Université de Montréal | Technologies de l'information

GUIDE D'ACCOMPAGNEMENT

Introduction

Maintenant implantée à l'UdeM, l'authentification forte à deux facteurs (A2F) ajoute un niveau de sécurité additionnel aux comptes personnels uniques des membres de la communauté universitaire. Il en va de même pour les comptes de gestion à hauts privilèges, qu'ils soient utilisés par les membres des TI ou par des employés d'autres secteurs. Un compte devrait avoir un utilisateur unique. La transition d'un compte « ca-unité » par unité vers un compte « admu_code d'accès » par utilisateur permettra d'assurer que le compte est utilisé par la bonne personne pour l'octroi des permissions d'accès aux ressources sécurisés de l'UdeM, et ainsi assurer que le compte ne pourra être dupliqué ou partagé.

Comment se préparer à la sécurisation du compte « ca-unité »

Afin de s'assurer de répondre à vos besoins de gestion des accès, il est nécessaire de prendre quelques instants pour faire une revue des utilisations et des personnes pouvant effectuer des opérations avec le compte de gestion à hauts privilèges de votre unité/département. À cette fin, nous vous invitons à compléter le formulaire Excel_Analyse de l'utilisation du *compte ca-unité*.

***Notez qu'il n'y a pas de contrainte quant au nombre de comptes « admu_code d'accès » requis par unité. De même, deux personnes peuvent avoir les mêmes privilèges de gestion des accès, mais avec un compte qui leur est unique.

Création compte admu_code d'accès

Suite à l'analyse et la mise à jour de vos besoins, la transition pourra débuter. Les comptes « admu_code d'accès », comptes de services, si requis, seront créés par l'équipe du projet A2F qui octroiera les bonnes permissions de gestion pour vos membres.

Sécurisation du compte

Dès la réception des nouveaux comptes « admu_code d'accès « pour votre unité, chaque propriétaire doit modifier le mot de passe temporaire pour un mot de passe permanent puis inscrire une méthode, ou deux, de 2e facteur d'authentification pour le compte à l'adresse a2f.umontreal.ca. Pour plus d'informations, consultez la FAQ de l'authentification à deux facteurs (A2F)

Note importante:

Pour des raisons de sécurité, le compte « admu_code d'accès » n'est pas autorisé à utiliser notre réseau privé virtuel (VPN) vers les ressources sécurisées de l'UdeM. L'accès distant aux systèmes sécurisés de l'UdeM par connexion privée virtuelle (VPN) devra s'effectuer **par le compte personnel d'un utilisateur (code d'accès-UNIP).** Lorsque le tunnel virtuel est autorisé, l'utilisateur doit s'authentifier sur le système de gestion ou serveur visé avec son compte « admu_code d'accès ».

Période de test et de validation des accès

Lorsque le compte est sécurisé, la période de test et de validation débute. Cette étape est cruciale pour certifier que les accès demandés, les méthodes d'utilisation ainsi que l'automatisation de scripts sont fonctionnels. Pendant cette période, le compte « ca-unité » sera inactivé, ou réactivé, selon les résultats de vos tests.

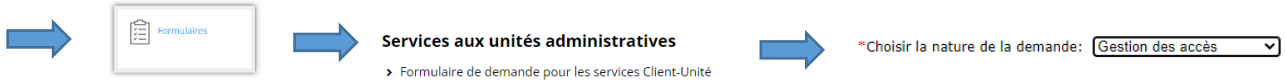
Nous vous recommandons de créer un groupe AD puis y ajouter les comptes « admu_code d'accès » pour la gestion des stratégies de groupe, automatisation de tâches ou scripts (GPO). Assurez-vous également d'avoir remplacé l'inscription du compte « ca-unité » partout où il est utilisé, soit par le compte de service créé à cet effet, ou par le compte « admu_code d'accès ».

Une période de tests et validation raisonnable sera déterminée entre la personne-ressource de l'unité et l'équipe du projet.

Ensuite, sur entente conjointe, le compte « ca-unité » de votre secteur sera **détruit.** Les comptes « admu_code d'accès » de gestion à hauts privilèges devront être utilisés pour les opérations de gestion.

Procédure pour demander ou modifier un compte à hauts privilèges admu_code d'accès

Pour demander la création d'un compte « admu_code d'accès » ou pour modifier les permissions d'accès d'un compte « admu_code d'accès » existant, vous devez compléter une demande d'aide par le formulaire d'aide aux unités qui se trouve sur le site web des TI. Assurez-vous de sélectionner dans le menu déroulant l'option *Gestion des accès*.



Pour accélérer le traitement de votre requête assurez-vous d'indiquer les informations suivantes : Nom, prénom et code d'accès de l'utilisateur du compte « admu_code d'accès » et spécifiez les besoins de gestion des permissions requises pour ce compte.

Procédure pour modifier le mot de passe d'un compte de gestion à hauts privilèges admu_code d'accès

De manière autonome, vous pouvez modifier le mot d'un compte de gestion admu_code d'accès de deux façons:

- Ouvrir une session Windows et y modifier le mot de passe
- Par l'application Changer
  MDP : https://identification.umontreal.ca/cas/ChangerMDP.aspxPar un responsable technique ou du CDS via l'application Indigo 2.0

Sinon, communiquez avec un responsable technique ayant accès à l'application *Indigo 2.0*, ou avec le Centre de services des TI.

Pour plus de détails sur la sécurisation des comptes à hauts privilèges ca-unité, consultez la page d'information disponible sur la FAQ L'authentification à nos services.

Les TI vous remercient de votre collaboration à la sécurisation des comptes.