

# Activation de l'authentification multifacteur pour Omnivox

## Qu'est-ce que l'authentification multifacteur (MFA) ?

L'authentification multifacteur est un mécanisme dans lequel l'utilisateur est invité pendant le processus de connexion à suivre une forme d'identification supplémentaire, consistant par exemple à entrer un code sur son téléphone portable ou à scanner son empreinte digitale.

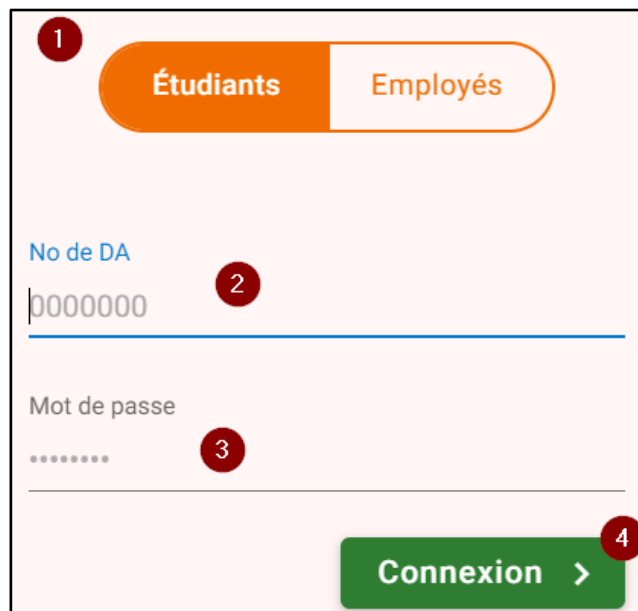
L'utilisation d'un mot de passe uniquement ne protège pas complètement des attaques. Si le mot de passe est faible ou s'il a été exposé ailleurs, est-ce vraiment l'utilisateur qui se connecte avec le nom d'utilisateur et le mot de passe, ou s'agit-il d'un attaquant ?

Avec une deuxième forme d'authentification, la sécurité est accrue, car ce facteur supplémentaire n'est pas un élément facile à obtenir ou à dupliquer par un attaquant. L'authentification multifacteur est nommée validation en deux étapes dans Omnivox et Clara.

## Comment activer l'authentification multifacteur (MFA)?

Pour activer l'authentification multifacteur, vous aurez besoin d'un téléphone mobile ou d'une tablette avec l'application « **Microsoft Authenticator** ». Voici la configuration recommandée par la DSTI :

1. Ouvrez la page Omnivox du Cégep Limoilou sur votre navigateur et choisissez votre catégorie :

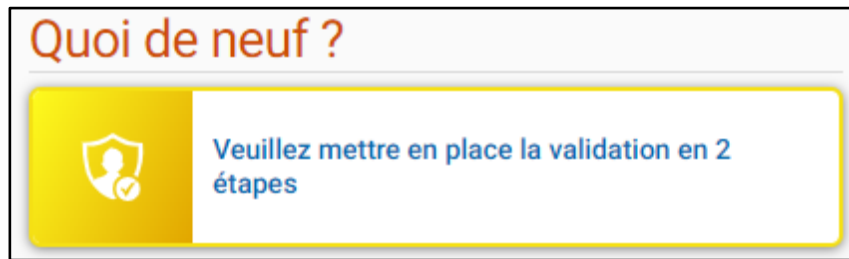


The screenshot shows the login interface of Omnivox. At the top, there are two tabs: 'Étudiants' (highlighted in orange) and 'Employés'. Below the tabs, there is a field for 'No de DA' (DA number) with the value '0000000'. Below that is a password field labeled 'Mot de passe' with masked characters. At the bottom right, there is a green button labeled 'Connexion >'. Red numbered circles (1, 2, 3, 4) are placed over the tabs, the DA number field, the password field, and the 'Connexion' button respectively.

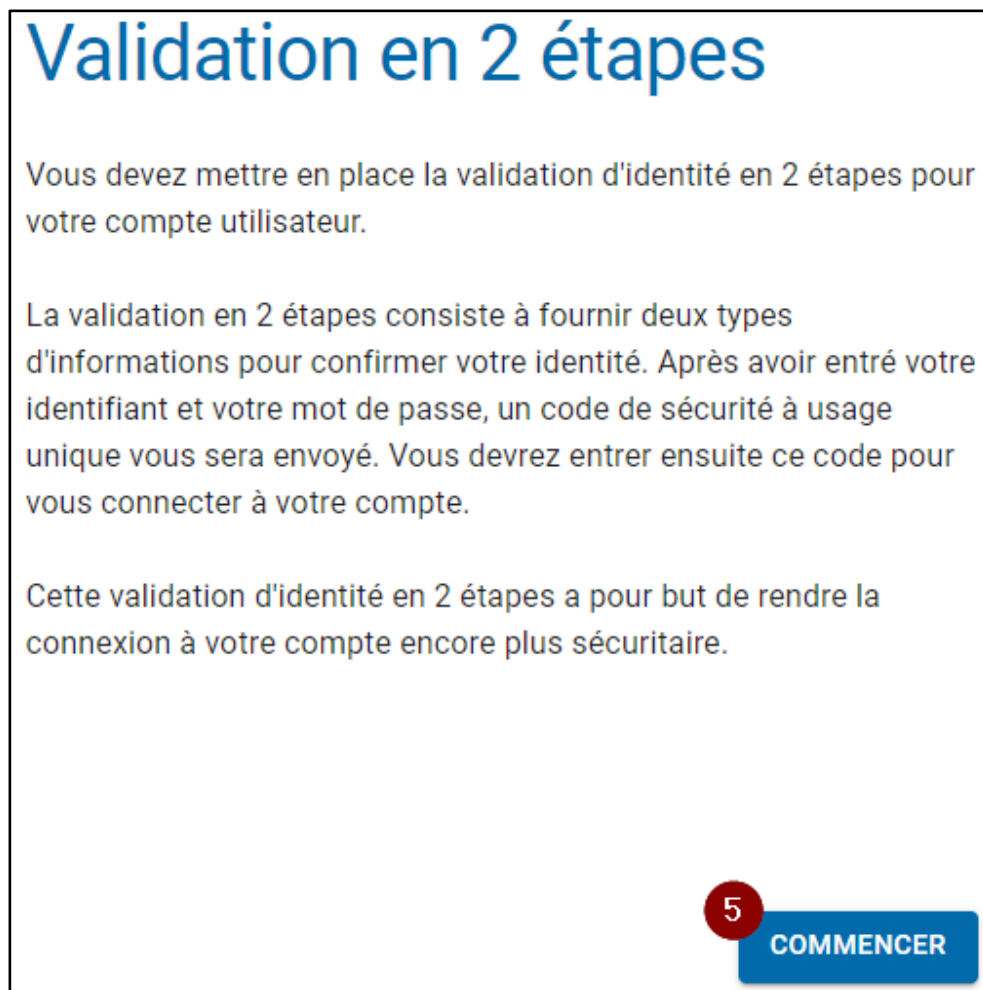
2. Indiquez votre numéro de DA<sup>1</sup>
3. Écrivez votre mot de passe associé à votre compte Omnivox
4. Cliquez sur le bouton « **Connexion** »

<sup>1</sup> Les employés doivent inscrire leur numéro d'employé fourni par les Ressources humaines à leur arrivée.

Si le MFA n'est pas encore rendu obligatoire, vous aurez une invitation à mettre en place la validation en deux étapes dans un quoi de neuf :



Dans le cas où, le MFA est rendu obligatoire vous aurez une fenêtre vous indiquant de mettre en place la validation en deux étapes dès votre entrée sur Omnivox :

A window titled "Validation en 2 étapes" in large blue font. The text inside explains that the user must set up two-step identity validation for their account. It details that this involves providing two types of information: a username and password, followed by a unique security code sent to the user. The purpose is to make the connection more secure. At the bottom right, there is a blue button with a red circle containing the number "5" and the word "COMMENCER" in white capital letters.

5. Cliquez sur le bouton « **Commencer** »<sup>2</sup>

<sup>2</sup> Sur la même page, vous pourriez avoir un texte en gris à gauche indiquant « **Remettre à plus tard** ». Si vous cliquez dessus, cela repoussera l'échéance de mise en place de l'authentification multifacteur.

6. Lisez les instructions d'ajout d'une application d'authentification avant de procéder et rendez-vous à l'étape 7 de cette procédure avant de cliquer sur le bouton « **Suivant** »

## Ajout d'une application d'authentification

6

1. Si nous ne possédons 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](#)

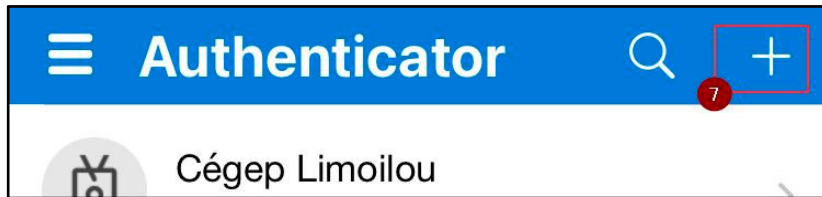
[Mettre en place une autre méthode de validation d'identité](#)

9

**SUIVANT**

Si vous ne possédez ni cellulaire ni tablette, cliquez sur « **Mettre en place une autre méthode de validation d'identité** » et allez directement à la section Comment activer le MFA sans cellulaire?

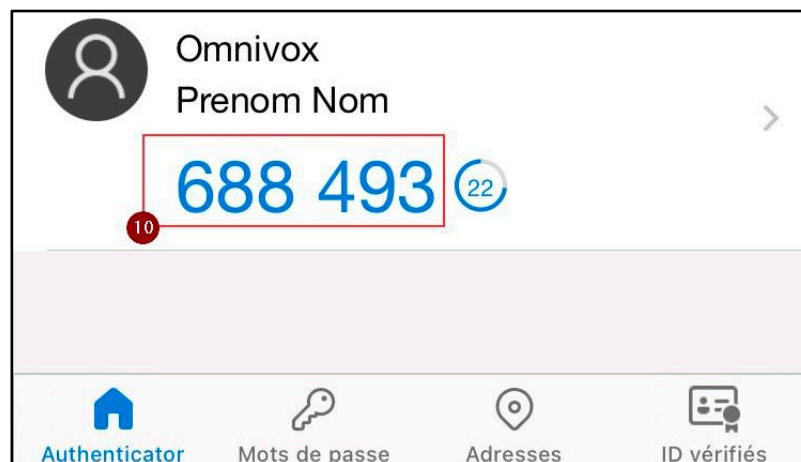
7. Ouvrez « **Microsoft Authenticator** » sur votre cellulaire ou tablette et cliquez sur le « + » en haut à droite



8. Sélectionnez ensuite le type de compte « **Autre (Google, Facebook, etc.)** »



9. Une fois le compte ajouté à « **Microsoft Authenticator** », veuillez cliquer sur le bouton « **Suivant** » dans la fenêtre de votre navigateur.
10. Vous avez un code qui est associé à votre compte Omnivox dans « **Microsoft Authenticator** »



- Inscrivez le code présent dans « **Microsoft Authenticator** » dans la page 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

- Cliquez sur le bouton « **Valider** »
- Inscrivez votre courriel du Cégep Limoilou afin d'avoir deux méthodes d'authentification multifacteur

**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

SUIVANT

- Cliquez sur le bouton « **Suivant** »

15. Vous allez recevoir un courriel à l'adresse indiquée avec un code de sécurité




16. Saisissez le code précédent dans la fenêtre Omnivox du navigateur



17. Cliquez sur le bouton « Valider »

18. L'activation du MFA est terminée, vous pouvez cliquer sur le bouton « **Continuer** »

## Activation terminée



Validation en 2 étapes  
activée

Dès votre prochaine connexion, vous devrez confirmer votre identité à l'aide d'une des méthodes associées à votre compte.

La gestion de ces méthodes s'effectue à partir du service "Validation en 2 étapes" disponible dans le menu des services.

18

**CONTINUER**

## Comment activer le MFA sans cellulaire?

Si vous ne possédez pas de cellulaire ou tablette, vous pouvez à partir de l'étape 6 ci-dessus choisir une autre méthode d'activation en cliquant sur « **Mettre en place une autre méthode de validation d'identité** ».

7. Choisissez l'option « **Courriel principal** »

**Méthodes disponibles**

Voici la liste des méthodes de validation de l'identité en 2 étapes que vous pouvez mettre en place pour votre compte utilisateur.

- Application d'authentification
- Courriel principal**
- Courriel secondaire

8. Inscrivez votre courriel du Cégep Limoilou comme méthode de validation

**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 \*

Ce champ est requis.

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

**SUIVANT**

9. Cliquez sur le bouton « **Suivant** »



10. Vous allez recevoir un courriel à l'adresse indiquée avec un code de sécurité




11. Saisissez le code précédent dans la fenêtre Omnivox du navigateur



12. Cliquez sur le bouton « Valider »

13. Répétez les étapes 8 à 12 avec une autre adresse de courriel pour avoir deux méthodes MFA
14. L'activation du MFA est terminée, vous pouvez cliquer sur le bouton « Continuer »

## Activation terminée



### Validation en 2 étapes activée

Dès votre prochaine connexion, vous devrez confirmer votre identité à l'aide d'une des méthodes associées à votre compte.

La gestion de ces méthodes s'effectue à partir du service "Validation en 2 étapes" disponible dans le menu des services.

14  
CONTINUER

Direction des systèmes et des technologies de l'information – DSTI  
Centre de Services : DSTI-SOSInformatique <http://centredeservices.cegeplimoilou.ca>  
Courriel : [sosinfo@cegeplimoilou.ca](mailto:sosinfo@cegeplimoilou.ca)  
Téléphone : 418 647-6600, 6533 (Québec et Charlesbourg)  
Avant d'imprimer, pensez à l'environnement