait défaut, ce qui vous évitera de devoir contacter le soutien technique. Nous recommandons l'utilisation de l'application « Microsoft Authenticator » comme moyen principal.**

Voici les deuxièmes facteurs proposés:

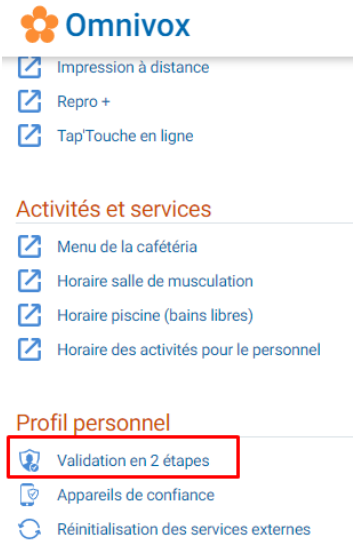
Pour configurer **l'application avec « Microsoft Authenticator » (option recommandée)**, la procédure est ici.

Pour configurer **l'application avec « Omnivox Mobile »,** la procédure est ici.

Pour configurer **l'application avec une « adresse courriel principale »**, la procédure est ici.

Application « Microsoft Authenticator »

1. Ouvrez une session Omnivox, puis en bas, à gauche, cliquez sur « Validation en 2 étapes » :



2. Vous pouvez cliquer sur « Ajouter », puis sélectionner « Application d'authentification » (Attention! Si vous utilisez déjà l'application « Omnivox Mobile » sur votre cellulaire, il se peut qu'un autre écran soit affiché, en quel cas nous vous recommandons de sélectionner l'option « Mettre en place une autre méthode de validation d'identité », puis de continuer avec les étapes suivantes, à partir du #3):

3. La fenêtre suivante s'affichera avec un code QR :

4. Si « Microsoft Authenticator » n'est pas déjà installé sur votre appareil mobile Android ou iOS, vous devez le téléchargez et l'installer dans le magasin d'applications de votre appareil:

5. Démarrer sur votre appareil mobile (téléphone ou tablette) l'application « *Microsoft Authenticator* ». *Si un code (ou empreinte digitale ou autre) vous est demandé pour l'ouverture d'Authenticator, il s'agit simplement du code de verrouillage de votre téléphone, qui est habituellement un code de type « PIN » à 4 ou 6 chiffres!*

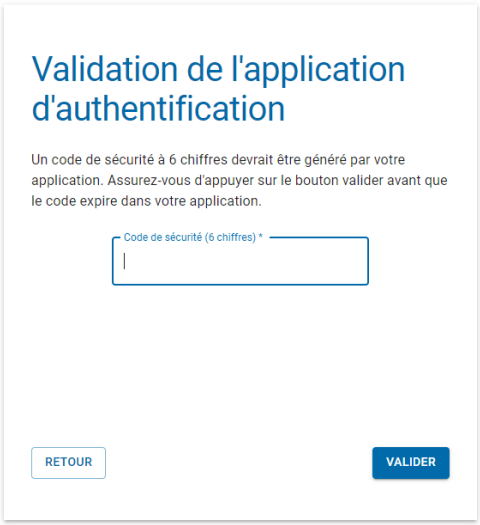
6. Appuyez sur le bouton qui permet l'ajout d'un compte (il s'agit du caractère « + » en haut à droite) et sélectionnez « Compte professionnel ou scolaire », puis « Scanner un code QR ».

7. L'application va vous demander une autorisation pour utiliser la caméra. Vous pouvez y consentir de façon permanente ou pour cette fois seulement, si l'option vous est offerte. Cette permission n'est requise que pour analyser le code QR.

8. Placez votre téléphone intelligent devant le code QR qui s'affiche à votre écran et numérisez-le. Votre compte Omnivox s'ajoutera dans l'application mobile et il vous sera indiqué que l'opération a réussi. Si vous n'y arrivez pas, réessayez. Si vos tentatives sont infructueuses, vous pouvez appuyer sur « Je ne suis pas en mesure de scanner ce code » à l'écran de l'ordinateur. Des instructions vous seront données pour utiliser un code chiffré, lequel permet également l'enregistrement de votre compte sur votre appareil mobile.

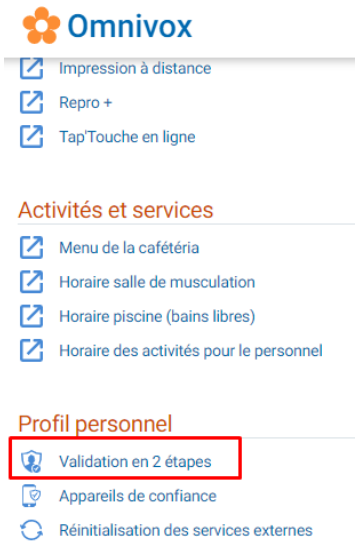
9. Sur votre ordinateur, cliquez sur le bouton « Suivant ».

10. Vous verrez un écran comme celui-ci à l'ordinateur, où un code à 6 chiffres sera exigé, code que vous retrouverez dans « Microsoft Authenticator » en appuyant sur l'item « Omnivox » (*il est important de ne pas trop attendre de passer à la prochaine étape, puisque le délai de validité du code est court)* :



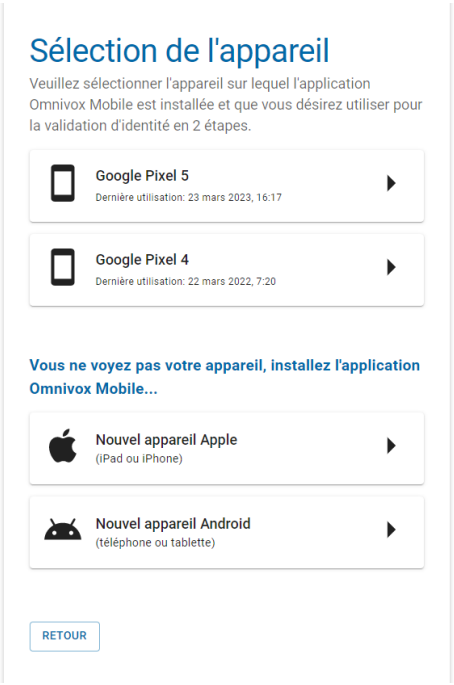
11. Cliquez sur « Valider » et le tour est joué! Si toutefois l'opération ne fonctionne pas, il faut recommencer du début, en prenant soin de détruire l'entrée « Omnivox » sur votre téléphone, en appuyant sur celle-ci, puis sur la petite roue dentelée en haut à droite, pour finalement cliquer sur « Supprimer le compte ».

1. Ouvrez une session Omnivox, puis en bas, à gauche, cliquez sur « Validation en 2 étapes » (Attention! Si vous utilisez déjà l'application « Omnivox Mobile » sur votre cellulaire, il se peut qu'un autre écran soit affiché, en quel cas vous pouvez suivre les étapes qui suivent à partir du #3):



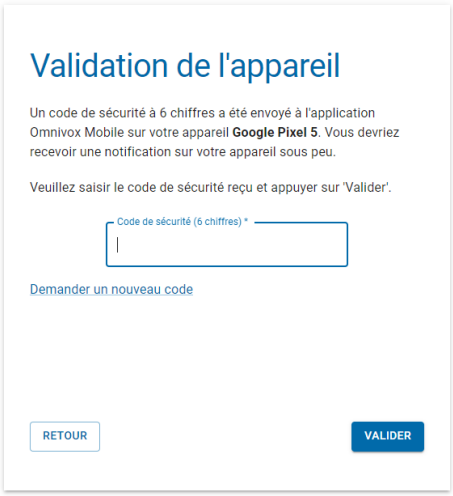
2. Vous pouvez cliquer sur « Ajouter », puis sélectionner « Application Omnivox Mobile » :

3. Un écran semblable s'affichera avec ou sans appareil, selon que vous avez déjà installé « Omnivox Mobile » sur l'un de vos appareils :



4. Si vous pouvez choisir un appareil et que vous désirez utiliser l'un d'eux pour les validation de deuxième facteur, cliquer sur celui-ci à l'écran. Sinon, suivez les consignes à l'écran en cliquant sur le type d'appareil que vous souhaitez utiliser (Apple ou Android).

5. Vous verrez un écran comme celui-ci à l'ordinateur, où un code à 6 chiffres sera exigé, code que vous retrouverez dans les notifications de votre appareil mobile (*il est important de ne pas trop attendre de passer à la prochaine étape, puisque le délai de validité du code est court)* :

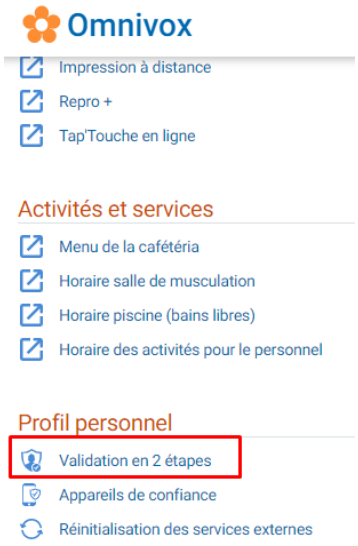


6. Cliquez sur « Valider » et le tour est joué! Si toutefois l'opération ne fonctionne pas, il faut cliquer sur « Demander un nouveau code » et réessayer.

Adresse courriel principale

Employés : cette option n'est pas offerte pour Omnivox-Test et Clara-Test! Bien qu'il soit possible de sélectionner l'option, vous ne recevrez jamais de courriel! Il faut donc choisir un autre deuxième facteur.

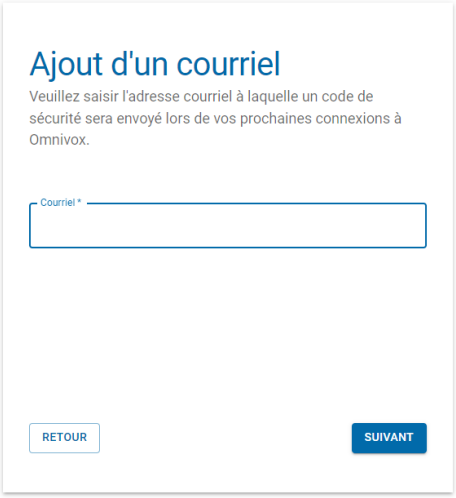
1. Ouvrez une session Omnivox, puis en bas, à gauche, cliquez sur « Validation en 2 étapes » (Attention! Si vous utilisez déjà l'application « Omnivox Mobile » sur votre cellulaire, il se peut qu'un autre écran soit affiché, en quel cas nous vous recommandons de sélectionner l'option « Mettre en place une autre méthode de validation d'identité », puis de continuer avec les étapes suivantes à partir du #3):



2. Vous pouvez cliquer sur « Ajouter », puis sélectionner « Courriel principal » :

3. **EMPLOYÉS** : Vous verrez ensuite cet écran où vous pouvez entrer votre courriel du Cégep, sous le format « @cegepsth.qc.ca », puis il faut cliquer sur « Suivant » :

   ÉTUDIANTS : Il faut utiliser votre adresse courriel en format da@etu.cegepsth.qc.ca et ensuite récupérer le code à l'étape 4 ci-dessous dans un navigateur Web de votre choix, tel Chrome ou Edge, à https://outlook.com), puis il faut cliquer sur « Suivant » :



4. Il faut ensuite entrer le code à 6 chiffres reçu dans votre boîte courriel (soyez patients, ça peut prendre plusieurs secondes!), pour ensuite cliquer sur « Valider » :

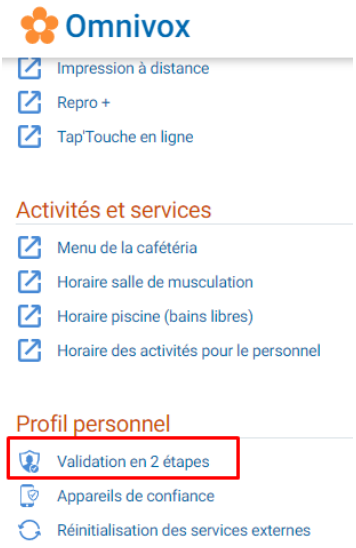
5. Cliquez sur « Valider » et le tour est joué! Si toutefois l'opération ne fonctionne pas, il faut cliquer sur « Demander un nouveau code » et réessayer.

CÉGEP DE SAINT-HYACINTHE

Comment modifier ses informations d'authentification à deux facteurs

ATTENTION! Si vous ne parvenez pas à suivre les étapes ci-dessous, veuillez vous présenter au CAT qui pourra retirer des deuxièmes facteurs inutilisables (exemple : vous avez changé de numéro de téléphone ou de cellulaire).

1. Ouvrez une session Omnivox, puis en bas, à gauche, cliquez sur « Validation en 2 étapes » :

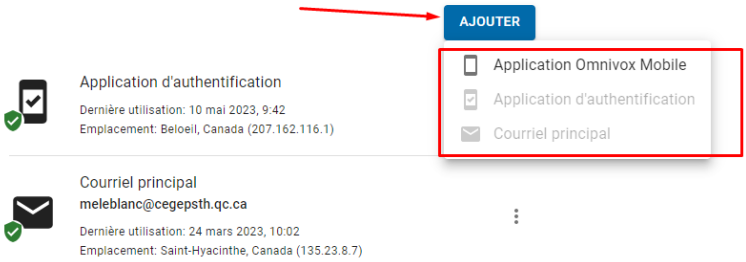


2. À la droite du facteur que vous désirez modifier ou supprimer, cliquez sur les 3 points, puis sélectionnez l'option appropriée :

3. Pour ajouter un facteur supplémentaire, il s'agit de cliquer sur « Ajouter », puis sélectionnez le facteur que vous désirez ajouter:

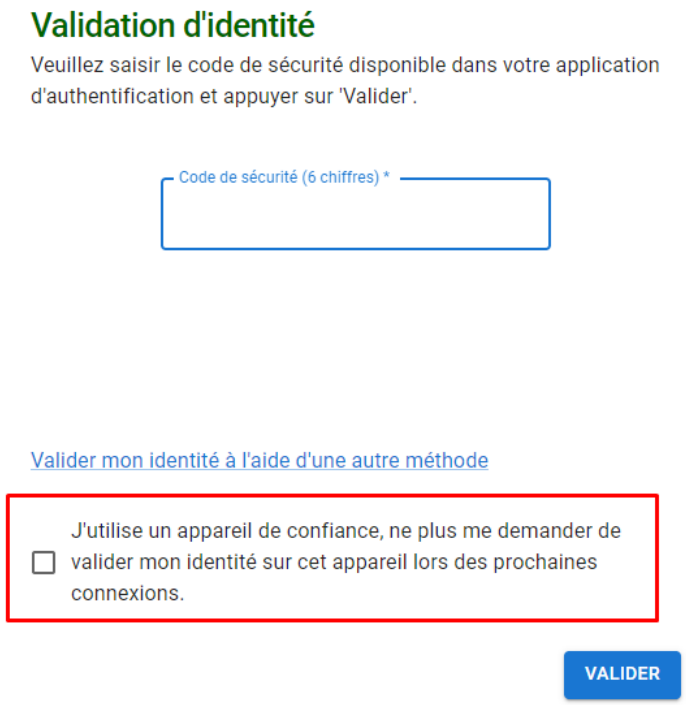
Validation en 2 étapes

Voici la liste des méthodes de validation de l'identité en 2 étapes associées à votre compte. Une deuxième étape après l'entrée du mot de passe permet de vérifier que c'est bien vous qui vous connectez à votre compte.



Appareils de confiance

Lorsque vous vous connectez à Omnivox ou Clara d'un *poste de confiance* (exemple : votre portable du Cégep), il est possible de cocher la case ci-dessous pour ne plus que soit demandé le 2ème facteur sur l'appareil en question pour 90 jours :



Dans Omnivox, dans le menu « Appareils de confiance », vous pourrez constater l'ajout de l'appareil en question, et même le retirer si c'est votre souhait :