Université de Montréal | StudiUM

ACCÈS HORS CAMPUS

À partir du 28 février 2022*, l'accès à Studium hors campus s'ajoute à la liste des plateformes déjà soumises à l'authentification forte.

Ainsi, tous les membres de la communauté universitaire bénéficiant de l'authentification forte qui accèderont à StudiUM pour un cours, un examen ou une formation RH, à partir d'un appareil qui n'utilise pas le réseau de l'UdeM, sont concernés.

L'authentification forte A2F, c'est une manière simple et sûre de protéger l'accès aux ressources informatiques UdeM par l'ajout d'une 2e validation de l'identité d'une personne, en plus du code d'accès et mot de passe UNIP.

AVIS – Condition d'utilisation : Dès le 24 février 2022, tout utilisateur de la plateforme StudiUM devra confirmer avoir pris connaissance de cette règle de sécurité en cochant la fenêtre contextuelle (« pop-up ») une seule fois, avant de pouvoir accéder à StudiUM.

L'authentification par code d'accès/UNIP demeure requise pour accéder à StudiUM à partir du réseau UdeM.

*selon la situation pandémique

Liens utiles A2F

FAQ A2F ou code QR ->

Procédures de configuration

A2f.umontreal.ca

Libre-service d'auto-exclusion temporaire A2F

Vidéothèque A2F

Présentation de l'authentification forte A2F (0:48)
Pourquoi l'authentification forte A2F à l'UdeM? (0:54)
Quelles sont les méthodes de 2e facteur autorisées à l'UdeM? (1:20)
J'ai besoin d'aide (1:20)
Microsoft Authenticator sur un appareil mobile ANDROID (2 :47)
Microsoft Authenticator sur un appareil mobile iOS (2 :31)
Oracle Authenticator sur un poste Windows (5 :02)
KeePassXC sur un poste MAC

Technologies de l'information
Université de Montréal et du monde.

Dépannage et soutien

Étudiant(e) : Bureau du registraire
- Téléphone au 514-343-7212
- Bureau du registraire

CDS des TI (UNIP/A2F): L-V 16h30 à 23h et S-D 8h à 16h
- Téléphone au 514-343-7288
- clavardage.ti.umontreal.ca

Membre du personnel : Centre de services TI: L-V 8h à 23h - S-D 8h à 16h

- Téléphone au 514-343-7288
- Clavardage à l'adresse : clavardage.ti.umontreal.ca
- Formulaire d'aide

A
S
T
U
C
E
S

★ Vous n'avez pas accès à un téléphone cellulaire? Installez *Oracle Authenticator* sur votre poste de travail Windows ou *KeePassXC* sur votre poste de travail MAC.
★ Évitez les demandes répétitives A2F en conservant les fichiers témoins (« cookies ») de votre fureteur.
★ « ***Clé de sécurité*** » est une méthode **non supportée.**
★ Le 2e facteur d'authentification peut être modifié en tout temps à l'adresse a2f.umontreal.ca. Inscrivez plus d'un 2e facteur à votre compte; si vous oubliez votre premier choix, vous pourrez utiliser votre 2e choix de facteur d'authentification.
★ Vous utilisez Synchro? Choisissez un fureteur pour accéder à Synchro en supprimant les fichiers témoins ("cookies") et un second fureteur pour les autres accès, en conservant les fichiers témoins.
★ Si vous utilisez un ordinateur MAC, accédez au VPN par un fureteur (vpn.umontreal.ca/campus) pour éviter une bouche d'authentification causée par un protocole de sécurité natif sur ces postes.
★ Si vous devez modifier votre mot passe SIM et vous êtes en télétravail, assurez-vous de suivre les procédures indiquées dans la notification courriel d'expiration pour éviter les délais de synchronisation.
★ Gagnez du temps en consultant les capsules vidéo d'installation.
★ Vous avez oublié votre 2e facteur d'authentification ? Utilisez le Libre-service d'auto-exclusion temporaire A2F disponible de la page d'authentification UdeM. Assurez-vous d'avoir inscrit vos questions de vérification pour en profiter.

La sécurité des comptes UdeM, c’est une responsabilité conjointe!

Technologies de l'information

Université de Montréal et du monde.