

Déploiement Microsoft Intune + Defender for Business

Contexte : ~50 postes Windows, licences Microsoft 365 Business Premium, hybrid Entra join (sync AD → Entra ID), objectif gestion des postes + sécurisation renforcée.

1. Prérequis Entra

- Vérifier qu'Entra Connect est en place et que la synchro fonctionne (objets device synchronisés).
- Configurer le hybrid Entra join (voir détail §1.1).
- Vérifier que les postes remontent bien en *Hybrid Azure AD joined* via `dsregcmd /status`.
- S'assurer que les utilisateurs ont la licence Intune (incluse dans Business Premium) assignée.

1.1 Configurer le hybrid Entra join

Objectif : faire en sorte que les postes joints au domaine AD on-prem s'enregistrent automatiquement comme devices dans Entra ID.

Côté Entra Connect

1. Lancer **Microsoft Entra Connect** sur le serveur de synchro.
2. Choisir **Configure** → **Configure device options** → **Next**.
3. S'authentifier avec un compte Hybrid Identity Administrator (Entra).
4. Sélectionner **Configure Hybrid Azure AD join** → **Next**.
5. **Device operating systems** : cocher **Windows 10 or later domain-joined devices**.
6. **SCP configuration** (Service Connection Point) : sélectionner la forêt AD, choisir l'authentification service **Azure Active Directory**, et renseigner un compte Enterprise Admin pour écrire le SCP dans le Configuration Naming Context.
7. Valider → **Configure**.

<note>Le SCP peut aussi être écrit manuellement par script PowerShell si on ne veut pas donner les droits Enterprise Admin à Entra Connect.</note>

Côté GPO (déclenche l'enregistrement sur les postes)

1. Ouvrir la **Group Policy Management Console**.
2. Créer / éditer une GPO liée à l'OU des postes.
3. Chemin : **Computer Configuration** → **Politiques** → **Administrative Templates** → **Windows Components** → **Device Registration**.
4. Activer : **Register domain-joined computers as devices** → **Enabled**.
5. Appliquer la GPO (`gpupdate /force` sur un poste de test).

Vérification

- Sur un poste cible : `dsregcmd /status`
- Contrôler que **AzureAdJoined : YES** et **DomainJoined : YES**.
- Le device apparaît dans **Entra admin center → Devices**, Join Type = *Hybrid Azure AD joined*.

<note important>L'enregistrement peut prendre un certain temps (tâche planifiée Automatic-Device-Join au prochain logon / redémarrage). Compter jusqu'à ~30 min voire plusieurs heures de propagation à l'échelle du parc.</note>

2. Enrollment Intune (MDM)

2.1 Activer l'auto-enrollment MDM

Objectif : une fois le poste hybrid joined, il s'inscrit automatiquement dans Intune sans action manuelle.

Prérequis dans Entra

1. **Entra admin center → Mobility (MDM and MAM) → Microsoft Intune.**
2. **MDM user scope** : régler sur **All** (ou **Some** + groupe pilote pour un déploiement progressif).
3. Laisser les URLs par défaut (Terms of use, Discovery, Compliance).

Méthode A — via GPO (recommandée en hybrid join)

1. Ouvrir / éditer une GPO liée à l'OU des postes.
2. Chemin : **Computer Configuration → Policies → Administrative Templates → Windows Components → MDM.**
3. Activer : **Enable automatic MDM enrollment using default Azure AD credentials → Enabled.**
4. Option **Select Credential Type to Use** : choisir **User Credential**.
5. Appliquer la GPO.

<note>Prérequis : les ADMX récents (Windows 10 1803+ / Windows 11) doivent être présents dans le Central Store pour que le paramètre apparaisse.</note>

Méthode B — via la config Entra (MDM user scope)

Si on ne passe pas par GPO, le simple fait d'avoir **MDM user scope = All** (§2.1) suffit : une tâche planifiée déclenche l'enrollment automatiquement sur les postes hybrid joined dont l'utilisateur est licencié Intune.

<note important>Ne pas combiner les deux méthodes de façon incohérente. En pratique, le MDM user scope = All est le socle, et la GPO force/fiabilise le déclenchement. Choisir une approche claire et la documenter.</note>

Vérification

- `dsregcmd /status` → section *MDM URLs* renseignée, **MdmUrl** présent.
- Le poste apparaît dans **Intune admin center** → **Devices** → **Windows** avec un statut *Managed*.
- Observer l'Event Viewer : Applications and Services Logs → Microsoft → Windows → DeviceManagement-Enterprise-Diagnostics-Provider.

3. Gestion des postes

- Créer des **groupes dynamiques** Entra (par device et/ou par user) pour le ciblage.
- **Configuration profiles** : baselines, BitLocker, Windows Update for Business (rings de mise à jour), Wi-Fi / VPN si nécessaire.
- **Déploiement d'applications** : Win32 (via Intune Management Extension), Microsoft Store, Office/M365 Apps via policy de configuration.

4. Sécurisation — Defender for Business

- Onboarding automatique via Intune une fois les postes enrôlés (connecteur MDE ↔ Intune activé).
- Appliquer les **Security Baselines** (Defender + Windows).
- Configurer les **ASR rules** (Attack Surface Reduction) → **commencer en mode Audit** avant de passer en Block.
- Mettre en place les **Compliance policies** + **Conditional Access** (bloquer l'accès si poste non conforme).

Points d'attention transverses

- **Éviter le double management** GPO vs Intune sur les mêmes paramètres → décider qui pilote quoi pour éviter les conflits.
- **ASR en audit d'abord** pour ne pas casser les applications métier.
- **Conditional Access** : prévoir un compte **break-glass** exclu de toutes les politiques.

From:
<http://wiki.makeitsimple.be/> - makeITsimple wiki

Permanent link:
<http://wiki.makeitsimple.be/doku.php?id=windows:defender-for-business>

Last update: 2026/10/19 09:22

