

# 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.

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with links for Accueil, Copilot, Agents, Utilisateurs, Appareils, Teams et groupes (selected), Marketplace, Facturation, Configuration, and Personnaliser la navigation. The main content area is titled "Équipe et groupes actifs". It has tabs for Groupes Teams & Microsoft 365, Liste de distribution, and Groupes de sécurité (which is selected). Below these tabs are buttons for Ajouter un groupe de sécurité, Ajouter un groupe de sécurité à extension courrier, and Exporter. A table lists three security groups: GRP-SEC-ADMINS, GRP-SEC-COMMERCIAUX, and GRP-SEC-FINANCE. Each group entry includes a checkbox, an ellipsis button, and a "État de sy..." button. At the top of the main content area, there's a search bar labeled "Rechercher".

## 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

The screenshot shows the Microsoft Intune Conditional Access Strategies blade. The strategy is named "SEC-IAM-01-MFA-Finance". The "Affectations" section is configured to apply to "Utilisateurs ou assistants (Préversion)" and "Utilisateurs spécifiques inclus". The "Ressources cibles" section is set to "Toutes les ressources (anciennement « Toutes les applications cloud »)". The "Octroyer" section is configured to "Accorder l'accès" and includes the condition "Exiger une authentication multifacteur". The "Conditions" section shows 0 conditions sélectionnées.

Centre d'administration Microsoft Intune

SEC-IAM-01-MFA-Finance

Stratégie d'accès conditionnel

Supprimer Afficher les informations de stratégie Afficher l'impact de stratégie

Contrôlez l'accès en fonction de la stratégie d'accès conditionnel pour regrouper les signaux, prendre des décisions et appliquer des stratégies organisationnelles. En savoir plus

Nom \* SEC-IAM-01-MFA-Finance

Affections Utilisateurs ou assistants (Préversion) Utilisateurs spécifiques inclus

Ressources cibles Toutes les ressources (anciennement « Toutes les applications cloud »)

Réseau NOUVEAUTÉ Non configuré

Conditions 0 conditions sélectionnées

Contrôles d'accès Octroyer 1 contrôle sélectionné

Session 0 contrôles sélectionnés

Sélectionner ce à quoi cette stratégie s'applique Ressources (anciennement applications ...)

Octroyer

Contrôlez l'application de l'accès pour bloquer ou accorder l'accès. En savoir plus

Bloquer l'accès Accorder l'accès

Exiger une authentication multifacteur

## 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

Nom	Type d'emplacement	Approuvé	Stratégies d'accès conditionnel	Date de création	Date de modifica...
Pays-Autorisés	Pays (IP)	✓	SEC-IAM-02-Block-International	27/01/2026 20...	27/01/2026 20...

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

The screenshot displays the Microsoft Intune Admin Center interface. On the left, the navigation menu includes options like Accueil, Tableau de bord, Tous les services, Explorateur, Appareils, Applications, Sécurité du point de terminaison, Assistants, Rapports, Utilisateurs, Groups, Administration de locataire, and Dépannage + support. The main content area shows a strategy named "SEC-IAM-03-Admin-MFA-Compliance". The "Octroyer" (Grant) screen is open, showing various access controls. Two specific controls are highlighted with red boxes: "Exiger une authentification multifactor" (checkbox checked) and "Exiger que l'appareil soit marqué comme conforme" (checkbox checked). Other visible controls include "Bloquer l'accès" (unchecked), "Exiger la force de l'authentification" (unchecked), "Ne bloquez pas votre accès!" (unchecked), and several others like "Demandez une application cliente approuvée" and "Exigez une stratégie de protection des applications".

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 :

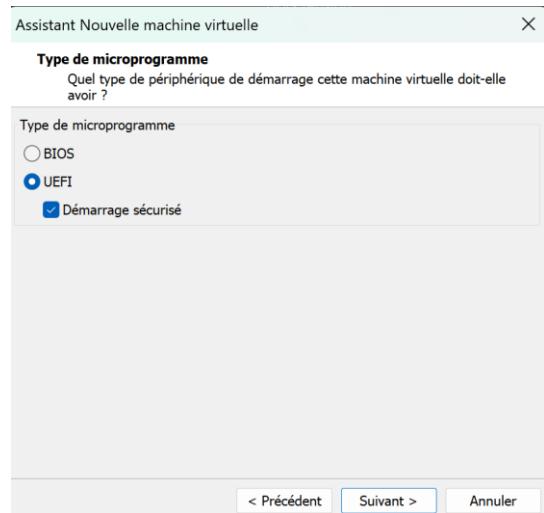
- **Intégrité de l'appareil** : Activation obligatoire du **Secure Boot**.
- **Chiffrement** : Exigence du chiffrement des données via **BitLocker**.
- **Sécurité Système** : Obligation d'un mot de passe pour déverrouiller l'appareil.

The screenshot shows the Microsoft Intune Admin Center interface. On the left, there's a sidebar with various navigation links like Accueil, Tableau de bord, Tous les services, Explorateur, Appareils, Applications, Sécurité du point de terminaison, Assistants, Rapports, Utilisateurs, Groupes, Administration de locataire, and Dépannage + support. The main content area is titled "W10-11-SEC-COMPLIANCE-ADMINS" and describes it as a "Stratégie de conformité -Windows 10 et ultérieur". It has tabs for "Monitorer" and "Propriétés", with "Propriétés" being active. Under "Informations de base", it shows "Nom: W10-11-SEC-COMPLIANCE-ADMINS", "Description: --", "Plateforme: Windows 10 and later", and "Type de profil: Stratégie de conformité Windows 10/11". There are "Modifier" buttons for both "Informations de base" and "Paramètres de conformité". The "Paramètres de conformité" section is collapsed. Below that is the "Intégrité de l'appareil" section, which is expanded and highlighted with a red box. It lists two requirements: "BitLocker" (Obligatoire) and "Démarrage sécurisé" (Obligatoire). The "Sécurité système" section is also highlighted with a red box and lists one requirement: "Exiger le chiffrement du stockage des données sur l'appareil" (Obligatoire). At the bottom, there's a "Sécurité de l'appareil" section with one requirement: "Exiger un mot de passe pour déverrouiller les appareils mobiles" (Obligatoire).

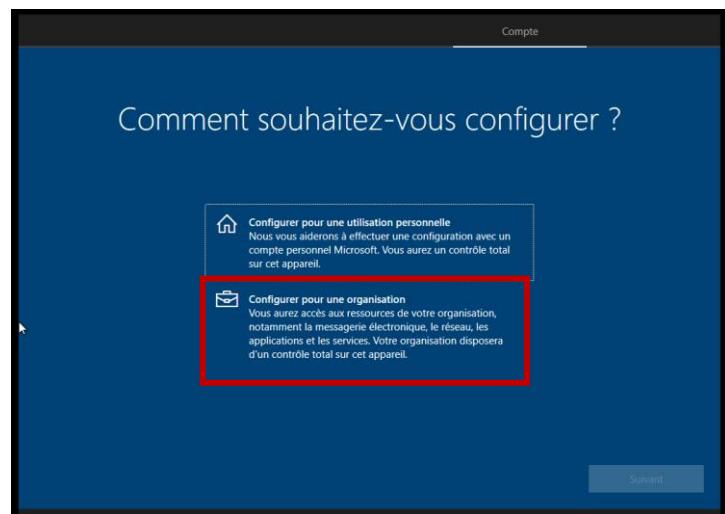
#### 4. Déploiement

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

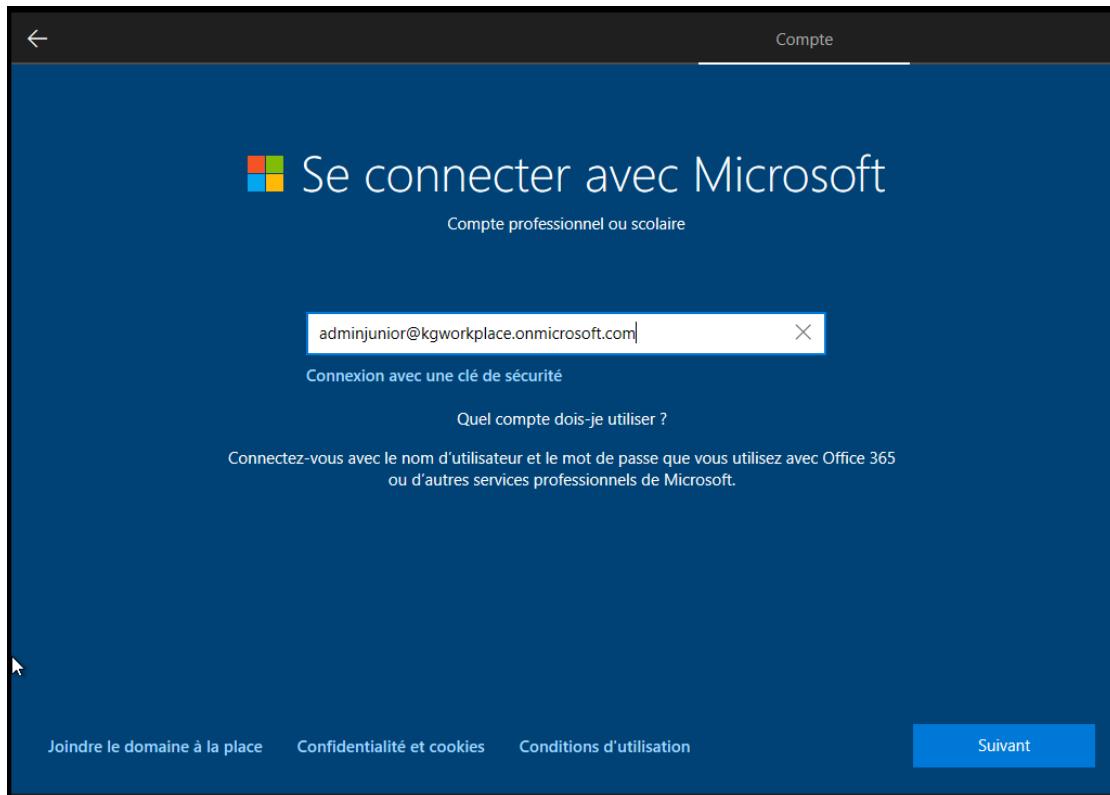
**Configuration UEFI/TPM :** Pour satisfaire aux exigences de BitLocker, le microprogramme de la VM a été configuré en **UEFI** avec l'activation du **Démarrage sécurisé** (Secure Boot).



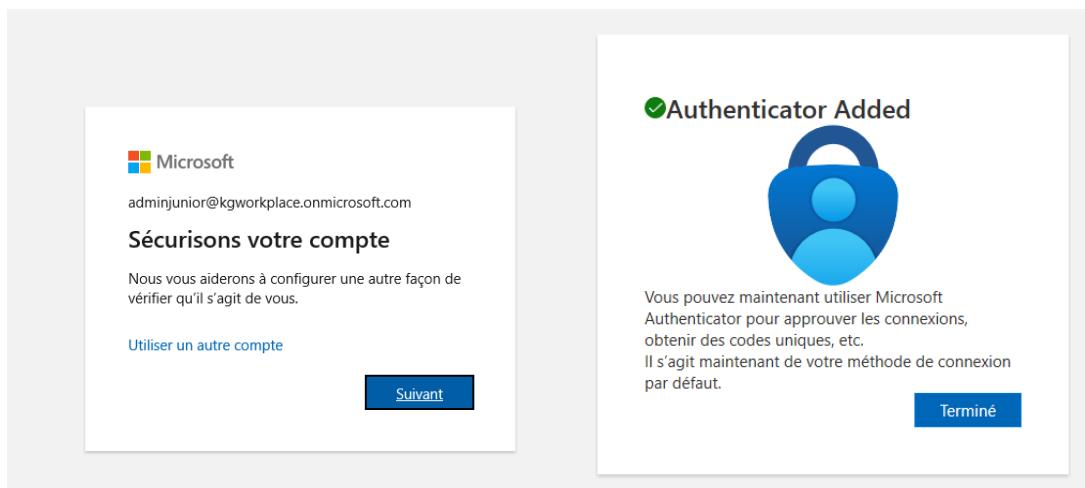
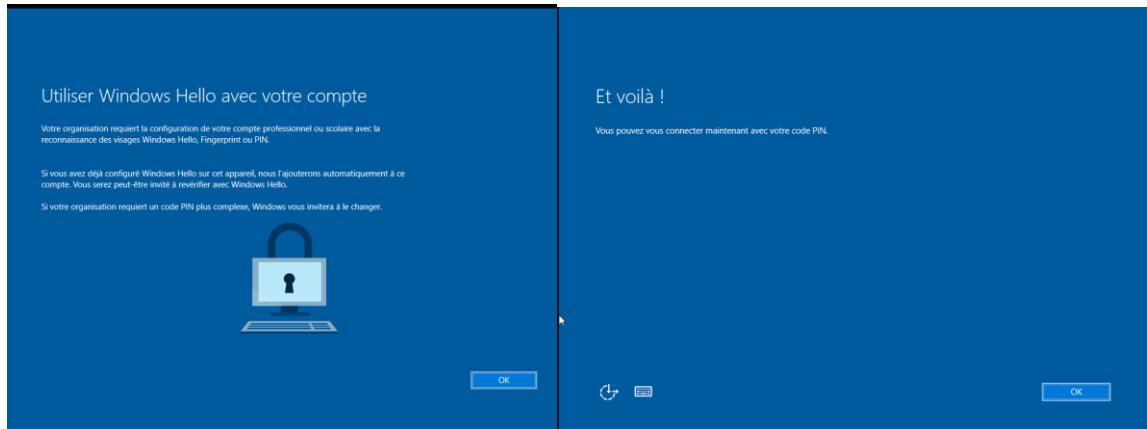
Une fois Windows 10 installé, il faut configurer le poste



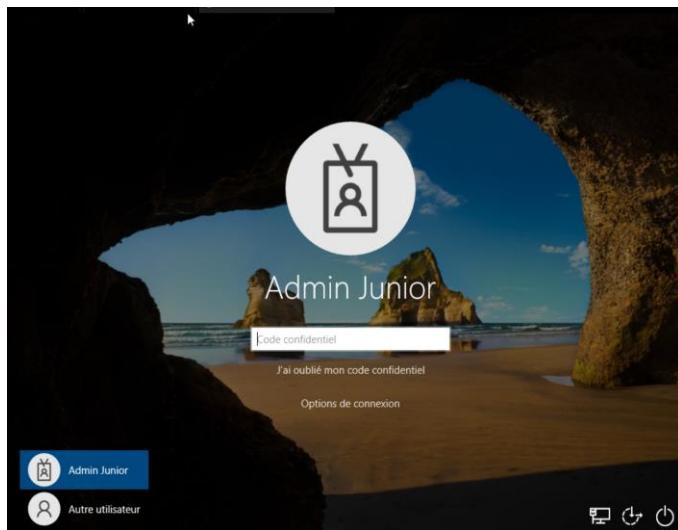
L'utilisateur se connecte avec son compte professionnel afin de joindre le poste à **Microsoft Entra ID**



**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

Accueil > KG IT | Appareils > Appareils | Vue d'ensemble

Tous les appareils ... X

Download devices Update Manage display Activate Deactivate Delete Manage Preview features More

Search for device name or ID Add filters GPM: None Reset filters

1 device found

Nom	Activé	Système d'e...	Version	Type de jointure	Propriétaire	GPM	Gestion des param...
DESKTOP-NIHIEFL	Oui	Windows	10.0.19045.2006	Microsoft Entra jo...	Admin Junior	Aucun	N/A

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

Centre d'administration Microsoft Intune

Accueil Tableau de bord Tous les services Windows | Windows appareils ...

Rechercher Actualiser Exporter Colonnes ... 0 appareils

Moniteur Intégration de l'appareil Windows 365 Inscription

Gestion des appareils Gérer les mises à jour Organiser les appareils Règles de nettoyage d'appareil Filtres d'attribution

Nom de l'a... Géré par Propriété Conformité Système Version d'

## 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

Accueil > KG IT | Mobilité (GPM et WIP)

**Microsoft Intune** ...

Étendue de l'utilisateur Gestion des données de référence ⓘ

Aucun  Partiel  Tout

URL des conditions d'utilisation Gestion des données de référence ⓘ

https://portal.manage.microsoft.com/TermsOfUse.aspx

URL de découverte Gestion des données de référence ⓘ

https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc

URL de conformité Gestion des données de référence ⓘ

https://portal.manage.microsoft.com/?portalAction=Compliance

[Restaurer les URL Gestion des données de référence par défaut](#)

Étendue de l'utilisateur Protection des informations Windows (WIP) ⓘ

Aucun  Partiel  Tout

URL des conditions d'utilisation TEC ⓘ

URL de découverte TEC ⓘ

https://wip.mam.manage.microsoft.com/Enroll

URL de conformité TEC ⓘ

[Restaurer les URL TEC par défaut](#)

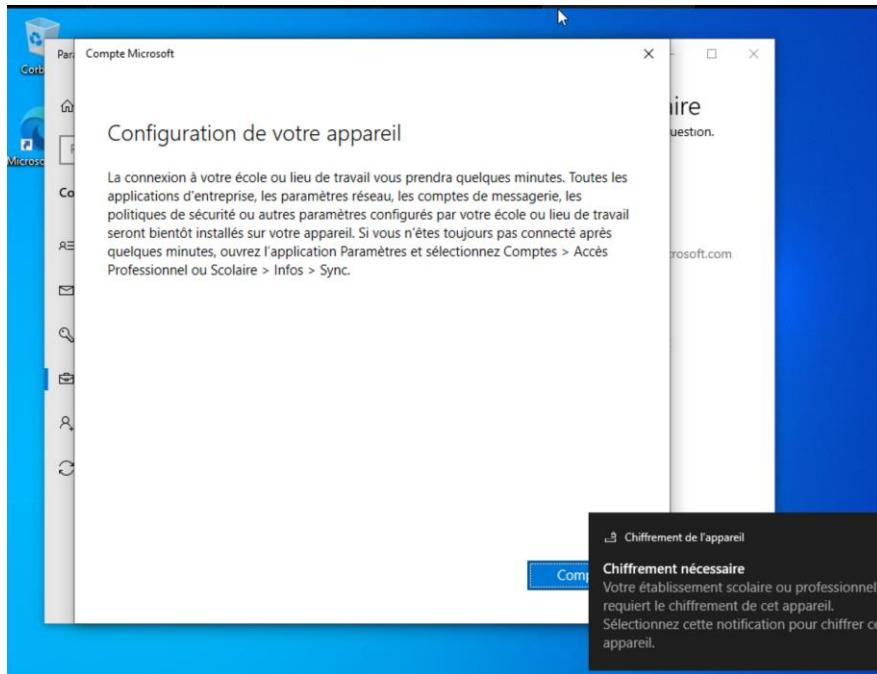
ⓘ La création de nouvelles stratégies WIP sans stratégie d'inscription (WIP-ME) n'est plus prise en charge. Pour plus d'informations, voir [Protection des informations Windows](#).

Enregistrer Abandonner Supprimer

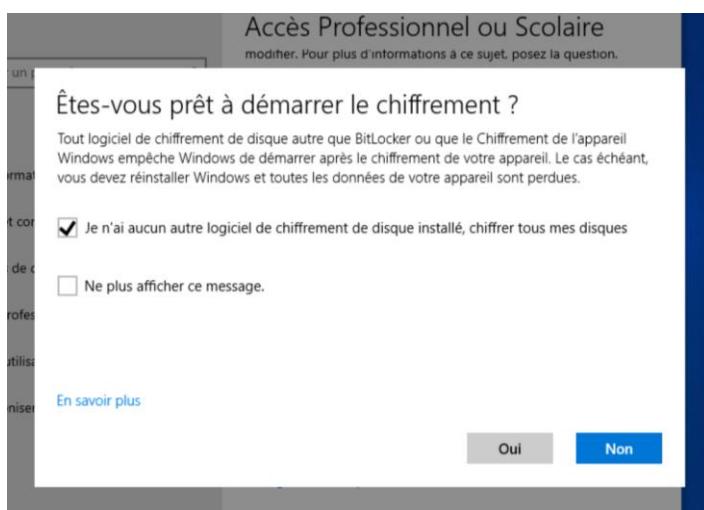
*Note technique : En entreprise, ce réglage est généralement positionné sur 'Partiel' afin de limiter l'enrôlement à un groupe de test (Pilote) et de maîtriser l'impact du déploiement sur le parc informatique*

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 travail : 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 :



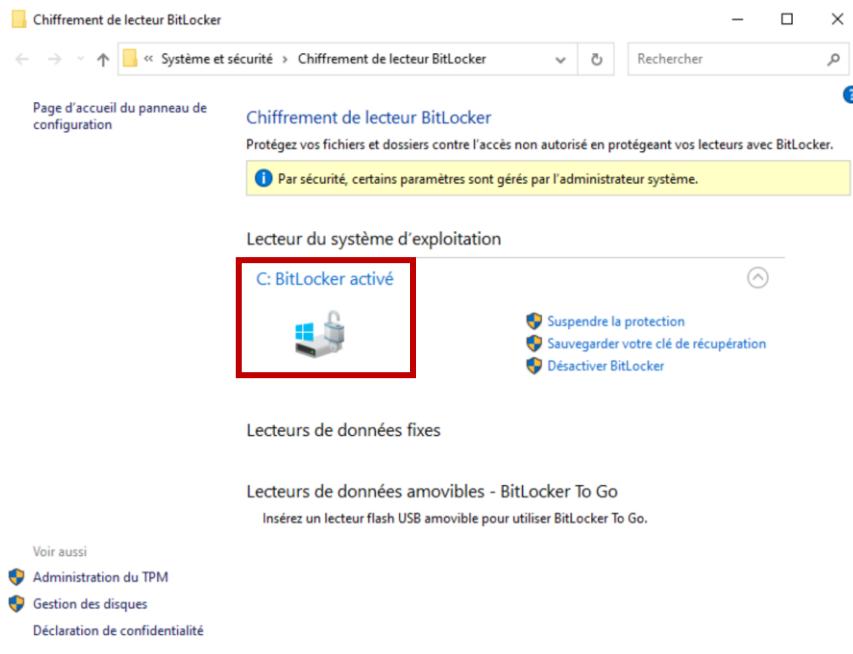
J'ai sélectionné l'option "**Enregistrer dans votre compte Azure AD**" pour ne pas perdre l'accès aux données en cas d'oubli de mot de passe.

The screenshot shows the 'Comment sauvegarder votre clé de récupération?' (How do you want to save your recovery key?) step of the BitLocker setup wizard. At the top, there is a note: 'Certs certains paramètres sont gérés par votre administrateur système.' Below it, a note states: 'Une clé de récupération vous permet d'accéder à vos fichiers et vos dossiers, si vous rencontrez des problèmes pour déverrouiller votre PC. Il est préférable d'en avoir plusieurs et de les conserver ailleurs que sur votre PC.' Three options are listed: 'Enregistrer sur votre compte Azure AD' (selected), 'Enregistrer dans un fichier', and 'Imprimer la clé de récupération'. A link 'Comment retrouver ma clé de récupération ultérieurement?' is at the bottom, and 'Suivant' and 'Annuler' buttons are at the bottom right.

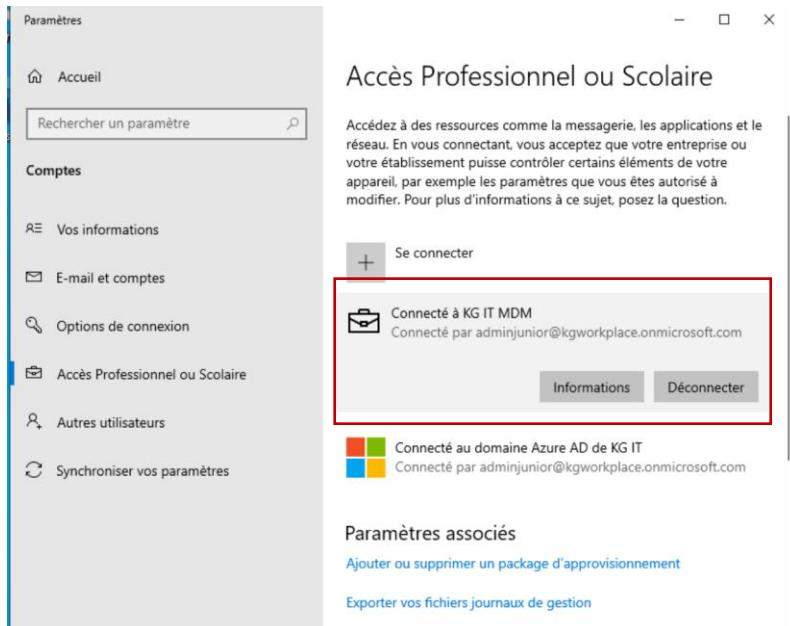
**Méthode de chiffrement :** J'ai choisi de chiffrer "l'espace disque utilisé uniquement" pour plus de rapidité dans ce lab, tout en garantissant la sécurité des données existantes.

The screenshot shows two steps of the BitLocker setup wizard. The first step, 'Choisir dans quelle proportion chiffrer le lecteur', contains notes about chipping the used disk space and selecting the encryption mode. It includes radio buttons for 'Ne chiffrer que l'espace disque utilisé' (selected) and 'Chiffrer tout le lecteur'. The second step, 'Choisir le mode de chiffrement à utiliser', contains notes about the XTS-AES mode and the Compatible mode. It includes radio buttons for 'Nouveau mode de chiffrement' (selected) and 'Mode Compatible'.

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.

Nom	Activé	Système d'e...	Version	Type de jointure	Propriétaire	GPM	Gestion des param...	Conforme	Inscrit	Activité
DESKTOP-NIHIEFL	Oui	Windows	10.0.19045.2006	Microsoft Entra jo...	Admin Junior	Aucun	N/A	N/A	28/01/2026 21:03	28/01/2026 21:...

**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**".

Nom	Activé	Système d'e...	Version	Type de jointure	Propriétaire	GPM	Gestion des param...	Conforme	Inscrit	Activité
DESKTOP-NIHIEFL	Oui	Windows	10.0.19045.2006	Microsoft Entra jo...	Admin Junior	Aucun	N/A	N/A	28/01/2026 21:03	28/01/2026 21:...
DESKTOP-NIHIEFL	Oui	Windows	1.0			Aucun	Microsoft Intune	Microsoft Intune	N/A	28/01/2026 22:...

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.

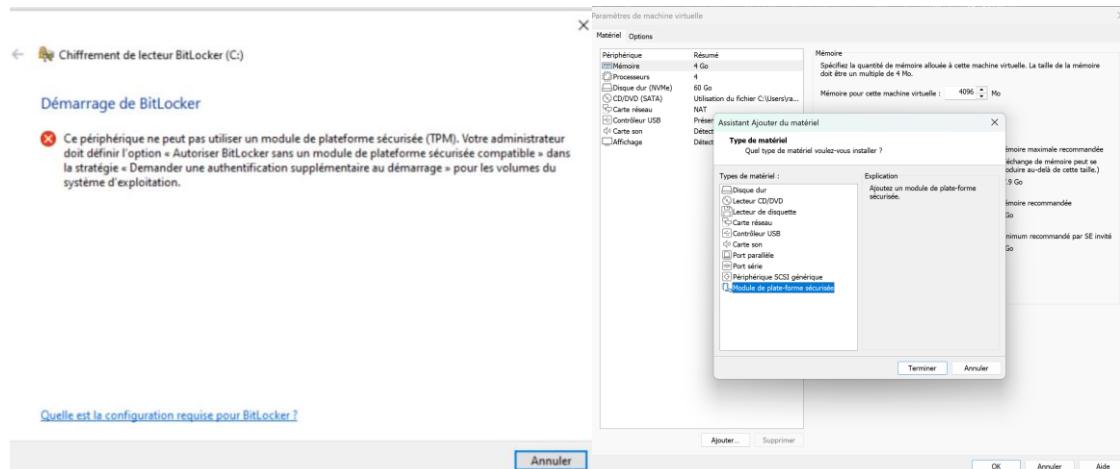
Nom de l'appareil	Géré par	Propriété	Conformité	Système d'exploitation	Version du système	UPN de l'utilisateur	Dernier check-in
DESKTOP-NIHIEFL	Intune	Personnel	Conforme	Windows	10.0.19045.2006	adminjunior@k...	28/01/2026 23:17

## 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.

Nom	Activé	Système d'exploitation	Version	Type de jointure	Propriétaire	GPM	Gestion des paramètres	Conforme	Inscrit
DESKTOP-NIIHIEFL	Oui	Windows	10.0.19045.2006	Microsoft Entra jointure	Admin Junior	Aucun	N/A	N/A	28/01/2026 21:03
DESKTOP-NIIHIEFL	Oui	Windows	10.0.19045.2006		Aucun	Microsoft Intune	Microsoft Intune	N/A	N/A

## 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.