

Modern Workplace et Sécurité Cloud




Introduction et Objectifs

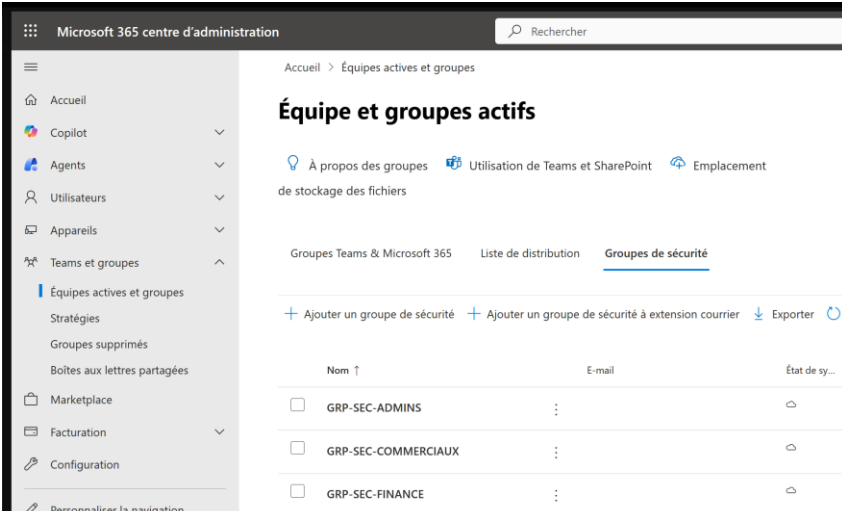
L'objectif de ce lab est de mettre en place une infrastructure de gestion moderne des terminaux (Modern Endpoint Management) en utilisant la suite **Microsoft 365**. Ce projet se concentre sur la sécurisation des accès et des données via des politiques de conformité et l'accès conditionnel.

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.

Nom ↑	Nom d'utilisateur pour la connexion	Licences
 Admin Junior	adminjunior@kgworkplace.onmicrosoft.com	Microsoft 365 Business Premium
 Commercial Nomade	commercialnomade@kgworkplace.onmicrosoft.com	Microsoft 365 Business Premium
 Directeur Finance	directeurfinance@kgworkplace.onmicrosoft.com	Microsoft 365 Business Premium



Nom ↑	E-mail	État de sy...
<input type="checkbox"/> GRP-SEC-ADMINS	:	
<input type="checkbox"/> GRP-SEC-COMMERCIAUX	:	
<input type="checkbox"/> GRP-SEC-FINANCE	:	

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

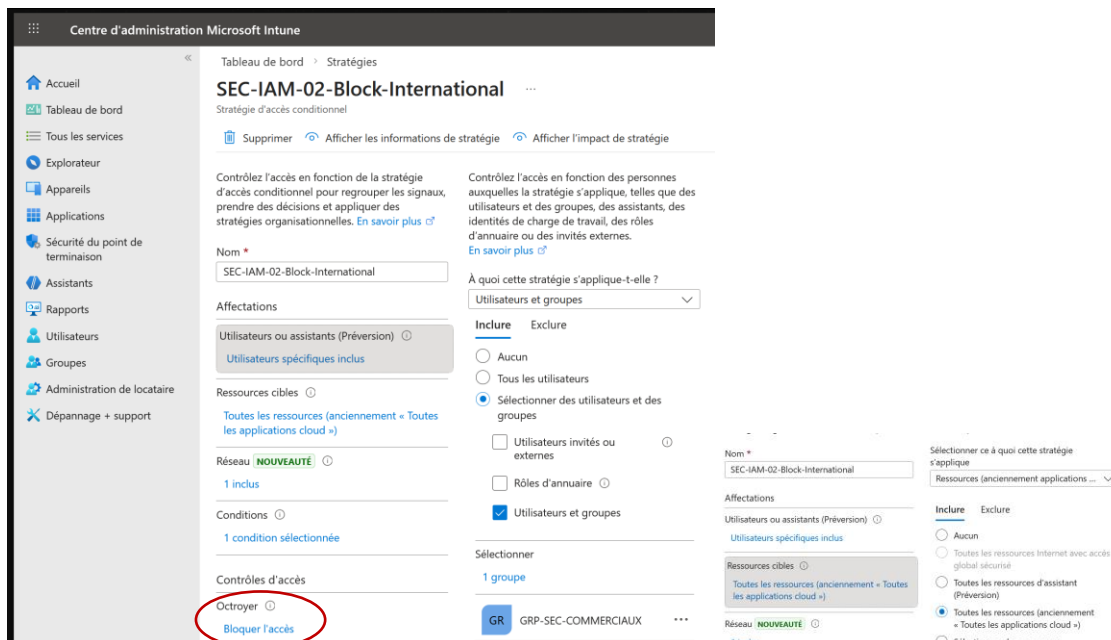
The screenshot displays the Microsoft Intune 'Centre d'administration' interface for configuring a Conditional Access policy named 'SEC-IAM-01-MFA-Finance'. The left sidebar shows navigation options like 'Accueil', 'Tableau de bord', 'Explorateur', and 'Sécurité du point de terminaison'. The main content area is divided into several sections:

- Nom**: SEC-IAM-01-MFA-Finance
- Affectations**: 'Utilisateurs ou assistants (Préversion)' with 'Utilisateurs spécifiques inclus' selected.
- Ressources cibles**: 'Toutes les ressources (anciennement « Toutes les applications cloud »)'.
- Réseau**: 'NOUVEAUTÉ' with 'Non configuré'.
- Conditions**: '0 conditions sélectionnées'.
- Contrôles d'accès**: 'Octroyer' with '1 contrôle sélectionné'.
- Session**: '0 contrôles sélectionnés'.

On the right, the 'À quoi cette stratégie s'applique-t-elle ?' section is expanded, showing 'Inclure' and 'Exclure' options. Under 'Inclure', 'Sélectionner des utilisateurs et des groupes' is selected, and a list shows '1 groupe' (GRP-SEC-FINANCE). Below this, 'Sélectionner ce à quoi cette stratégie s'applique' is set to 'Ressources (anciennement applications ...)'. The 'Inclure' section also lists options like 'Aucun', 'Toutes les ressources Internet avec accès global sécurisé', 'Toutes les ressources d'assistant (Préversion)', 'Toutes les ressources (anciennement « Toutes les applications cloud »)', and 'Sélectionner des ressources'.

An 'Octroyer' (Grant) dialog box is open on the right, showing options to 'Bloquer l'accès' or 'Accorder l'accès' (selected). It also includes a checkbox for 'Exiger une authentification multifacteur' (checked).

Blocage International : Restriction des accès basée sur la géolocalisation

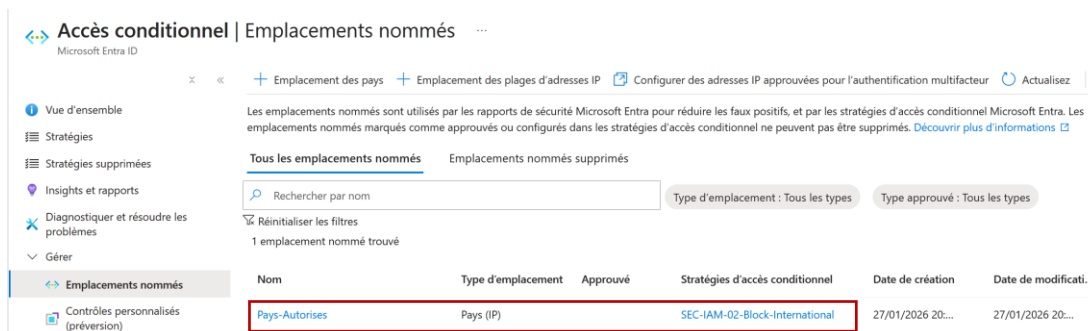


Cette configuration a pour but :

- **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

The screenshot displays the Microsoft Intune admin center interface. On the left, the navigation pane shows the 'Stratégies' (Policies) section. The main area shows the configuration for the 'SEC-IAM-03-Admin-MFA-Compliance' policy. The 'Affectations' (Assignments) section shows it is assigned to 'Utilisateurs ou assistants (Préversion)' and 'Utilisateurs spécifiques inclus'. The 'Ressources cibles' (Target resources) section shows it applies to 'Toutes les ressources (anciennement « Toutes les applications cloud »)'. The 'Conditions' (Conditions) section shows '1 condition sélectionnée'. The 'Contrôles d'accès' (Access controls) section shows '2 contrôles sélectionnés'. The 'Octroyer' (Grant) section on the right shows the policy is configured to 'Accorder l'accès' (Grant access) and requires 'Exiger une authentification multifactor' (Require multi-factor authentication) and 'Exiger que l'appareil soit marqué comme conforme' (Require the device to be marked as compliant). The 'Octroyer' section also includes a warning: 'Exiger la force de l'authentification' (Require the strength of authentication) cannot be used with 'Exiger une authentification multifactor' (Require multi-factor authentication).

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

- **L'authentification multifactor (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.

Centre d'administration Microsoft Intune

Accueil

W10-11-SEC-COMPLIANCE-ADMINS ...

Stratégie de conformité - Windows 10 et ultérieur

Supprimer

Monitorer **Propriétés**

Informations de base [Modifier](#)

Nom: W10-11-SEC-COMPLIANCE-ADMINS

Description: --

Plateforme: Windows 10 and later

Type de profil: Stratégie de conformité Windows 10/11

Paramètres de conformité [Modifier](#)

Intégrité de l'appareil

BitLocker	Obligatoire
Démarrage sécurisé	Obligatoire

Sécurité système

Exiger le chiffrement du stockage des données sur l'appareil	Obligatoire
--	-------------

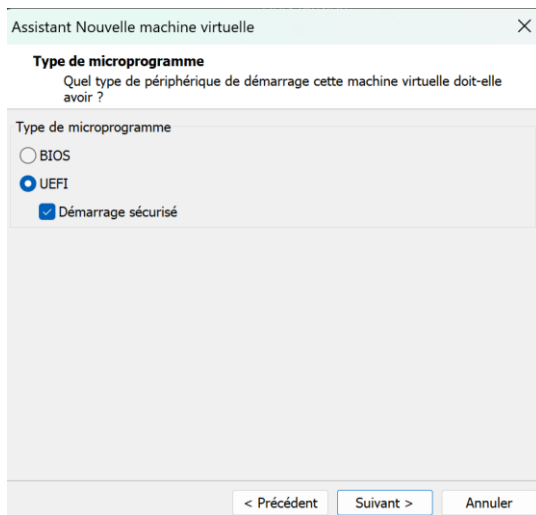
Sécurité de l'appareil

Exiger un mot de passe pour déverrouiller les appareils mobiles	Obligatoire
---	-------------

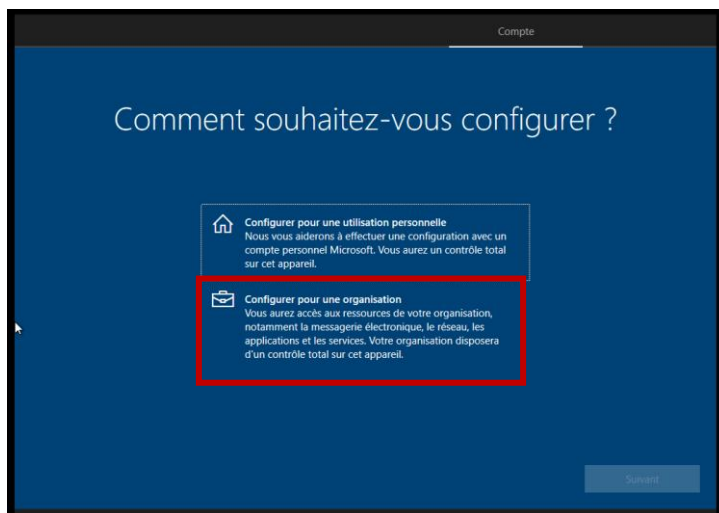
4. Déploiement

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

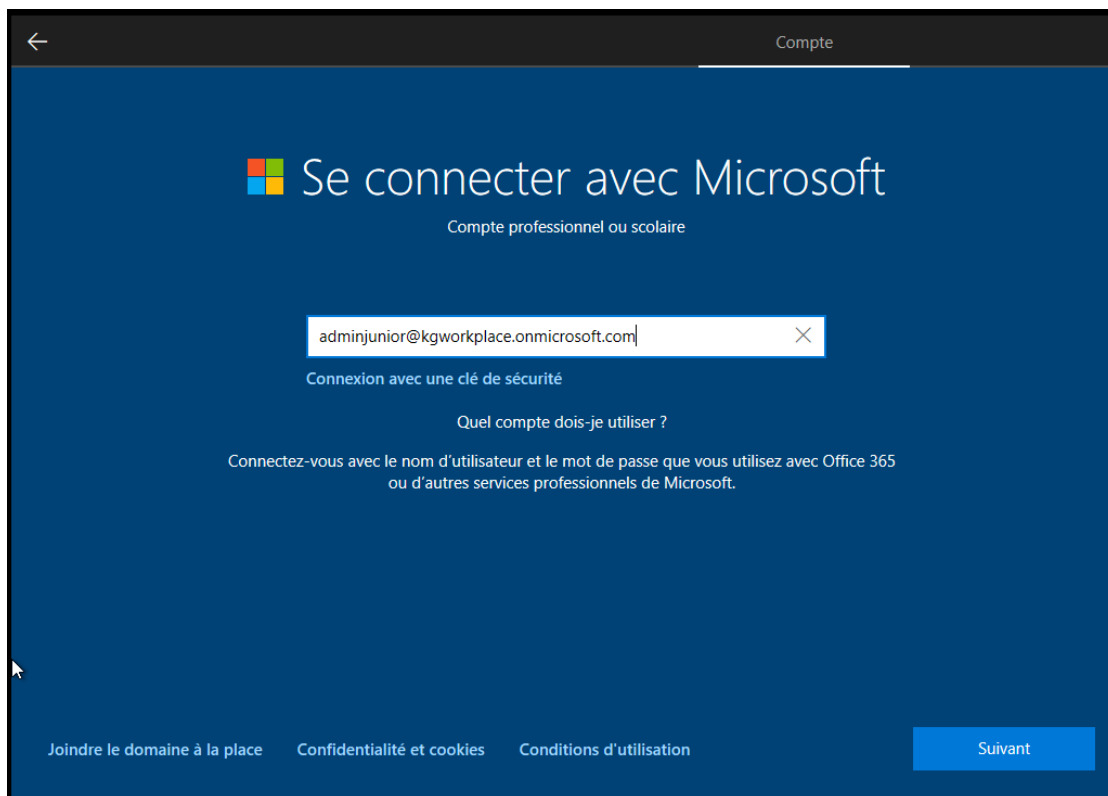
Configuration UEFI/TPM : Pour satisfaire aux exigences de BitLocker, le microprogramme de la VM a été configuré en **UEFI** avec l'activation du **Démarrage sécurisé** (Secure Boot).



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**



The image shows a Microsoft login interface with a dark blue background. At the top, there is a navigation bar with a back arrow on the left and the word 'Compte' on the right. The main heading is 'Se connecter avec Microsoft' with the Microsoft logo to its left. Below this, it says 'Compte professionnel ou scolaire'. A text input field contains the email 'adminjunior@kgworkplace.onmicrosoft.com' with a clear button (X) on the right. Below the input field, it says 'Connexion avec une clé de sécurité'. Then, it asks 'Quel compte dois-je utiliser ?' and provides instructions: 'Connectez-vous avec le nom d'utilisateur et le mot de passe que vous utilisez avec Office 365 ou d'autres services professionnels de Microsoft.' At the bottom, there are four links: 'Joindre le domaine à la place', 'Confidentialité et cookies', 'Conditions d'utilisation', and a blue 'Suivant' button.

← Compte

 Se connecter avec Microsoft

Compte professionnel ou scolaire

X

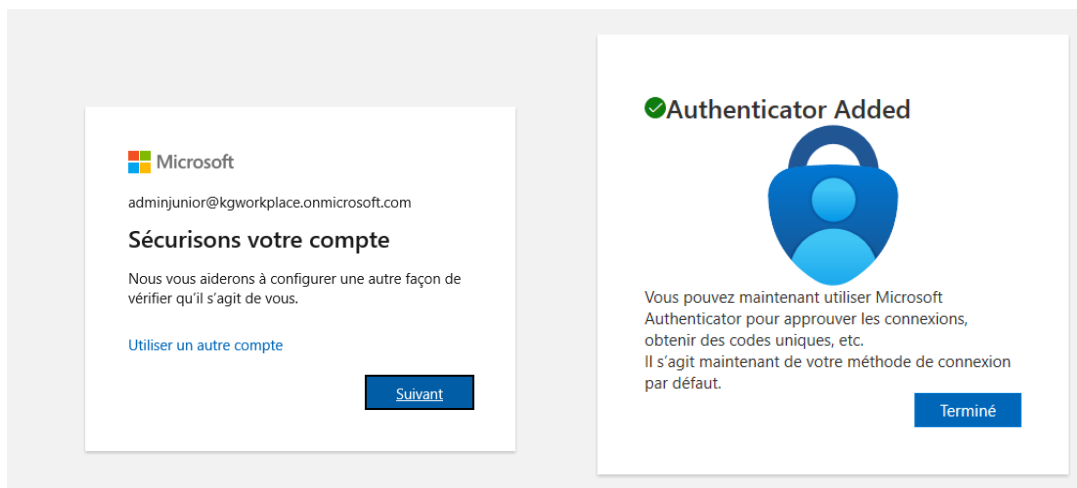
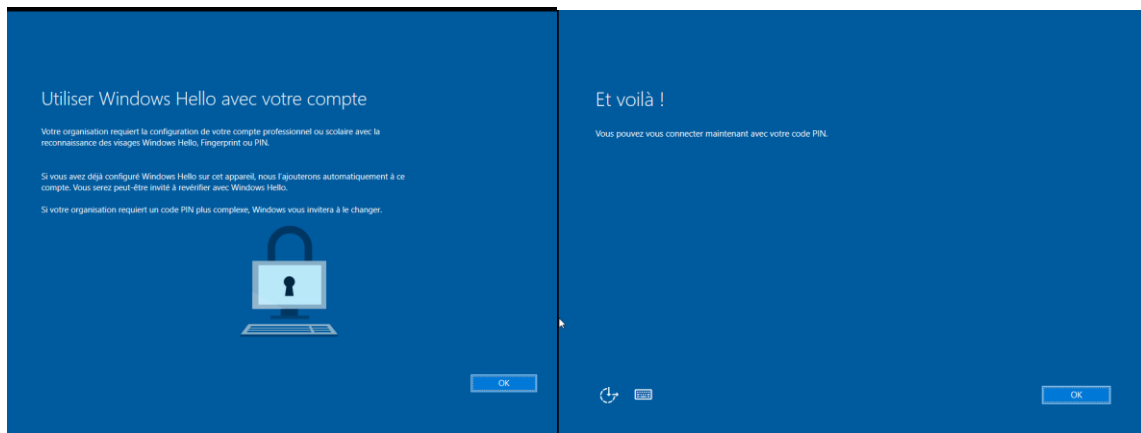
Connexion avec une clé de sécurité

Quel compte dois-je utiliser ?

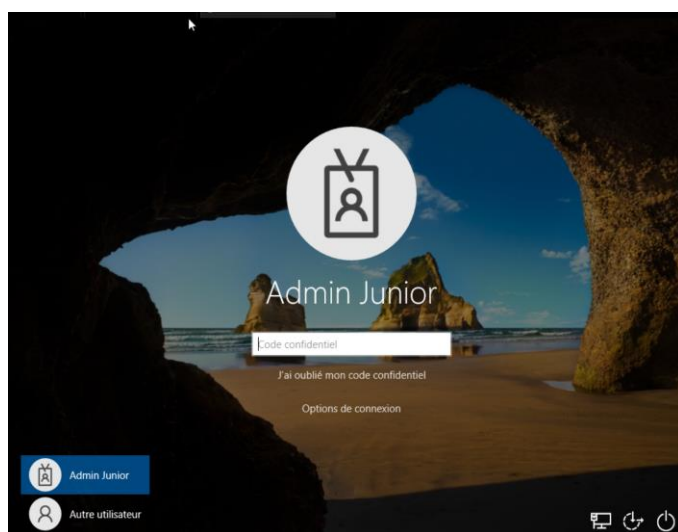
Connectez-vous avec le nom d'utilisateur et le mot de passe que vous utilisez avec Office 365 ou d'autres services professionnels de Microsoft.

[Joindre le domaine à la place](#) [Confidentialité et cookies](#) [Conditions d'utilisation](#) [Suivant](#)

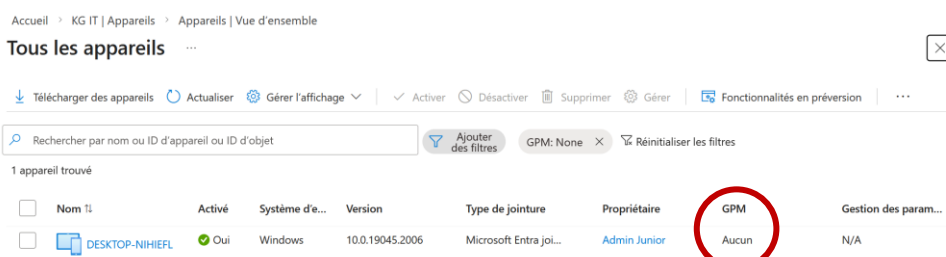
Authentification Forte : L'utilisateur a configuré son compte via l'application **Microsoft Authenticator** et a défini un code PIN Windows Hello pour une connexion sécurisée



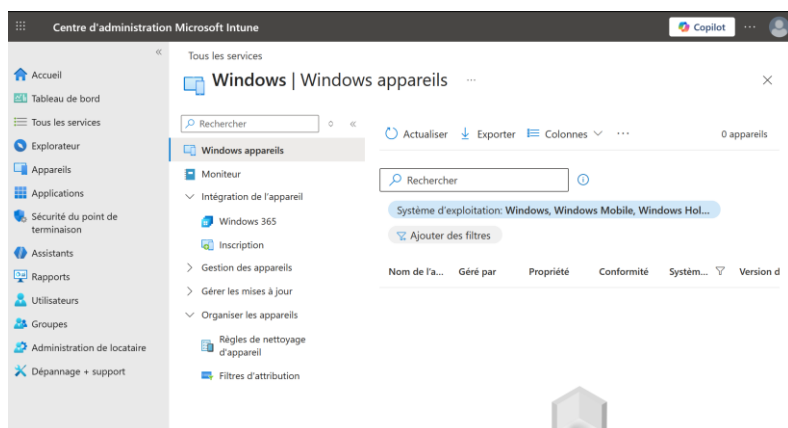
L'utilisateur "Admin Junior" peut maintenant accéder à sa session



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

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 ⓘ

URL de découverte Gestion des données de référence ⓘ

URL de conformité Gestion des données de référence ⓘ

[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 ⓘ

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

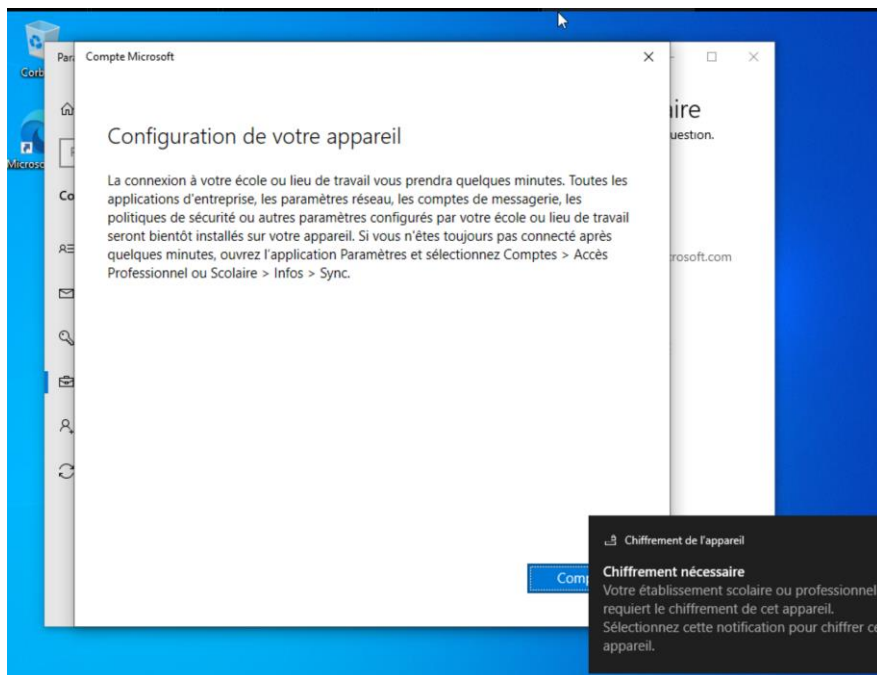
Abandonner

Supprimer

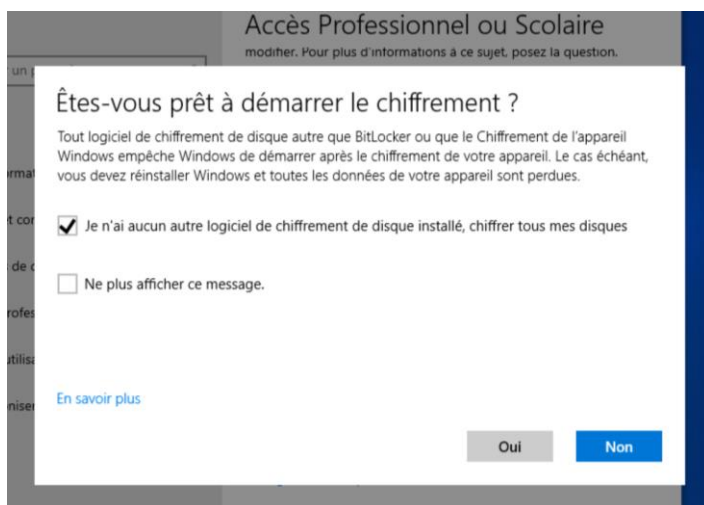
*Note technique : En entreprise, ce réglage est généralement positionné sur '**Partiel**' afin de limiter l' enrôlement à un groupe de test (Pilote) et de maîtriser l' impact du déploiement sur le parc informatique*

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.

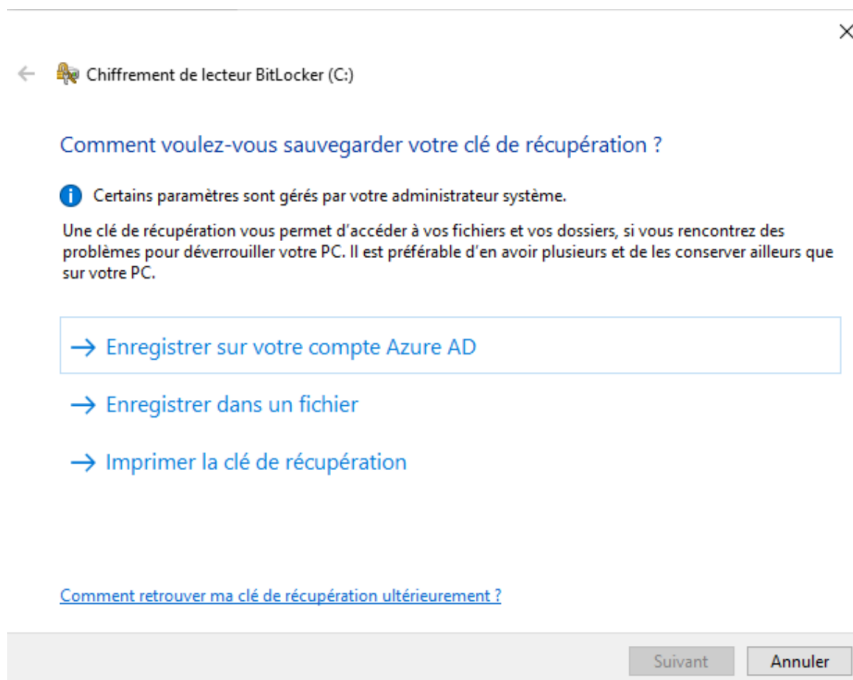
Constat immédiat sur le poste de travail : Dès la connexion du compte professionnel, nous pouvons confirmer que l'enrôlement a réussi grâce à la notification de demande de chiffrement



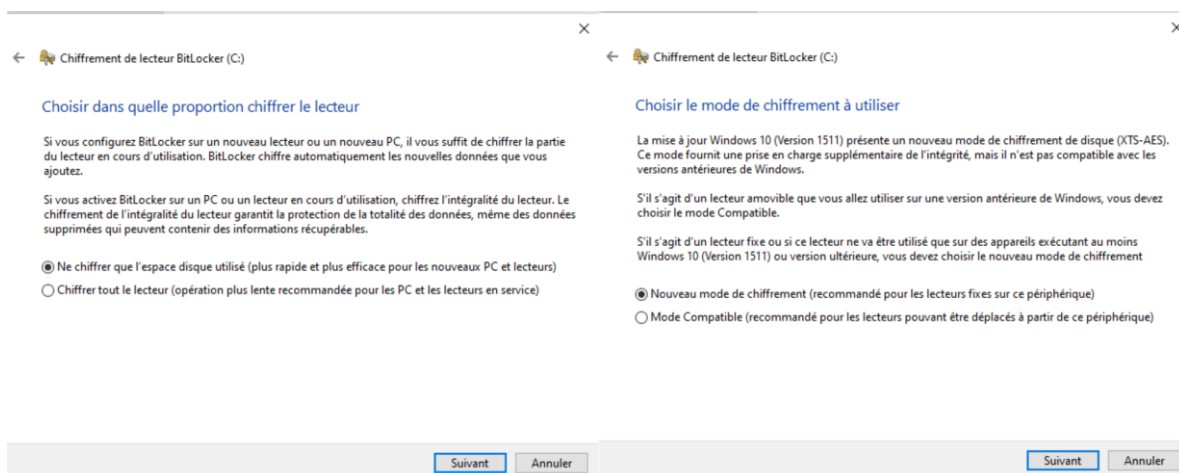
Suite à la notification de chiffrement, le processus de mise en conformité est lancé. Ces captures montrent les étapes critiques du chiffrement :



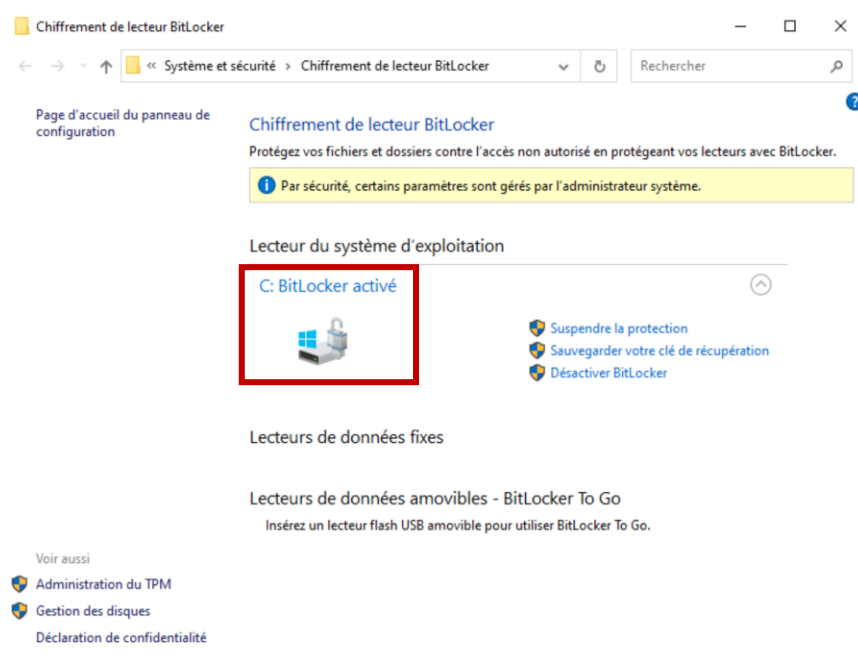
J'ai sélectionné l'option "**Enregistrer dans votre compte Azure AD**" pour ne pas perdre l'accès aux données en cas d'oubli de mot de passe.



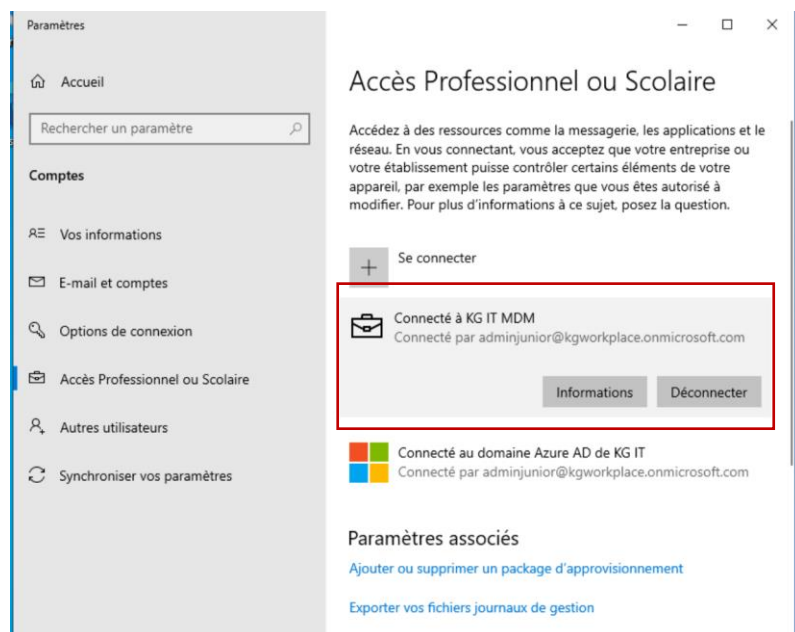
Méthode de chiffrement : J'ai choisi de chiffrer "l'espace disque utilisé uniquement" pour plus de rapidité dans ce lab, tout en garantissant la sécurité des données existantes.



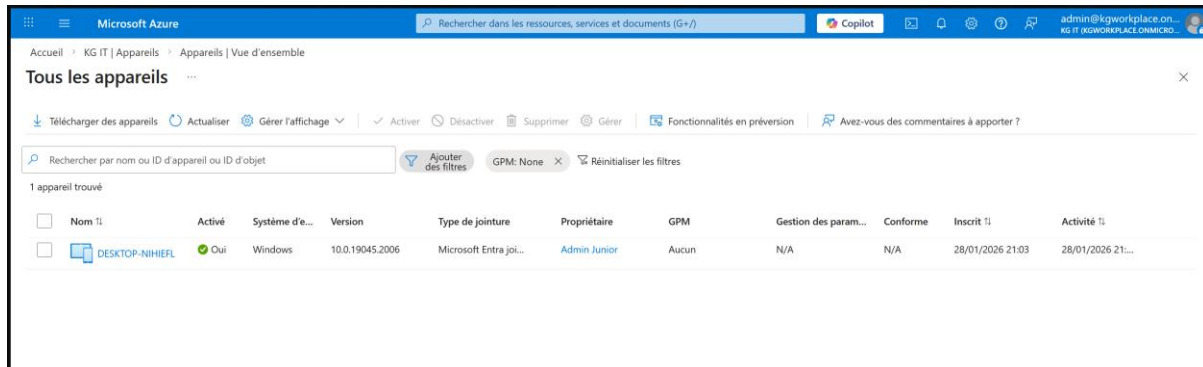
Dans le Panneau de configuration, le lecteur système affiche désormais explicitement le statut "**C: BitLocker activé**"



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.

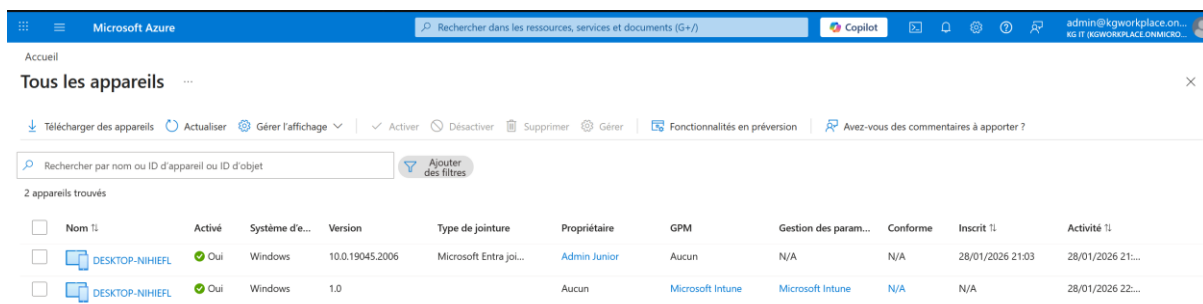


L'état initial (Ligne 1) : On observe l'appareil DESKTOP-NIHIEFL avec un statut **"GPM : Aucun"**. À ce stade, le PC est bien inscrit dans l'annuaire (Microsoft Entra joined), mais il n'est pas encore piloté par Intune. C'est pour cette raison qu'il n'apparaissait pas initialement dans la console de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



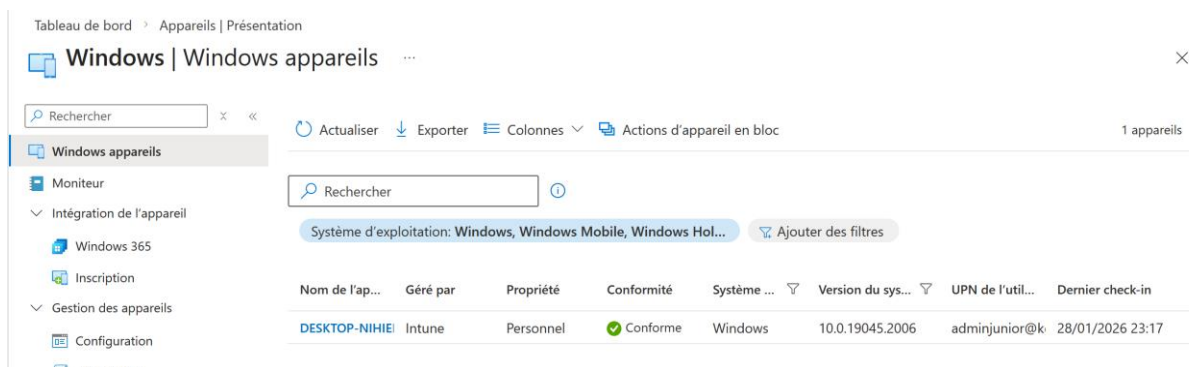
Nom	Activé	Système d'e...	Version	Type de jointure	Propriétaire	GPM	Gestion des param...	Conforme	Inscrit	Activité
DESKTOP-NIHIEFL	Oui	Windows	10.0.19045.2006	Microsoft Entra joi...	Admin Junior	Aucun	N/A	N/A	28/01/2026 21:03	28/01/2026 21:...

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 joi...	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	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.



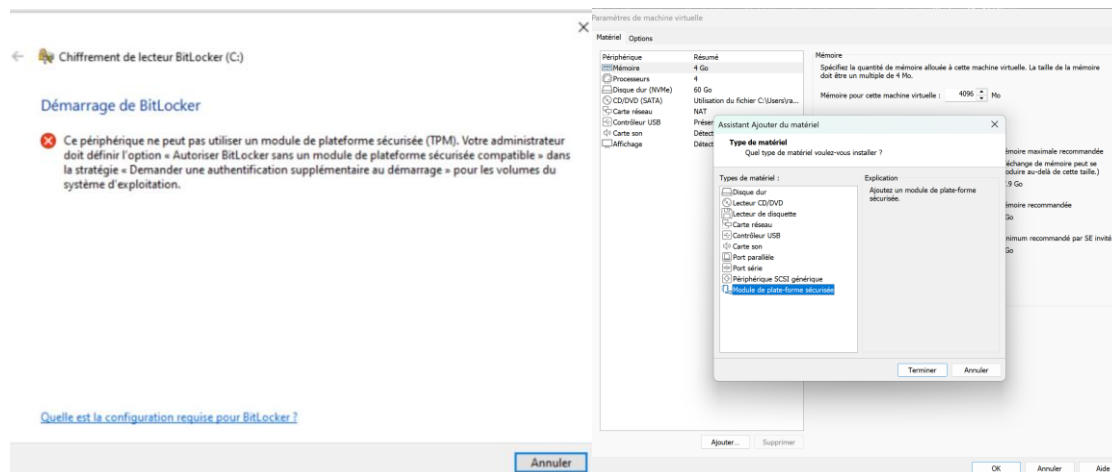
Nom de l'appareil	Géré par	Propriété	Conformité	Système d'exploitation	Version du système d'exploitation	UPN de l'utilisateur	Dernier check-in
DESKTOP-NIHIEFL	Intune	Personnel	Conforme	Windows	10.0.19045.2006	adminjunior@k...	28/01/2026 23:17

Challenges techniques rencontrés

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

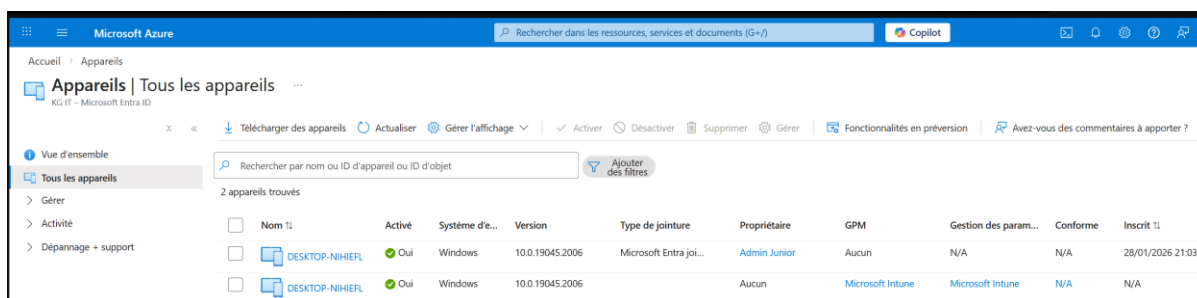
- **Symptôme** : Lors de l'enrôlement, l'appareil restait en état "Non conforme" et le chiffrement ne se lançait pas.
- **Analyse** : Le diagnostic a révélé l'absence de puce TPM et un démarrage en mode BIOS Legacy, incompatibles avec les exigences de sécurité modernes.
- **Résolution** : Intervention 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.



Microsoft Azure										
Rechercher dans les ressources, services et documents (G+/I)										
Copilot										
Accueil > Appareils										
Appareils Tous les appareils										
KG IT - Microsoft Entra ID										
Télécharger des appareils Actualiser Gérer l'affichage Activer Désactiver Supprimer Gérer Fonctionnalités en prévision Avez-vous des commentaires à apporter ?										
Vue d'ensemble										
Tous les appareils										
Rechercher par nom ou ID d'appareil ou ID d'objet										
Ajouter des filtres										
2 appareils trouvés										
<input type="checkbox"/>	Nom TI	Activé	Système d'e...	Version	Type de jointure	Propriétaire	GPM	Gestion des param...	Conforme	Inscrit TI
<input type="checkbox"/>	DESKTOP-NHIEFL	Oui	Windows	10.0.19045.2006	Microsoft Entra joi...	Admin Junior	Aucun	N/A	N/A	28/01/2026 21:03
<input type="checkbox"/>	DESKTOP-NHIEFL	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.