FAQ - Mobile Application Management (MAM)

Table des matières

1. **Qu'est-ce que le Mobile Application Management (MAM) ?**

La politique MAM est l'une des mesures de sécurité retenue par Santé Québec à la demande du Centre opérationnel de cyberdéfense afin de s'assurer de la protection des données Microsoft 365 (M365) de l'organisation accédées par des appareils mobiles. Il permet de séparer les données professionnelles des données personnelles, tout en assurant la protection des informations sensibles de l'entreprise.

2. **Qui est touché par l'application de cette mesure ?**

Tout appareil mobile iOS et Android qui a un système d'exploitation supporté par le manufacturier, et sur lequel l'utilisateur tente d'accéder aux données de l'organisation (M365).

3. **Quel sont les principaux changements lors de l'application de cette politique MAM sur mon appareil mobile ?**

- Un code secret (NIP) d'au moins six caractères sera requis pour accéder aux applications M365 sur mobile. Celui-ci est différent du code de déverrouillage de votre appareil. L'authentification biométrique peut être utilisée sur le NIP à 6 chiffres si elle a été activée.
- L'accès à une application gérée sera verrouillé après 5 tentatives de connexions infructueuses.
- Les applications M365 seront isolées pour empêcher l'échange d'informations avec d'autres applications de l'appareil et les données de l'organisation seront chiffrées.
- Le téléchargement de fichiers provenant des applications M365 sur l'appareil mobile sera restreint.
- Les fonctions de copier-coller et de capture d'écran seront désactivées pour les informations provenant des applications M365.
- L'utilisation des applications Courrier (Android) et Mail (iOS) pour les courriels et l'agenda professionnels ne sera plus possible. L'application mobile Outlook devra obligatoirement être utilisée.

4. **Comment ouvrir des liens internet à partir d'une application gérée sur un appareil personnel (BYOD) (Outlook, Teams) ?**

Pour ouvrir les liens internet au sein des applications M365 sur les appareils mobiles, vous devez avoir installé le navigateur Microsoft Edge à partir de vos espaces de téléchargement habituels (App Store pour IOS et Play store pour Android). Microsoft Edge est le seul navigateur avec lequel vous serez capable d'ouvrir un lien internet depuis votre application mobile M365.

5. **Que se passe-t-il si l'utilisateur refuse l'installation de Portail d'entreprise Microsoft inTune sur son cellulaire ?**

Si l'utilisateur refuse l'installation, il ne sera plus en mesure d'accéder aux données de l'organisation (M365) via une application gérée. Donc, il n'aura plus accès aux courriels professionnels ou à l'application Teams.

6. **Quelle est la différence entre le MAM et le MDM (Mobile Device Management) ?**

- **MDM** : Gère l'ensemble de l'appareil (téléphone ou tablette), y compris les paramètres système, les applications et les données.
- **MAM** : Se concentre uniquement sur la gestion des applications et des données professionnelles, sans avoir à contrôler l'appareil entier. Cela permet une meilleure flexibilité, notamment pour les environnements BYOD (Bring Your Own Device).

7. **Pourquoi LE CIUSSS utilise-t-elle le MAM ?**

Le CIUSSS utilise le MAM pour :

- Protéger les données professionnelles contre les fuites ou les accès non autorisés.
- Vous permettre d'utiliser vos applications métiers en toute sécurité, où que vous soyez.
- Respecter votre vie privée en ne gérant que les applications professionnelles, sans toucher à vos données personnelles.

8. **Le MAM est-il adapté aux environnements BYOD ?**

Oui, le MAM est idéal pour les environnements BYOD. Il permet de gérer uniquement les applications et données professionnelles sans interférer avec les données personnelles de l'utilisateur, respectant ainsi leur vie privée.

9. **Quelles applications peuvent être gérées via le MAM ?**

Le MAM peut gérer :

- Les applications métiers développées en interne.
- Les applications publiques (comme Microsoft Teams, Salesforce, etc.).

10. **Comment les applications sont-elles déployées avec le MAM ?**

Les applications peuvent être déployées via :

- Un catalogue d'applications d'entreprise (Enterprise App Store).

11. Le MAM peut-il empêcher la copie ou le partage de données sensibles ?

Oui, le MAM inclut des fonctionnalités de prévention des pertes de données (DLP) qui empêchent :

- La copie de données vers des applications non autorisées.
- Le partage de fichiers via des canaux non sécurisés.
- L'accès aux données professionnelles en dehors de l'environnement sécurisé.
- Il ne sera plus possible de télécharger des fichiers sur l'appareil mobile depuis une application contrôlée par le MAM.
- Il ne sera plus possible de copier ou transférer de l'information à partir des applications gérées vers des applications personnelles.
- L'utilisation des applications Courrier (Android) et Mail (iOS) pour les courriels et l'agenda professionnels ne sera plus possible. L'application mobile Outlook devra obligatoirement être utilisée.
- Les fonctions de copier-coller et de capture d'écran seront désactivées pour les informations provenant des applications M365.

12. Le MAM fonctionne-t-il sur tous les appareils et systèmes d'exploitation ?

Le MAM est compatible avec les principaux systèmes d'exploitation mobiles, notamment :

- L'appareil mobile devra être équipé de la version minimale
  - Android 12 pour les appareils Android
  - iOS 15 pour les appareils iOS (Apple)

13. Comment le MAM assure-t-il la sécurité des données ?

Le MAM utilise plusieurs mécanismes de sécurité :

- Obligation d'utiliser un NIP à 6 chiffres pour l'accès d'applications gérées qui permettent d'accéder aux données de l'organisation.
- L'accès à une application gérée sera verrouillé après 5 tentatives de connexions infructueuses.
- Chiffrement des données en transit et au repos.
- Authentification multi-facteurs (MFA).
- Effacement à distance des données professionnelles en cas de perte ou de vol.

14. Il est mentionné qu'après 5 tentatives de connexion infructueuses, l'accès aux M365 sera verrouillé. Qui doit se charger de déverrouiller l'accès ?

Le processus d'authentification sera désactivé pour 1 minute. Réessayer de nouveau après 1 minute. Si vous n'arrivez toujours pas à vous connecter après avoir réessayer, contacter le centre de service informatique via Octopus ou le 5656.

15. Si j'ai oublié mon NIP (PIN) à 6 chiffres me permettant d'accéder aux applications gérées. Que dois-je faire ?

Si vous avez oublié votre code PIN ou devez le changer, vous pouvez le faire directement à partir de l'application. Cliquez sur "Vous avez oublié votre code PIN ?" et suivez les instructions à l'écran. Une procédure détaillée est également disponible dans la boîte à outils.

16. Que se passe-t-il si un employé quitte l'entreprise ?

L'administrateur peut révoquer l'accès aux applications et données professionnelles en quelques clics, sans affecter les données personnelles de l'utilisateur et supprimer l'application si nécessaire. L'employé peut supprimer l'application Portail d'entreprise Microsoft inTune si celle-ci est installée sur un appareil personnel.

17. Le MAM peut-il être utilisé avec d'autres solutions de sécurité ?

Oui, le MAM peut être intégré à d'autres solutions comme :

- Le MDM pour une gestion complète des appareils : INTUNE
- Les solutions de sécurité des terminaux (Endpoint Security).
- Les plateformes de gestion unifiée des terminaux (UEM).

18. Le MAM va-t-il surveiller ou contrôler mon appareil personnel ?

Non, le MAM ne surveille pas votre appareil personnel. Il se concentre uniquement sur les applications professionnelles installées sur votre téléphone ou tablette.

- Vos données personnelles (photos, messages, etc.) ne sont pas accessibles ou gérées par l'entreprise.
- L'application ne permet pas de surveiller
    - Les déplacements GPS
    - La navigation internet
    - De contrôler les applications ou données personnelles

19. Que se passe-t-il si je perds mon appareil ?

Si vous perdez votre appareil, contactez le plus rapidement possible le centre de service informatique via Octopus ou le 5656. Afin de :

- Bloquer l'accès aux applications et données professionnelles.
- Effacer à distance les données professionnelles sans affecter vos données personnelles.

20. Dois-je être connecté à Internet pour utiliser les applications gérées par le MAM ?

La plupart des applications fonctionnent hors ligne une fois installées. Cependant, une connexion Internet est nécessaire pour :

- Synchroniser les données.
- Recevoir des mises à jour.
- Accéder à certaines fonctionnalités en temps réel.

21. Comment mettre à jour les applications professionnelles ?

Les mises à jour peuvent être gérées automatiquement par l'entreprise ou vous pouvez recevoir une notification pour les installer manuellement. Suivez les instructions fournies par le centre de service informatique.

22. Puis-je utiliser mes propres applications en plus des applications professionnelles sur mon propre appareil (BYOD)?

Oui, vous pouvez continuer à utiliser vos applications personnelles comme d'habitude. Le MAM ne gère que les applications professionnelles et ne restreint pas l'utilisation de vos applications personnelles.

23. Pourquoi dois-je utiliser une authentification multi-facteurs (MFA) pour certaines applications ?

L'authentification multi-facteurs (par exemple, un code reçu par SMS ou une application d'authentification) ajoute une couche de sécurité supplémentaire pour protéger les données sensibles de l'entreprise.

24. Que faire si une application professionnelle ne fonctionne pas correctement ?

Si vous rencontrez des problèmes avec une application professionnelle :

1. Vérifiez votre connexion Internet.
2. Redémarrez l'application ou votre appareil.
3. Contactez le centre de service informatique via Octopus ou au 5656 pour obtenir de l'aide.

25. Le MAM affecte-t-il la batterie ou les performances de mon appareil ?

Le MAM est conçu pour avoir un impact minimal sur les performances de votre appareil. Si vous remarquez des problèmes, contactez le centre de service informatique pour vérifier la configuration.

26. J’ai lancé l’application Portail D’entreprise Microsoft Intune sur mon appareil numérique Android et je n’y suis connecté avec mon compte professionnel M365. Quel est l’impact ?

Malheureusement, Votre appareil s’est automatiquement embarqué dans la console de gestion MDM sous le type <Appareil personnel géré par l’entreprise>. Veuillez contacter la DRI afin que votre appareil soit retiré de la console de gestion MDM

Annexe 1 : Quelles données sont visibles par le CIUSSS

Ce que le CIUSSS peut toujours voir	Ce que le CIUSSS ne peut jamais voir

• Modèle d'appareil
• Fabricant de l'appareil
• Système d'exploitation et sa version
• Inventaire des applications et noms des applications
  ○ Sur les appareils personnels: uniquement la liste de vos applications gérées;
  ○ Sur les appareils appartenant à l'entreprise avec profil professionnel: uniquement l'inventaire des applications de votre profil professionnel
• Propriétaire de l'appareil
• Nom de l'appareil
• Numéro de série de l'appareil
• *International Mobile Equipment Identity* (IMEI)
• Localisation : **Appareil appartenant à l'entreprise** : votre organisation peut voir l'emplacement d'un appareil perdu.
	• Historique de la navigation sur le web
	• Courrier électronique et messages textuels
	• Contacts
	• Calendrier
	• Mots de passe
	• Photos dans l'appareil
	• Fichiers
	• Pour les appareils appartenant à une entreprise et présentant un profil professionnel, les applications et les données de votre profil personnel
	• Localisation : **Appareil personnel :** votre organisation ne peut pas voir l'emplacement d'un appareil personnel.