Modern Workplace et Sécurité Cloud

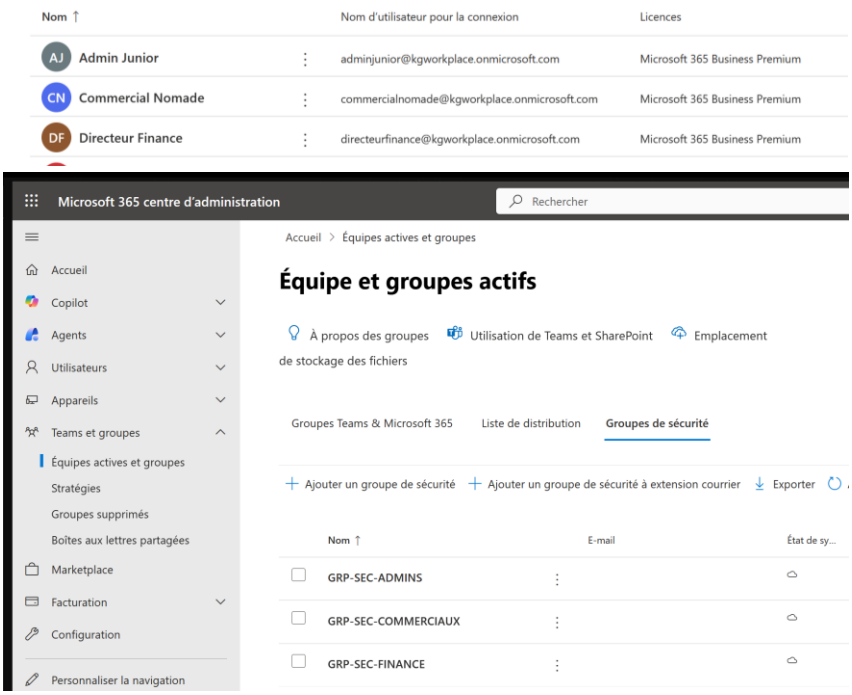
Introduction et Objectifs

L'objectif de ce lab est de mettre en place une infrastructure de gestion moderne des terminaux (Modern Endpoint Management) en utilisant la suite **Microsoft 365**. Ce projet se concentre sur la sécurisation des accès et des données via des politiques de conformité et l'accès conditionnel.

1. Gouvernance et Identités

La première phase a consisté à structurer l'annuaire **Microsoft Entra ID en** créant des groupes de sécurité adaptés aux besoins métiers de l'entreprise :

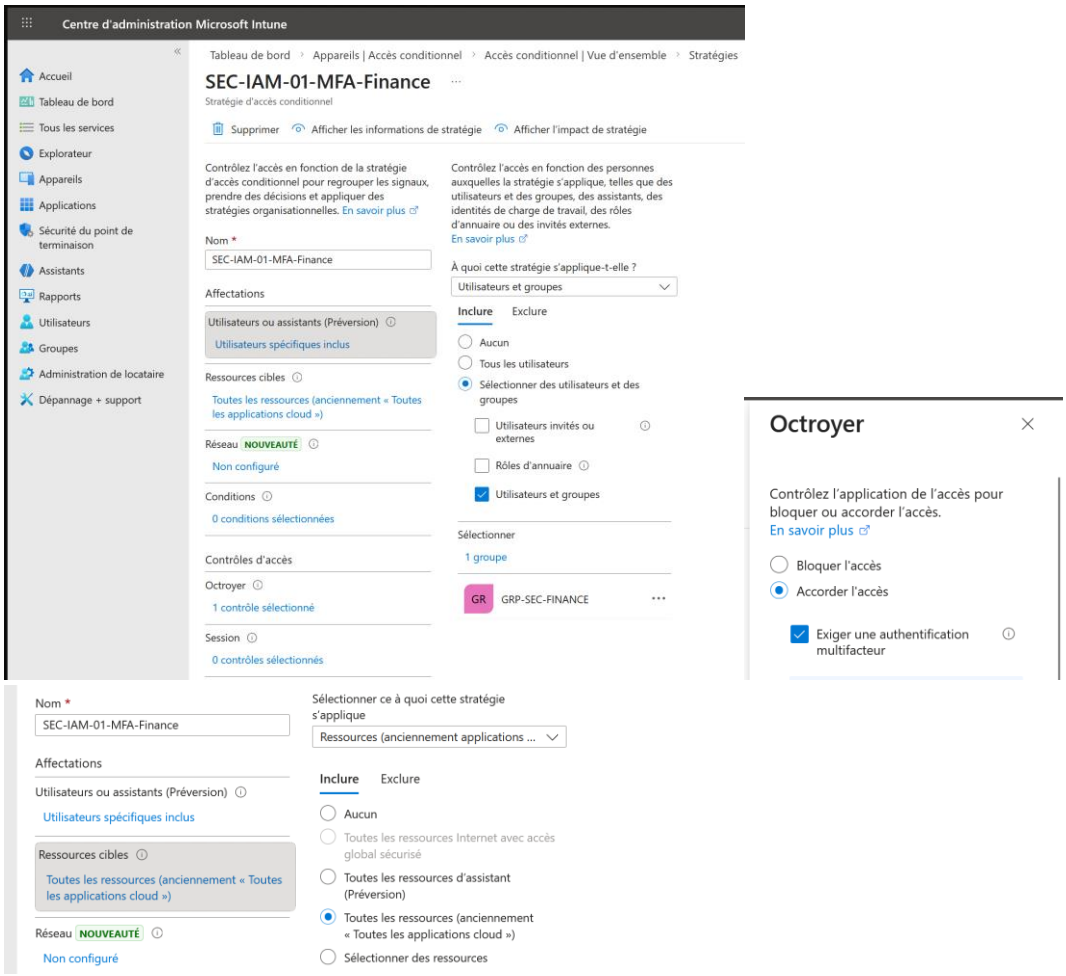
- **GRP-SEC-ADMINS** : Pour les comptes à hauts privilèges.
- **GRP-SEC-COMMERCIAUX** : Pour les profils nomades nécessitant une sécurité accrue.
- **GRP-SEC-FINANCE** : Pour les accès critiques aux données financières.



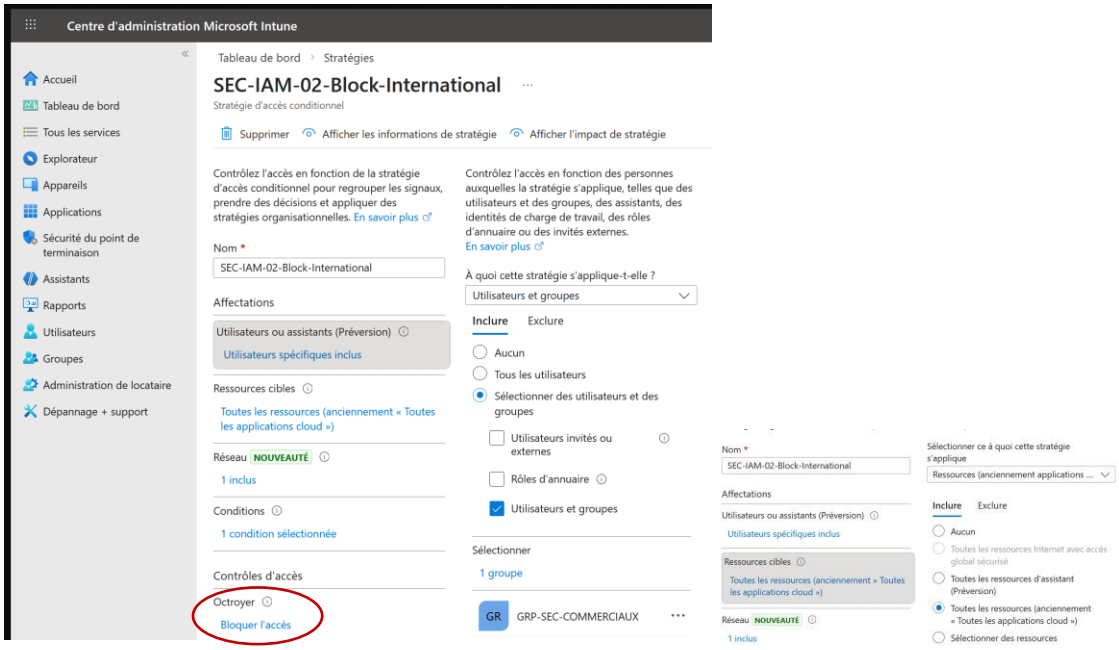
2. Stratégies d'Accès Conditionnel (Zero Trust)

Afin de protéger le tenant contre les accès non autorisés, plusieurs stratégies d'accès conditionnel ont été déployées :

MFA pour la Finance : Exigence d'une authentification multifacteur (MFA) pour le groupe Finance



Blocage International : Restriction des accès basée sur la géolocalisation

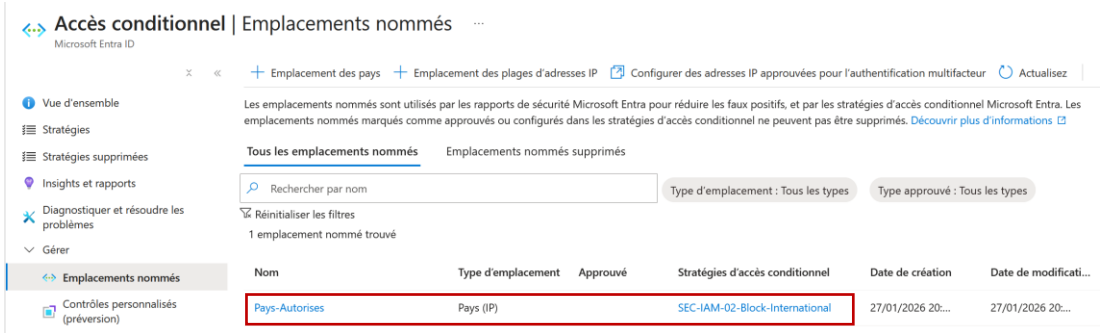


Cette configuration a pour but :

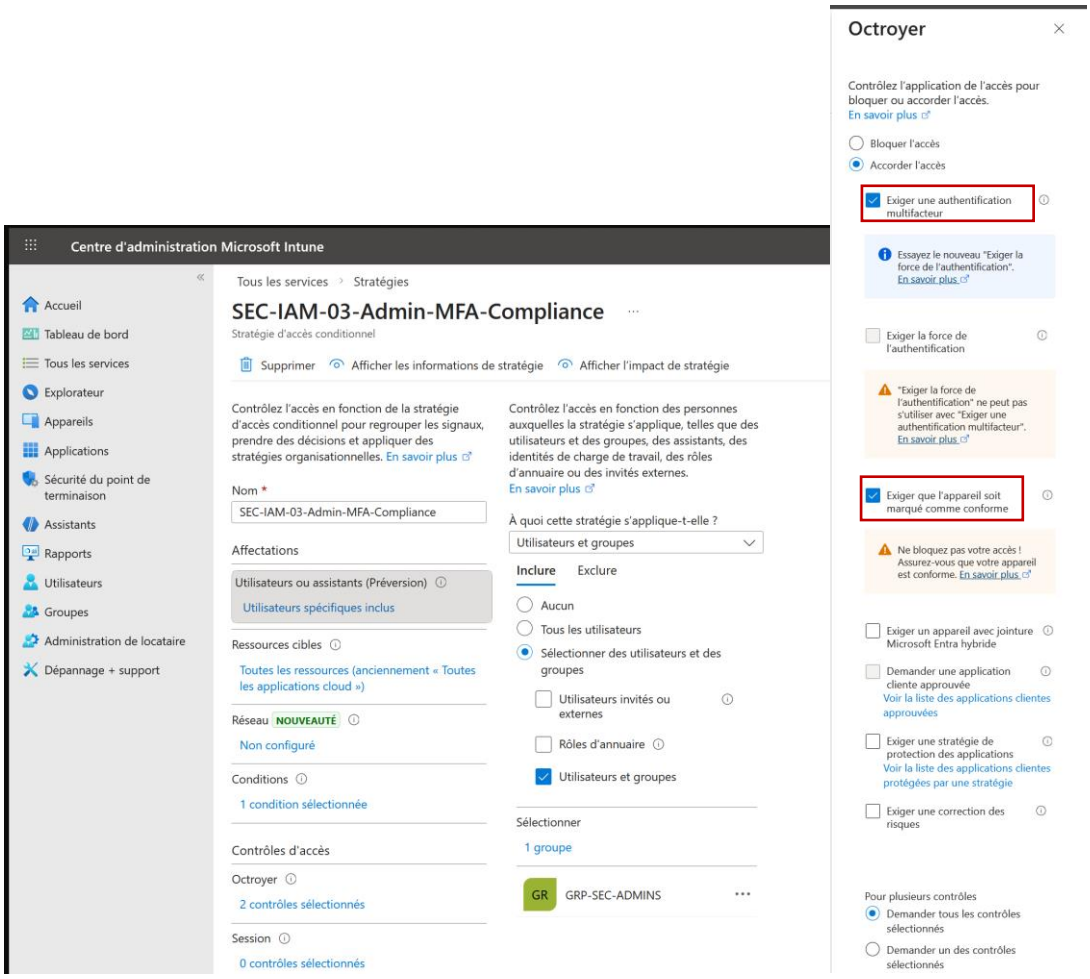
- **D'autoriser les connexions uniquement depuis les pays approuvés**,
- **De bloquer automatiquement les tentatives de connexion provenant de zones géographiques non autorisées**.

Cette approche permet de réduire significativement la surface d'attaque liée aux connexions internationales et s'inscrit dans une logique de sécurité **Zero Trust**, où la localisation constitue un signal de sécurité parmi d'autres dans la décision d'accès.

Ici, un emplacement de pays (France, Belgique, Suisse) a été configuré et associé à la stratégie



Conformité Admin : Obligation pour les administrateurs d'utiliser un appareil conforme et le MFA pour accéder aux ressources



Cette stratégie impose deux contrôles principaux pour l'accès aux ressources :

- **L'authentification multifacteur (MFA)** afin de renforcer la sécurité des comptes à privilèges,
- **L'utilisation d'un appareil marqué comme conforme**, garantissant que le poste respecte les politiques de sécurité définies dans Intune (chiffrement, état du système, configuration).

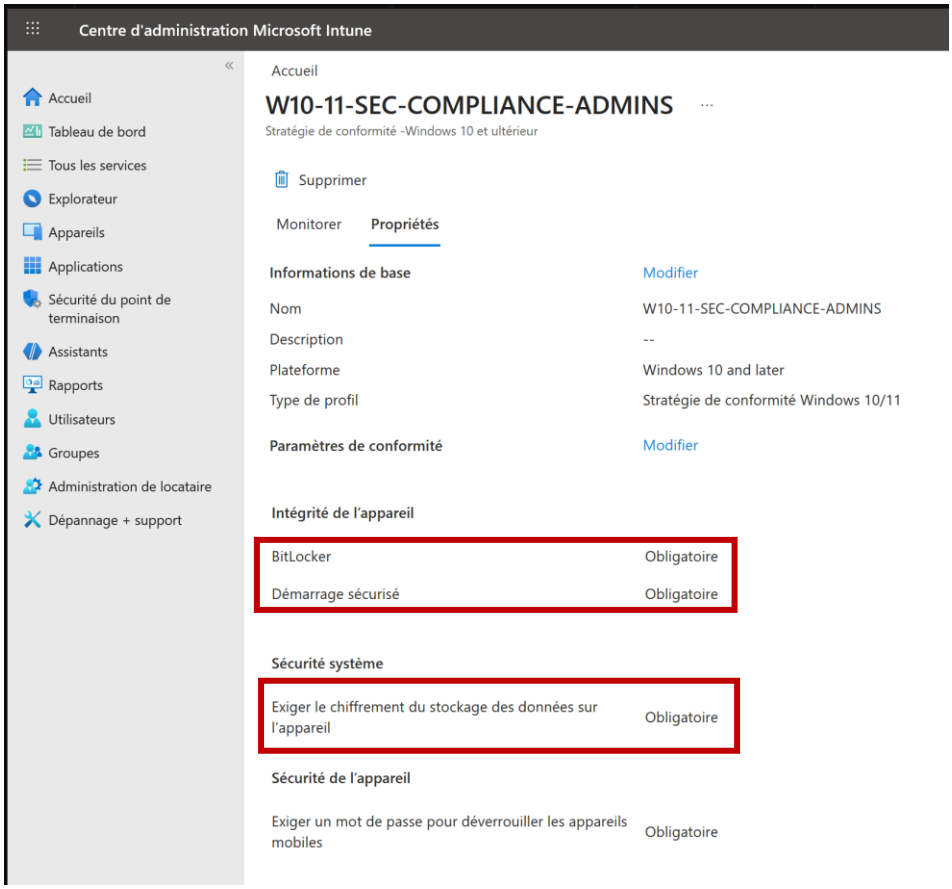
L'accès est accordé uniquement si **toutes les conditions sont satisfaites**, ce qui permet de s'assurer que les administrateurs se connectent depuis un environnement maîtrisé et sécurisé.

Cette configuration répond aux bonnes pratiques de sécurité en limitant les risques liés au vol d'identifiants et à l'utilisation de postes non conformes.

3. Sécurisation du Poste de Travail (Intune)

Une stratégie de conformité Windows 10/11 nommée **W10-11-SEC-COMPLIANCE-ADMINS** a été créée pour durcir le niveau de sécurité des postes :

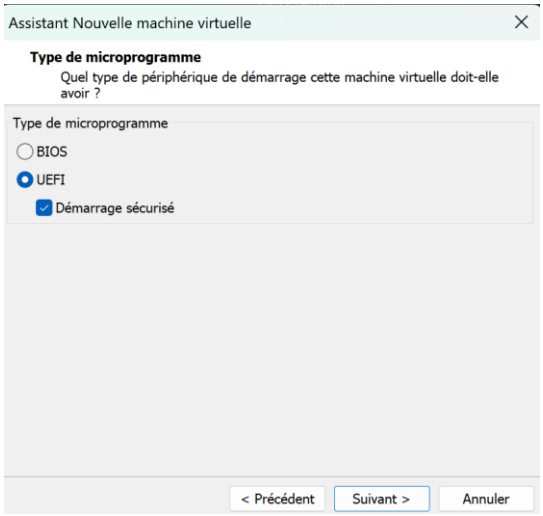
- **Intégrité de l'appareil** : Activation obligatoire du **Secure Boot**.
- **Chiffrement** : Exigence du chiffrement des données via **BitLocker**.
- **Sécurité Système** : Obligation d'un mot de passe pour déverrouiller l'appareil.



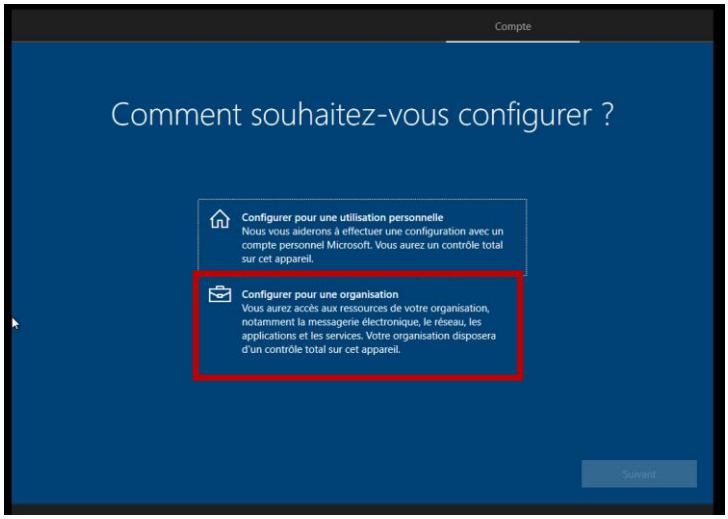
4. Déploiement

L'enrôlement de la machine de test (`DESKTOP-NIHIEFL`) pour l'utilisateur **Admin Junior** a nécessité une intervention technique sur l'hyperviseur **VMware**:

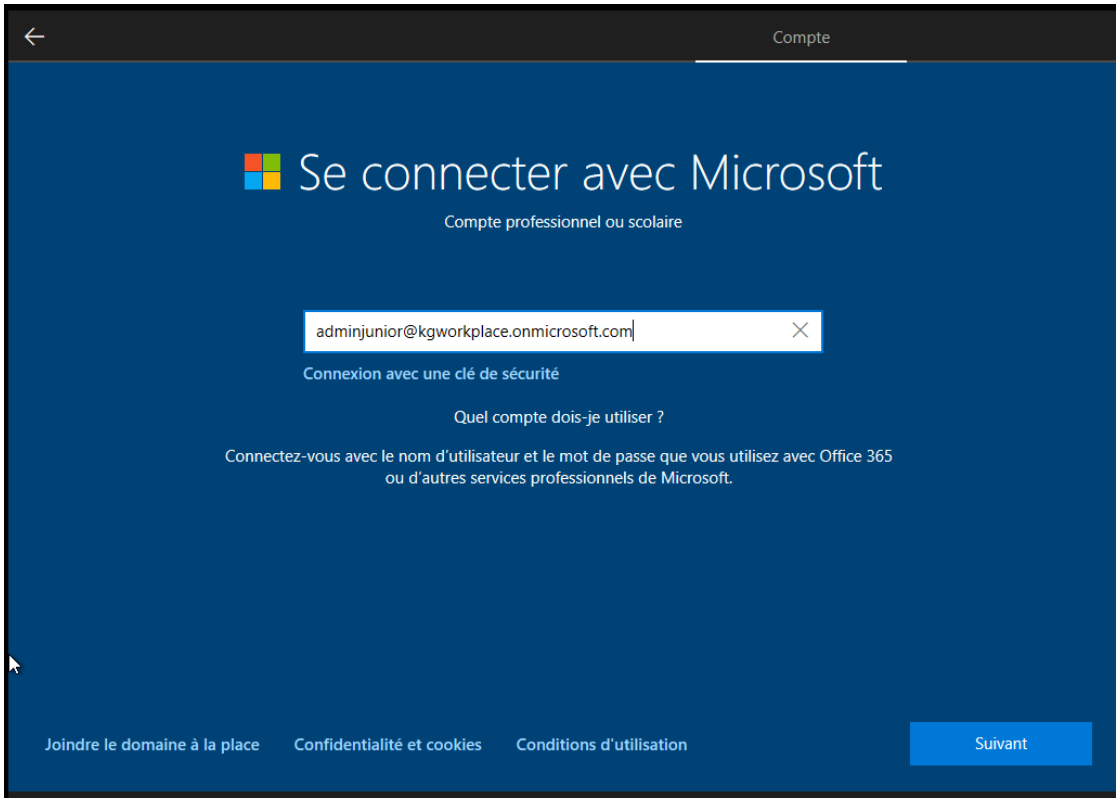
Configuration UEFI/TPM : Pour satisfaire aux exigences de BitLocker, le microprogramme de la VM a été configuré en **UEFI** avec l'activation du **Démarrage sécurisé** (Secure Boot).



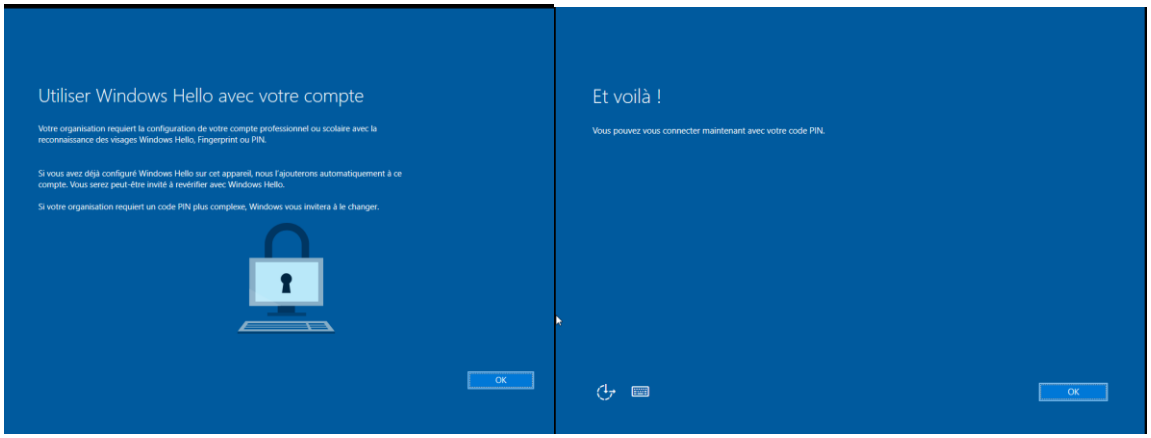
Une fois Windows 10 installé, il faut configurer le poste

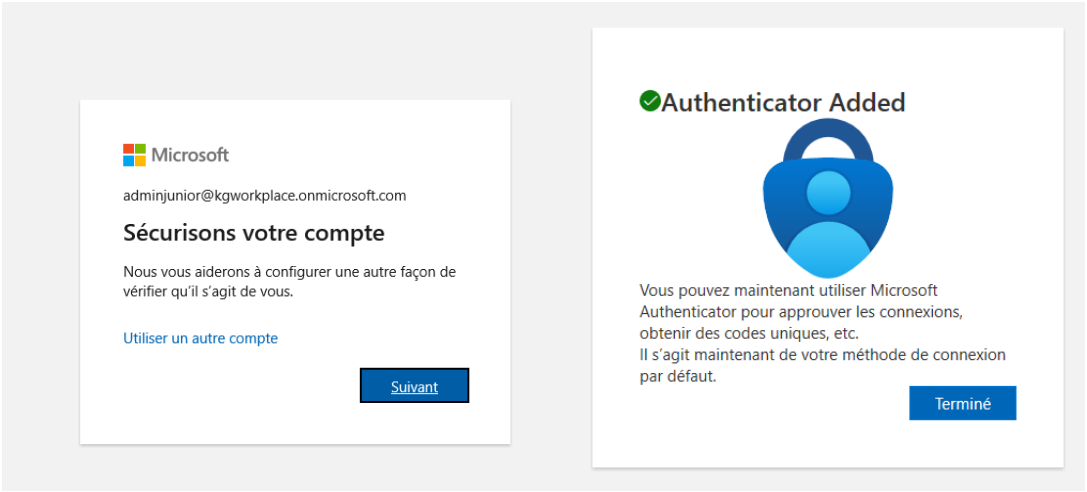


L’utilisateur se connecte avec son compte professionnel afin de joindre le poste à **Microsoft Entra ID**

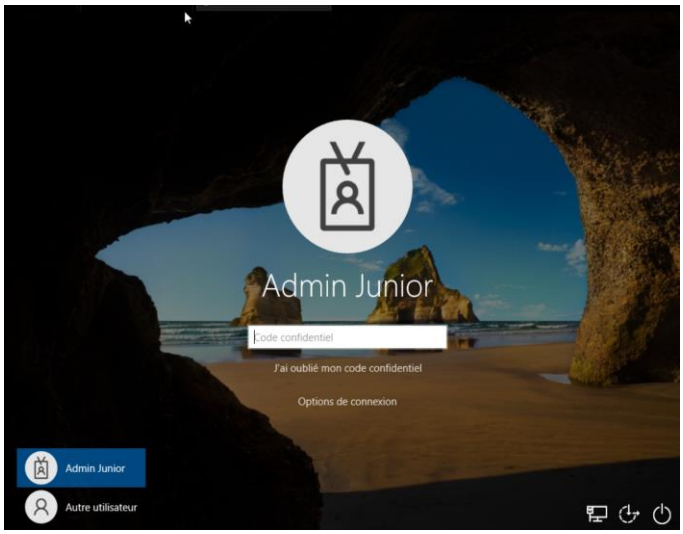


Authentification Forte : L'utilisateur a configuré son compte via l'application **Microsoft Authenticator** et a défini un code PIN Windows Hello pour une connexion sécurisée

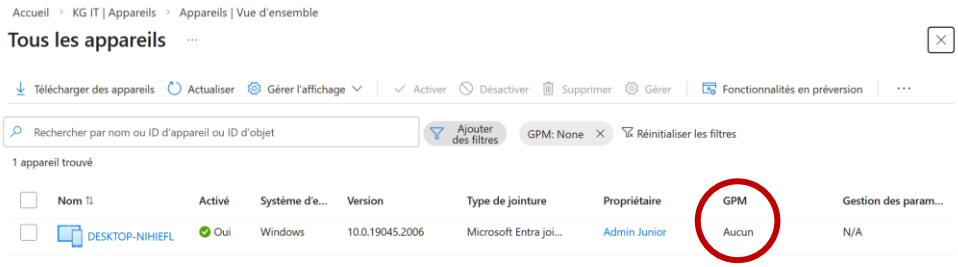




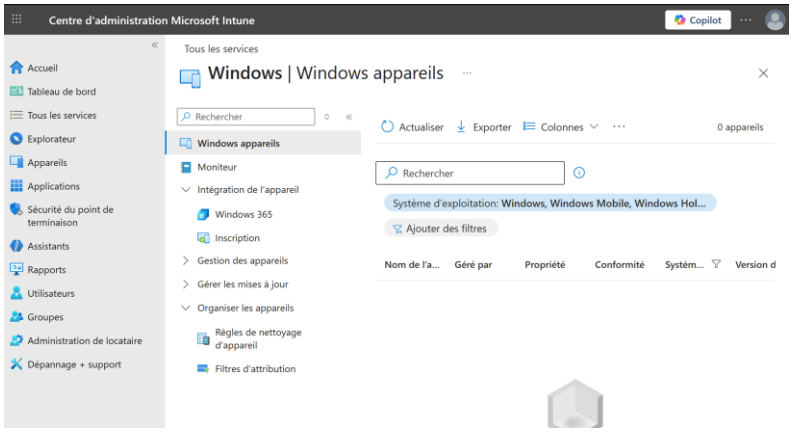
L’utilisateur “Admin Junior” peut maintenant accéder à sa session



L’appareil est enregistré sur Microsoft Entra, ici on aperçoit également que MDM (**Mobile Device Management**) n’est pas présent, cela a pour conséquence l’impossibilité pour l'organisation de piloter l'appareil, d'y déployer des applications ou d'appliquer des politiques de sécurité à distance via Intune



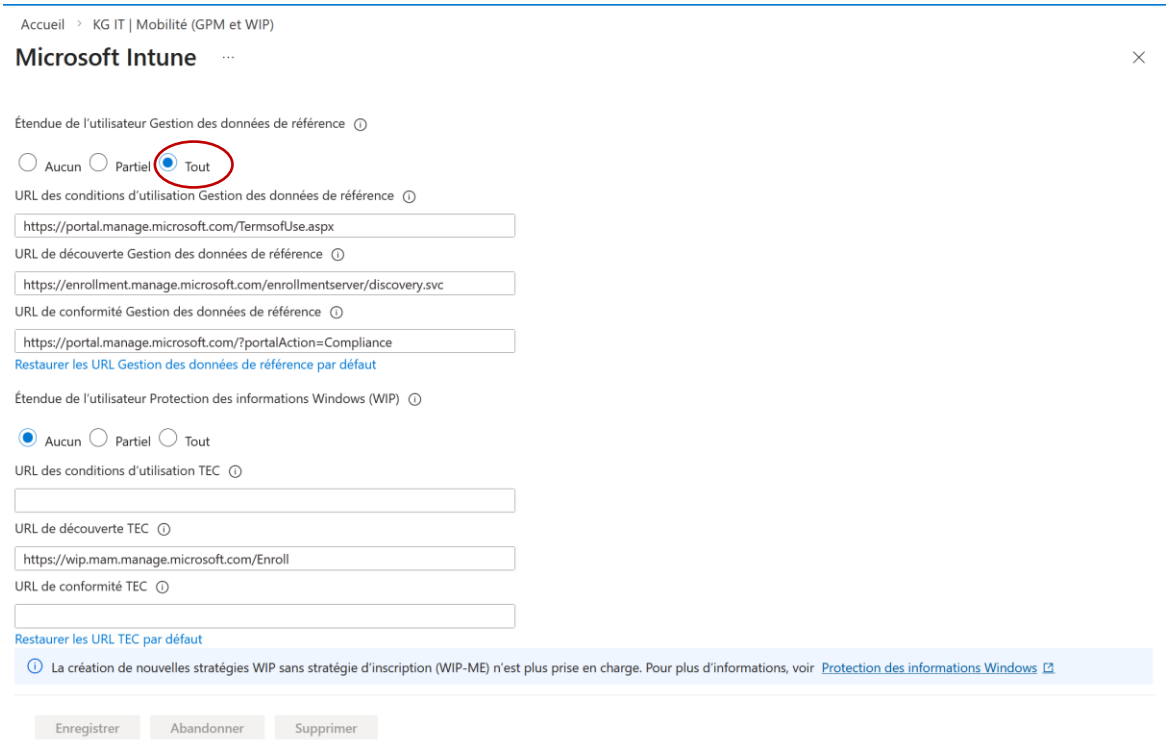
Cela se traduit directement par l’absence de l’appareil dans la console Intune



Configuration de la portée de l'enrôlement (Automatic Enrollment)

Cette configuration permet d'automatiser l'enrôlement des postes Windows dans **Microsoft Intune** via le mécanisme d'**enrôlement automatique MDM**.

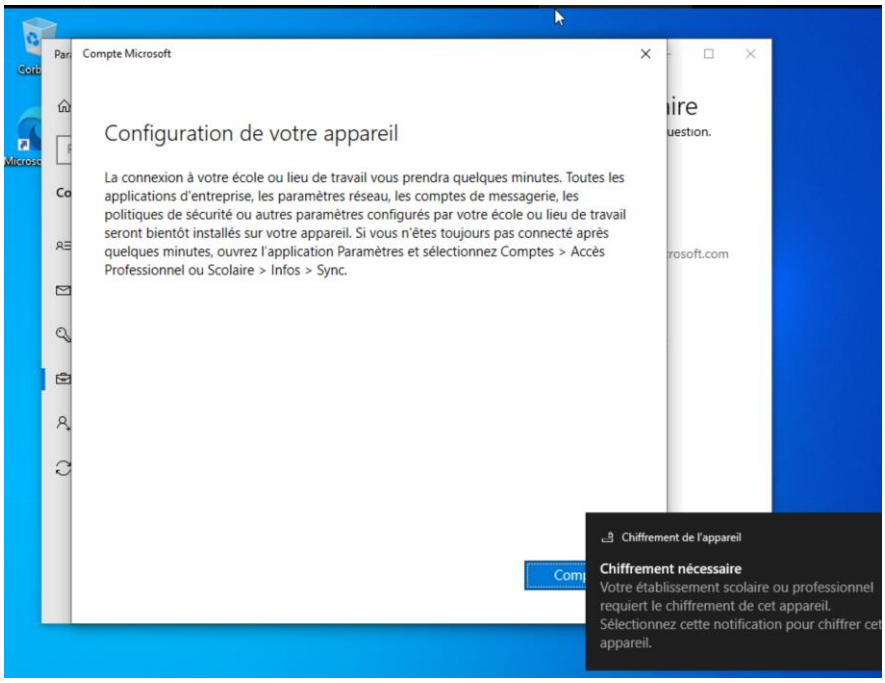
Lorsque l'utilisateur "Admin Junior" se connecte à un poste Windows joint à **Microsoft Entra ID**, le terminal est automatiquement inscrit dans Intune et bascule du statut



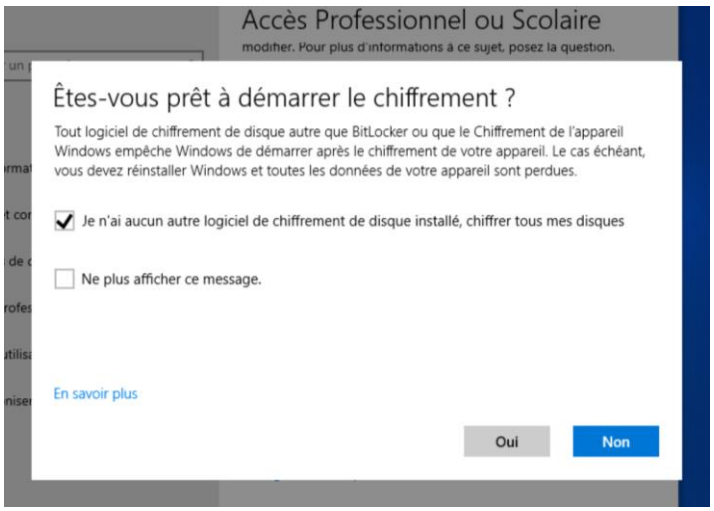
*Note technique : En entreprise, ce réglage est généralement positionné sur **'Partiel'** afin de limiter l'enrôlement à un groupe de test (Pilote) et de maîtriser l'impact du déploiement sur le parc informatique*

Une fois la configuration de l'**Étendue de l'utilisateur** activée sur **"Tout"** dans le portail Microsoft Intune, le lien entre l'infrastructure Cloud et le poste client est devenu opérationnel.

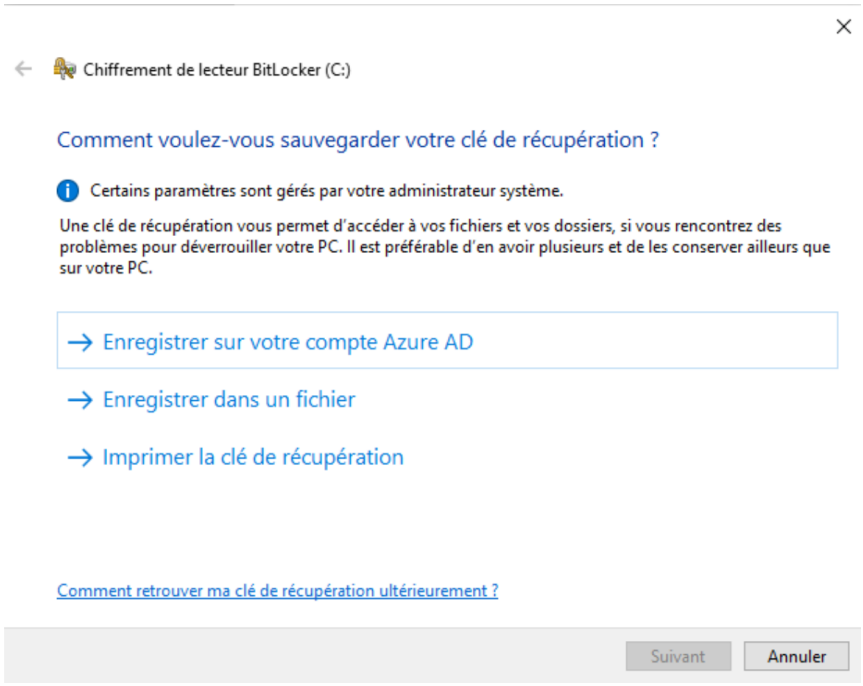
Constat immédiat sur le poste de travai**l :** Dès la connexion du compte professionnel, nous pouvons confirmer que l'enrôlement a réussi grâce à la notification de demande de chiffrement



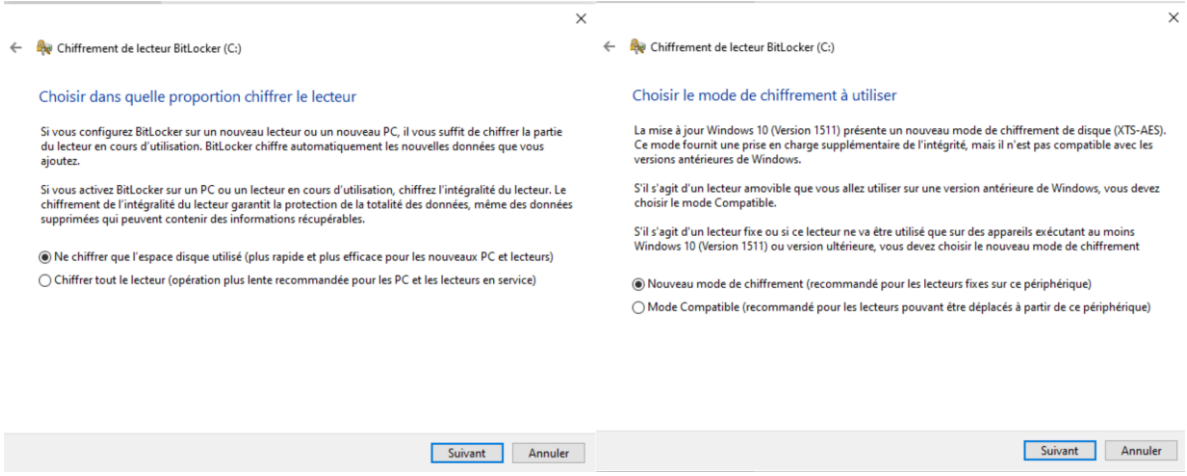
Suite à la notification de chiffrement, le processus de mise en conformité est lancé. Ces captures montrent les étapes critiques du chiffrement :



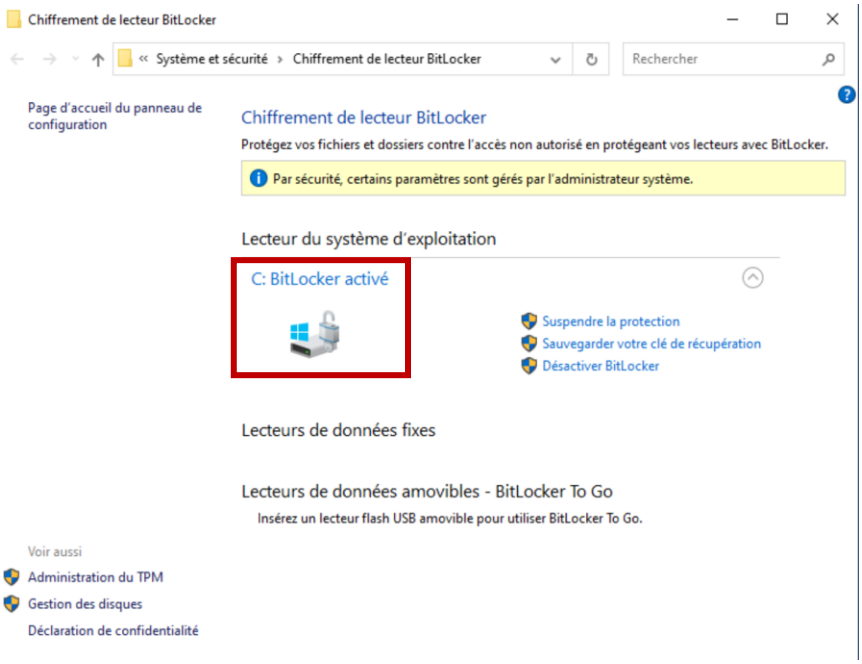
J'ai sélectionné l'option **"Enregistrer dans votre compte Azure AD"** pour ne pas perdre l'accès aux données en cas d'oubli de mot de passe.



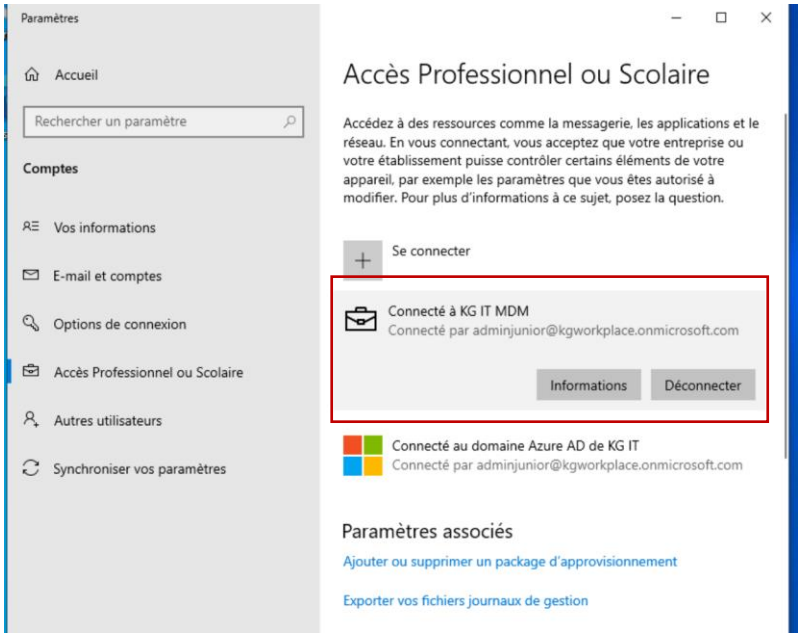
Méthode de chiffrement : J'ai choisi de chiffrer "l'espace disque utilisé uniquement" pour plus de rapidité dans ce lab, tout en garantissant la sécurité des données existantes.



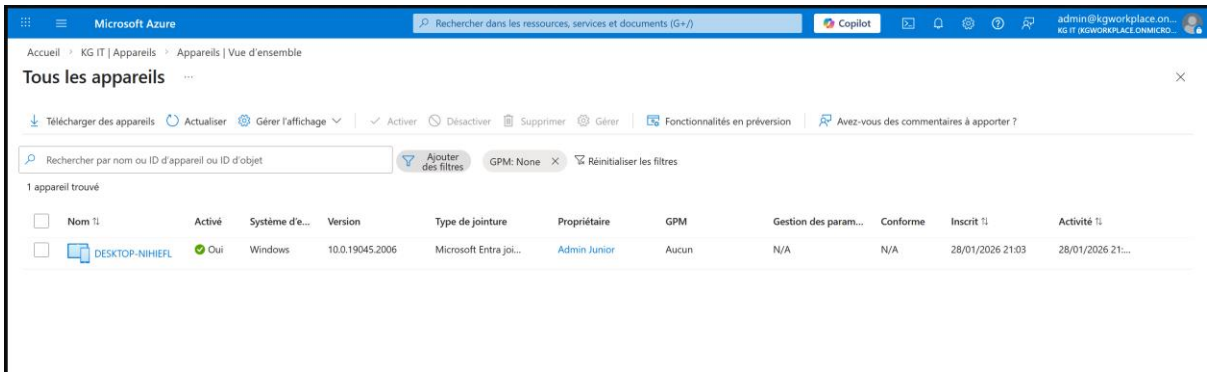
Dans le Panneau de configuration, le lecteur système affiche désormais explicitement le statut **"C: BitLocker activé"**



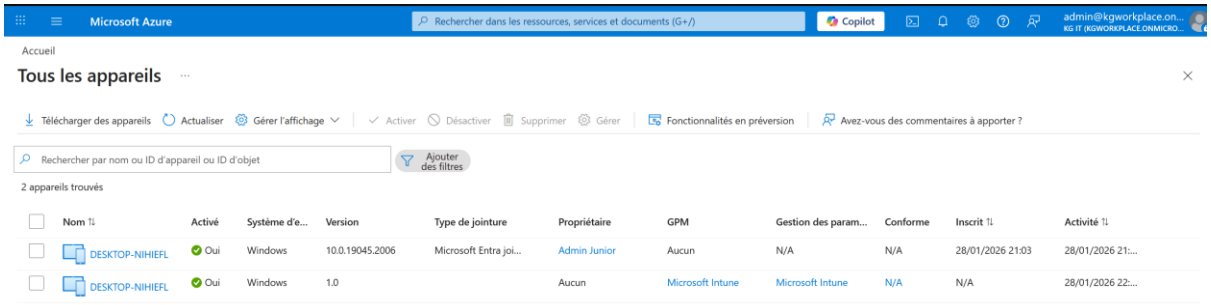
Liaison MDM et Azure AD : Dans les paramètres de compte, la section "Accès Professionnel ou Scolaire" confirme que l'appareil est **"Connecté à KG IT MDM"** et **"Connecté au domaine Azure AD de KG IT"**. L'adresse mail de l'utilisateur (admin junior) est correctement associée, validant l'identité et la gestion du périphérique.



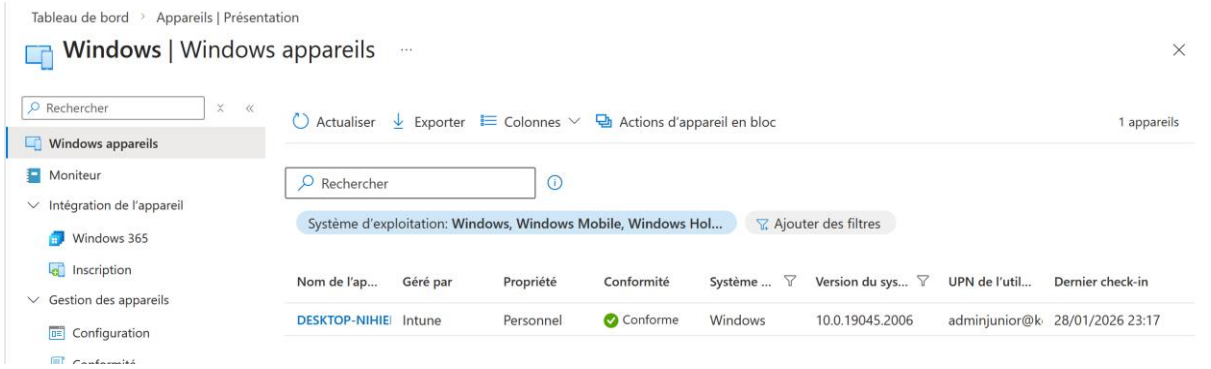
L'état initial (Ligne 1) : On observe l'appareil `DESKTOP-NIHIEFL` avec un statut **"GPM : Aucun"**. À ce stade, le PC est bien inscrit dans l'annuaire (Microsoft Entra joined), mais il n'est pas encore piloté par Intune. C'est pour cette raison qu'il n'apparaissait pas initialement dans la console de gestion MDM.



L'état final (Ligne 2) : Après l'activation de la portée de l'utilisateur et la finalisation de l'enrôlement sur le poste, une seconde entrée apparaît avec le statut **"GPM : Microsoft Intune"**.



Enfin, la console d'administration Intune confirme la réussite totale du déploiement : le terminal est désormais marqué comme **Conforme**, validant ainsi l'application du chiffrement BitLocker et la sécurisation du poste de travail.

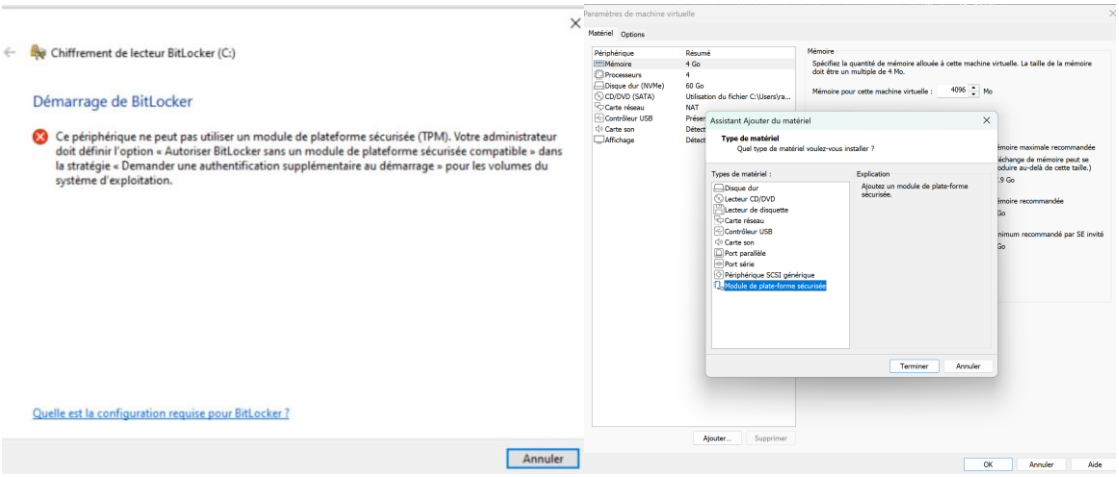


Challenges techniques rencontrés

1. Obstacle : Échec de la conformité BitLocker sur environnement virtuel

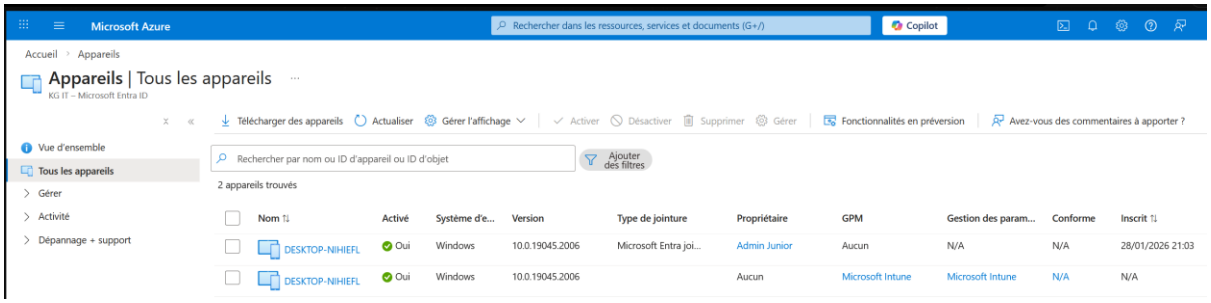
- **Symptôme :** Lors de l'enrôlement, l'appareil restait en état "Non conforme" et le chiffrement ne se lançait pas.
- **Analyse :** Le diagnostic a révélé l'absence de puce TPM et un démarrage en mode BIOS Legacy, incompatibles avec les exigences de sécurité modernes.
- **Résolution :** Intervention sur l'hyperviseur (VMware) pour :
    - Chiffrer la VM pour permettre l'ajout d'un **vTPM**.

  Résultat : Conformité validée immédiatement après le redémarrage.



2. Observation : Persistance d'un doublon d'objet dans le portail

- **Symptôme :** Présence de deux entrées pour le même poste dans Microsoft Entra.
- **Analyse :** Ce comportement est dû au délai de réplication entre la jonction Entra ID (Identité) et l'enregistrement Intune (MDM).
- **Vérification :** La validation s'est faite en vérifiant que l'objet géré par Intune possédait bien le certificat de conformité et la version d'OS correcte.



Conclusion du Lab : Gestion moderne et sécurisée

Ce lab a permis de valider la mise en place d'un poste de travail moderne, intégré à Microsoft 365 et entièrement supervisé par Intune. La structuration des identités dans Microsoft Entra ID et l'application de politiques d'Accès Conditionnel ont instauré une approche **Zero Trust**.

La résolution des problématiques de conformité a mis en évidence le lien direct entre sécurité logicielle (Intune, BitLocker) et prérequis matériels (TPM, Secure Boot), soulignant l'importance de l'architecture du poste dans une stratégie de chiffrement.

Au final, le poste est désormais géré par Intune, chiffré avec BitLocker et reconnu comme conforme aux politiques de sécurité.

Ce projet démontre ma capacité à concevoir, sécuriser et diagnostiquer un environnement Modern Workplace Microsoft, en tenant compte des contraintes matérielles, identitaires et organisationnelles rencontrées en entreprise.