CÉGEP DU VIEUX MONTRÉAL

Direction des Technologies de l'Information

Guide utilisateur de l'authentification multifactorielle

Version du 7 novembre 2022, DB, MH

Contexte

L'authentification multifactorielle peut se déclencher lorsque vous vous connectez aux applications suivantes :

- Courriel Outlook du Collège
- Suite Office 365
- Teams
- OneDrive
- Moodle

L'authentification multifactorielle ne concerne pas la connexion au réseau du Collège ni l'accès au VPN pour le moment.

Fréquence

Personnel administratif : Au moins une fois par jour, pour chaque appareil, le système d'authentification multifactorielle vous demandera de vous authentifier.

Pour les professeurs : Lorsque vous êtes **à l'extérieur du Collège**, le système d'authentification multifactorielle vous demandera de vous authentifier au moins une fois par jour, et ce pour chaque appareil.

Lorsque vous êtes connectés à notre réseau sans fil ou à notre réseau filaire dans les différents bâtiments du Collège, l'authentification multifactorielle sera désactivée. Il y a cependant une exception. Que vous soyez à l'interne ou à l'externe, la connexion à **Moodle** nécessitera l'authentification multifactorielle à chaque connexion.

Table des matières

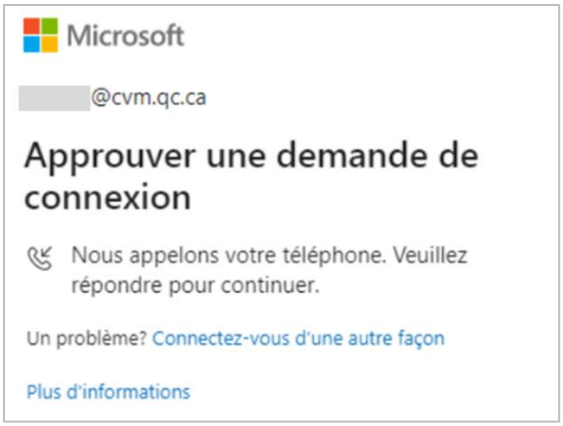
Authentification par appel téléphonique

Si, après vous être identifié, le système vous demande d'approuver une demande de connexion, vous recevrez un appel téléphonique vous demandant d'appuyer sur la touche dièse [#].

Note 1 : Il est possible que vous ayez besoin d'appuyer à deux reprises sur la touche dièse [#]. Assurez-vous, avant de raccrocher, que le système vous confirme au téléphone l'approbation de la demande de connexion.

Note 2 : Soyez patient, le système peut prendre jusqu'à une minute avant de vous appeler.

Note 3 : En cas de problème, vous devrez peut-être vous identifier de nouveau.

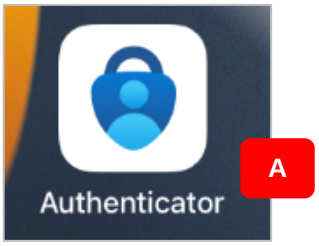


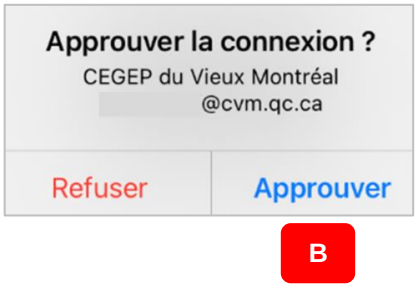
Authentification par l'application « Microsoft Authenticator »

Si, après vous être identifié, le système vous demande d'approuver une demande de connexion, vous recevrez une notification sur les appareils mobiles où vous avez installé et paramétré l'application « Microsoft Authenticator » pour le compte du CVM.

Sur votre appareil mobile :

A. Au besoin, démarrez l'application « Microsoft Authenticator »
B. Cliquez sur **« Approuver »**
C. Au besoin, authentifiez-vous sur votre appareil mobile (code, empreinte, reconnaissance faciale)





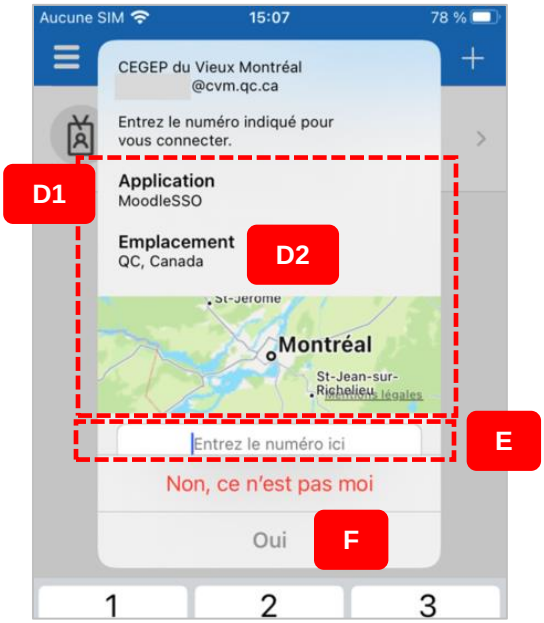
D. Vérifiez les points suivants :
   1. Vérifiez si l'application affichée est bien celle qui a déclenché l'authentification multifactorielle.
   2. Vérifiez si l'emplacement indiqué est bien celui où vous êtes actuellement.

E. Entrez le code qui apparait sur la demande de connexion (voir figure ci-dessus).

F. Cliquez sur **« Oui »** pour approuver la demande de connexion

G. Au besoin, authentifiez-vous sur votre appareil mobile (code, empreinte, reconnaissance faciale)

H. En cas de problème, vous devrez peut-être vous identifier de nouveau



Changer de méthode d'authentification lors de la connexion

Vous pouvez changer de méthode d'authentification lors de la connexion si vous avez paramétré plusieurs méthodes.

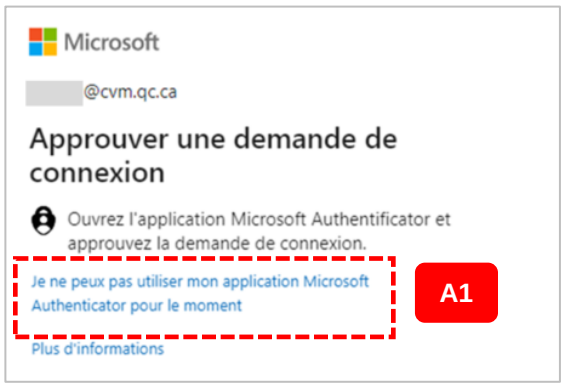
A. Ainsi, si vous devez vous authentifier et que votre méthode par défaut n'est pas disponible, vous pouvez :

1. Cliquer sur le lien **« Je ne peux pas utiliser mon application Microsoft Authenticator pour le moment »** si votre méthode par défaut est l'application « Microsoft Authenticator »

OU

2. Cliquer sur le lien **« Connectez-vous d'une autre façon »** si votre méthode par défaut est un appel téléphonique

B. Sélectionnez une autre méthode de connexion que vous avez paramétrée



OU