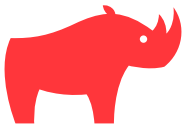
Synapsys

LIVRE BLANC

Gérer ses appareils Windows avec Intune

Simplifier, sécuriser, maîtriser



À l'ère où les environnements de travail hybrides deviennent la norme notamment avec le télétravail, les entreprises sont confrontées à des défis croissants pour garantir la sécurité, la flexibilité et l'efficacité dans leur gestion des périphériques Windows. Microsoft Intune, le MDM de Microsoft, permet aux organisations de relever ces défis tout en favorisant la productivité des utilisateurs.

Ce livre blanc examine les apports stratégiques et opérationnels d'une gestion des appareils Windows via Intune. Il présente les principales fonctionnalités, les configurations recommandées et plusieurs cas d'usage concrets, afin de fournir un cadre de référence applicable aux environnements professionnels modernes.

Synapsys

Sommaire

Introduction sur Intune

Microsoft Intune est une solution de gestion des appareils basée sur le cloud. Cette solution offre la possibilité de gérer les différents appareils amenés à se connecter aux ressources de votre entreprise, **qu'il s'agisse de postes de travail, de smartphones, de tablettes…**

Microsoft Intune prend en charge les systèmes d'exploitation suivant : Windows, MacOS, Linux, Chrome OS pour la partie « **Poste de travail** » et Android, iOS pour la partie « **Mobilité** ».

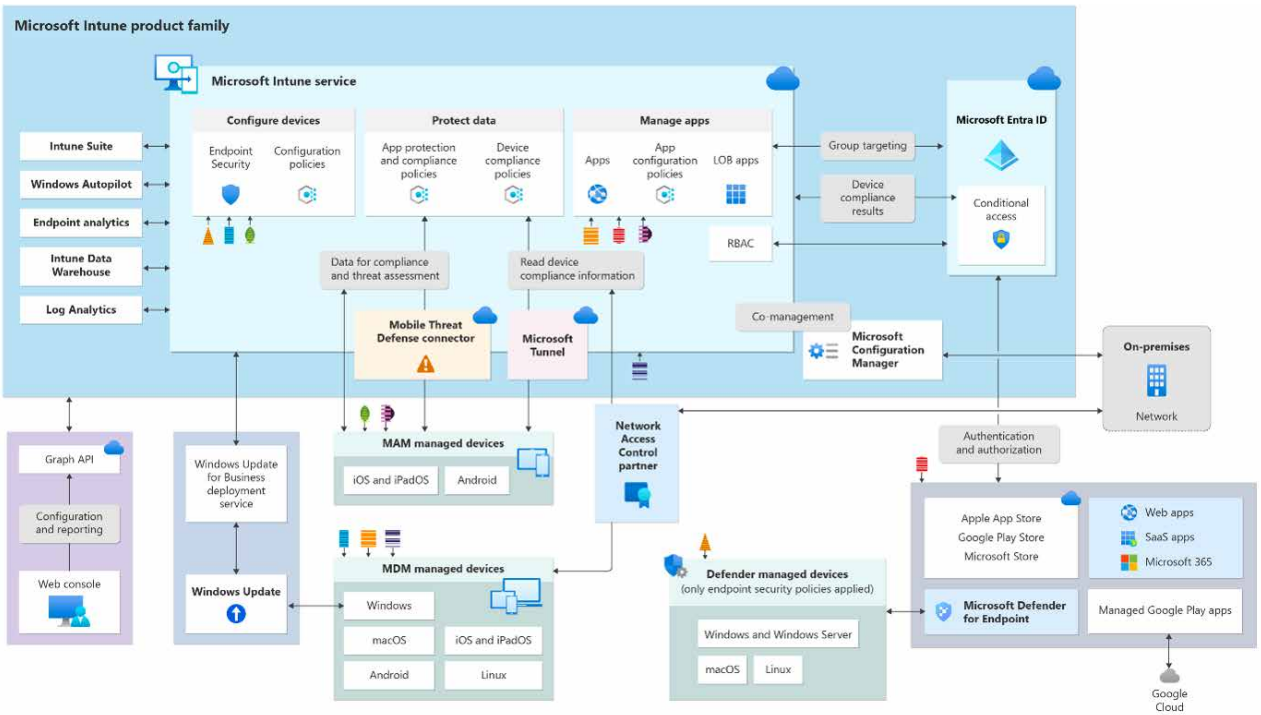
A travers ces OS, différents types de gestion sont possibles et les capacités varient d'un OS à un autre. Nous verrons dans ce livre blanc par exemple la capacité d'Intune à gérer des kiosques sous Windows.

Voici un schéma explicatif (source : *Microsoft*) du périmètre couvert par la solution Intune :

Microsoft Intune s'inscrit dans l'esprit du « **Modern Device Management** » où les appareils de l'entreprise sont pris en considération tout comme les appareils personnels (principe du BYOD), et le fait que l'utilisateur est susceptible de travailler depuis n'importe quel emplacement.

Pour finir, Microsoft Intune est capable de s'associer à **Configuration Manager** en mode co-gestion pour combiner l'utilisation des deux outils et ainsi entamer sa migration vers le Modern Management.

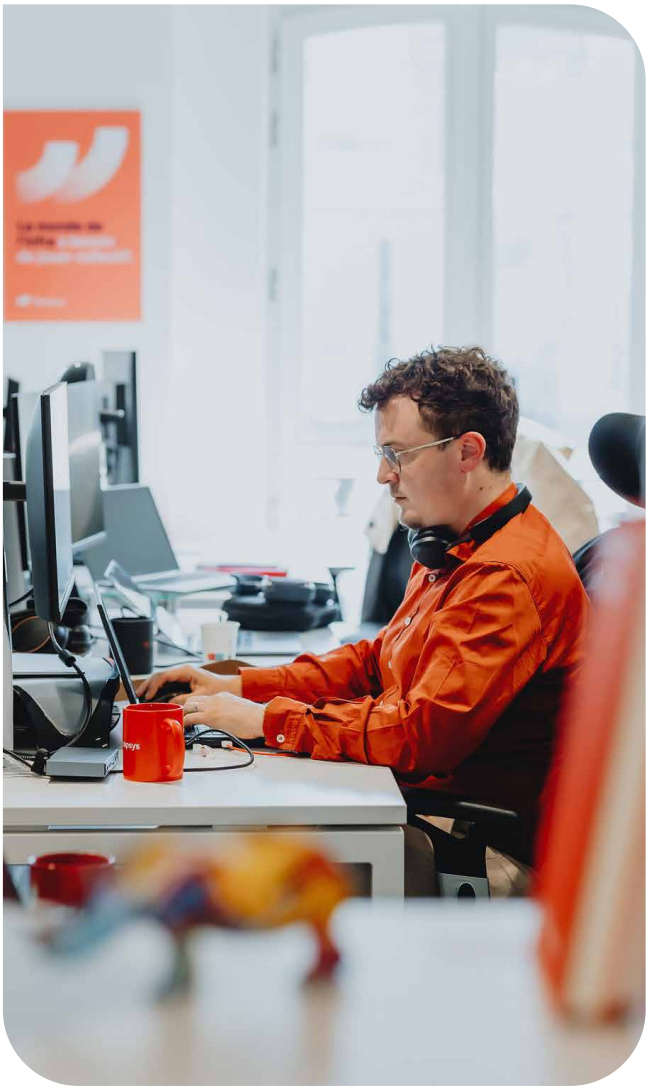
Voici un panorama des fonctionnalités et connexion possibles avec Microsoft Intune (source : *Microsoft*) :



Fonctionnement du licensing

Microsoft Intune est intégré dans plusieurs bundle de licences Microsoft 365 comme :

- Microsoft 365 E5
- Microsoft 365 E3
- Enterprise Mobility + Security E5
- Enterprise Mobility + Security E3
- Microsoft 365 Business Premium
- Microsoft 365 F1
- Microsoft 365 F3



Dans les environnements ne disposant pas de licences Microsoft 365 — notamment lorsqu'une autre suite collaborative est utilisée — l'abonnement à des licences Intune Plan 1 Utilisateur ou Intune Device reste possible.

Les licences Intune Device sont particulièrement adaptées aux scénarios de périphériques partagés (shared devices) ou de fonctionnement en mode Kiosk.

Méthodes d'enrôlement Windows avec Intune

Afin de pouvoir gérer un poste de travail Windows avec Microsoft Intune, ce dernier doit être **enrôlé** dans cette solution de gestion. Avant tout et selon s'il s'agit d'un appareil d'entreprise ou un appareil personnel, **l'appareil doit être joint à Entra ID.**

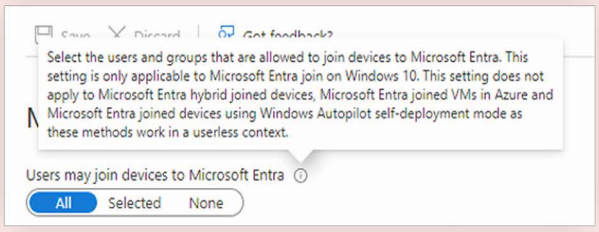
Il existe plusieurs modes d'inscriptions disponibles pour cela :

- **Microsoft Entra Registered** : pour les postes de travail personnels (BYOD).
- **Microsoft Entra Joined** : pour les postes de travail corporate intégré directement dans Microsoft Entra ID et inscrit dans Intune.
- **Microsoft Entra Hybrid Joined** : pour les postes de travail corporate, intégré dans l'Active Directory (on-premise) et synchronisé dans Microsoft Entra ID, puis inscrit dans Intune.

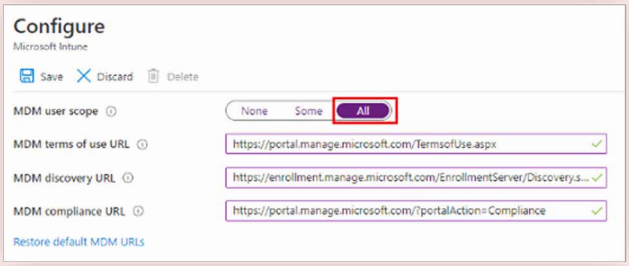
Microsoft Intune s'adapte aussi bien aux environnements entièrement cloud, où les appareils sont intégrés à Microsoft Entra ID, qu'aux **configurations hybrides** exploitant une infrastructure existante Active Directory. L'implémentation variera en fonction de la configuration initiale de votre environnement.

Avant d'inscrire les postes de travail dans Microsoft Intune, quelques pré requis techniques sous Entra ID sont à mettre en place comme :

Paramètres de jointure à Microsoft Entra



Étendue de l'utilisateur GPM :



Il est recommandé de mettre en place du hardening sur ces 2 paramétrages en utilisant plutôt « Selected » et « Some » en scopant avec un groupe Entra ID.

Méthodes d'enrôlement les plus couramment utilisées

Ce tableau présente un comparatif des principales méthodes d'enrôlement des postes dans un environnement Microsoft, en mettant en lumière **trois critères clés** : le type de propriété de l'appareil, l'affinité utilisateur et le niveau d'interaction nécessaire de l'utilisateur.

Méthode d'enrôlement	Ownership	User affinity	User interaction
Entra ID join avec auto enrollment	Corporate	Oui	Oui
Windows Autopilot	Corporate	Oui / Non	Oui / Non
Provisionning package (PPKG)	Corporate	Non	Non
Co-management (SCCM)	Corporate	Oui	Non
Group Policy (AD)	Corporate	Oui	Non

Entra ID join avec auto-enrôlement

Cette méthode consiste à rattacher l'appareil directement à Entra ID, avec un enrôlement automatique dans Intune. Elle est idéale pour les appareils d'entreprise. L'utilisateur est associé à l'appareil (user affinity) et une interaction est requise lors de la configuration initiale.

Windows Autopilot

Windows Autopilot permet de préconfigurer les appareils pour une mise en service rapide et personnalisée. Il s'applique aux appareils d'entreprise, avec ou sans affinité utilisateur selon le scénario choisi (mode self-deploying ou mode user-driven). L'interaction utilisateur est variable, pouvant aller d'aucune à une participation active.

Provisioning Package (PPKG)

Les packages de provisioning sont utilisés pour configurer rapidement un appareil via un fichier préparamétré. Cette méthode est adaptée aux appareils d'entreprise, sans affinité utilisateur, et sans interaction requise lors du déploiement.

Co-management (SCCM)

Le co-management permet de gérer un appareil à la fois avec SCCM et Intune. L'appareil reste sous propriété de l'entreprise, avec affinité utilisateur, mais sans interaction directe de l'utilisateur pour l'enrôlement si la configuration est automatisée.

Group Policy (GPO via Active Directory)

L'enrôlement via stratégie de groupe est une méthode classique dans les environnements Active Directory. Elle concerne uniquement les appareils d'entreprise, avec une affinité utilisateur, et ne nécessite aucune interaction manuelle de la part de l'utilisateur.

Le rôle d'Autopilot

Avantages d'Autopilot

Windows Autopilot permet de configurer ou de préconfigurer de nouveaux appareils Windows au sein d'un environnement d'entreprise. Il peut également être utilisé pour réinitialiser ou réaffecter des appareils existants à l'aide d'un processus automatisé, rapide et simplifié.

Les avantages proposés par Autopilot sont multiples :

- **La réduction du temps** pour effectuer le déploiement des appareils.
- **L'optimisation des ressources** pour la gestion des appareils, en limitant le support nécessaire.
- **L'amélioration de l'expérience utilisateur** grâce au processus de configuration simplifié.

Autopilot ne constitue pas une solution de déploiement d'OS à proprement parler, comme c'est le cas avec OSD dans SCCM. Il repose sur le **système d'exploitation préinstallé** par le constructeur pour transformer l'appareil en un poste prêt à l'usage en entreprise (Corporate Ready). Certains fabricants, comme HP, proposent des images système allégées de type corporate-ready, exemptes de logiciels indésirables.

L'installation d'un OS de base reste possible via une clé USB utilisant une image ISO officielle de Microsoft, ou à l'aide de solutions alternatives comme OSD Cloud.

L'utilisation d'**Autopilot** nécessite une licence complémentaire à Intune, notamment une licence Entra ID P1.

Pour plus d'informations, c'est par ici.

Fonctionnement d'Autopilot

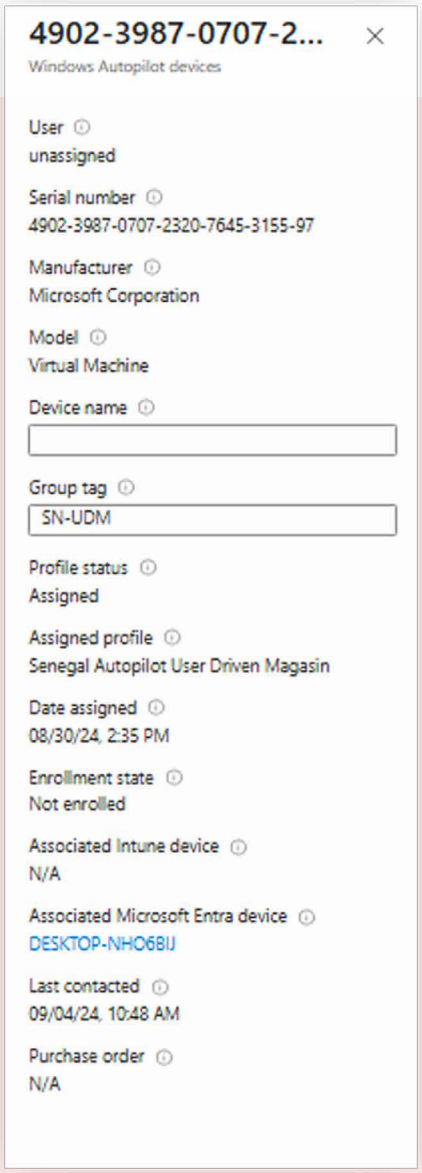
Le processus commence par **l'enregistrement de l'appareil** dans le service cloud **Autopilot** via un script Powershell. D'autres méthodes automatisées sont également disponibles (facilement trouvables sur Internet). Cette étape, réalisée par l'équipe informatique, permet également d'attribuer un « Groupe Tag » (par exemple, par BU ou par service) à chaque appareil.

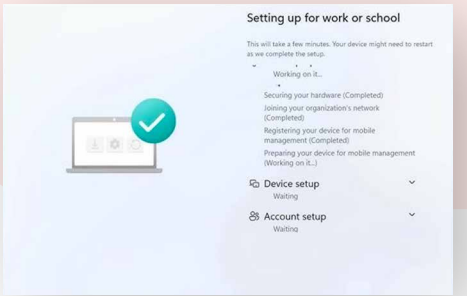
Une fois l'appareil enregistré, il est automatiquement ajouté à un groupe dynamique dans Azure AD, basé sur ce tag. Il est également possible dans un scénario « **Entra ID Join** » d'affecter directement l'utilisateur et le hostname de l'appareil.

Pour l'utilisateur final, l'expérience commence par l'authentification sur un appareil neuf ou réinitialisé. L'appareil télécharge et applique automatiquement les configurations et les applications définies par l'IT via Intune.
Cette étape, appelée « **Enrollment Status Page** » (ESP) peut durer d'une à deux heures, en fonction des applications et configurations à installer.
Grâce au tag appliqué un peu plus haut, il est possible de faire appliquer des configurations différentes ou faire installer des applications différentes selon celui-ci.

Il est également possible de définir des **applications obligatoires**, comme l'installation d'un antivirus ou autre logiciel avant que l'utilisateur ne puisse accéder au bureau.
L'objectif étant que l'utilisateur accède à son poste une fois que tous les logiciels critiques et nécessaires sont installés.

Il sera également possible prochainement de faire en sorte d'installer les derniers patches de sécurité Windows pendant le process Autopilot.





Scénarios Autopilot

Windows Autopilot prend en charge une liste de scénarios qui couvre généralement tous les besoins que peut avoir une organisation. En voici un résumé :

	Scénarios	Description
1	Windows Autopilot user-driven mode	Déploiement et configuration de l'appareil par l'utilisateur final
2	Windows Autopilot self-deploying mode	Déploiement et configuration automatique pour une utilisation partagée, en tant que kiosque par exemple
3	Windows Autopilot reset	Redéploiement d'un appareil dans un état prêt pour l'entreprise
4	Pre-provisionning	Provisionnement d'un appareil avec des applications, des stratégies et des paramètres à jour
5	Windows Autopilot for existing devices	Déploiement sur un appareil Windows existant

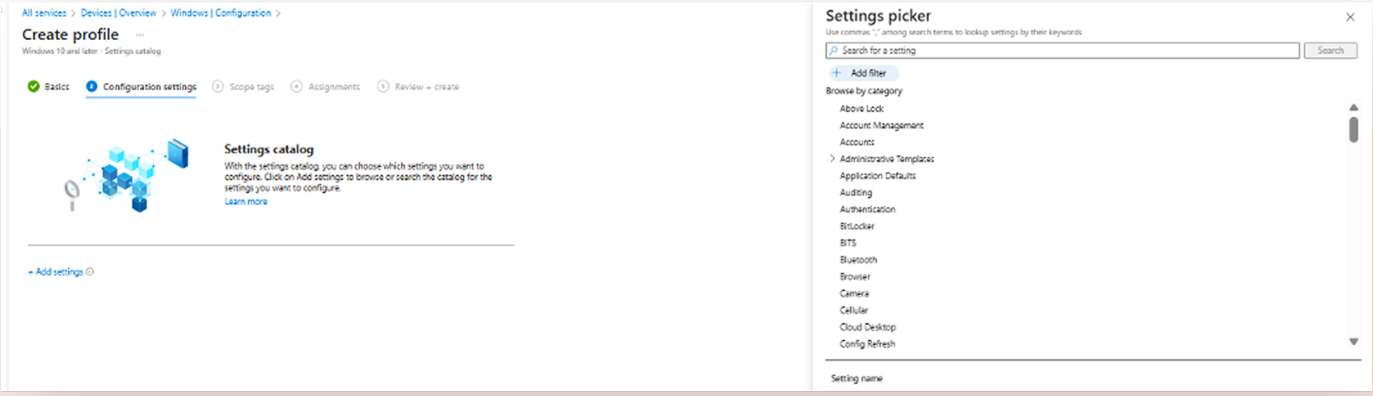
Les scénarios 1, 2 et 4 sont généralement les plus utilisés en entreprise. Si vous voulez en savoir plus, cliquez sur le lien de chaque scénario.

Les processus de déploiement Windows Autopilot sont très bien résumés dans ces schémas mis en ligne par Microsoft, à consulter **ici.**

Microsoft a annoncé en mai 2024, une nouvelle version d'Autopilot nommée Autopilot Device Preparation.
En savoir plus.

Gestion de la configuration

Microsoft Intune offre une large possibilité pour configurer les postes de travail Windows, voici un tour d'horizon de ces différentes possibilités :



Les settings Catalog

L'utilisation des Settings Catalog représente une évolution naturelle de la **gestion des paramètres**, en particulier pour les organisations habituées aux stratégies de groupe (GPO), vers une approche basée sur le cloud.

Les Settings Catalog centralisent l'ensemble des paramètres configurables dans un **référentiel unique**, facilitant ainsi la création et la gestion des stratégies de configuration. Microsoft enrichit régulièrement ce catalogue, ce qui en fait aujourd'hui la méthode recommandée pour administrer, configurer et sécuriser les postes de travail Windows.

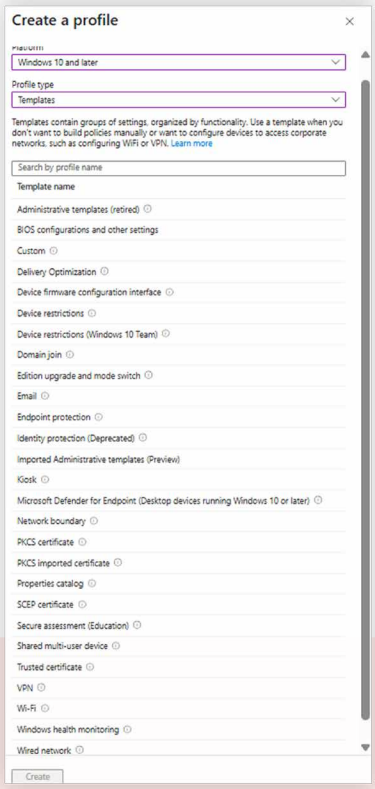
Cette fonctionnalité est également disponible pour d'autres systèmes d'exploitation, notamment macOS.

Un moteur de recherche et un système de filtres intégrés permettent d'identifier rapidement les paramètres souhaités. Il est possible d'utiliser plusieurs mots-clés, séparés par des virgules, pour affiner les résultats.

La liste des paramètres actuellement contenue dans le catalogue est disponible ici

Les templates

Les templates incluent un regroupement de paramètres qui configurent une fonctionnalité comme un profil VPN, un profil Wifi, un mode Kiosk ou encore le déploiement d'un certificat approuvé.



Paramétrage CSP / Scripts

Certains paramètres ne sont pas disponibles dans les types de configuration ci-dessous, bien qu'ils soient pris en charge par Windows, pour cela plusieurs solutions sont possibles :

Utilisation des OMA-URI / CSP

Certains paramètres avancés peuvent être configurés via des profils personnalisés utilisant les OMA-URI, basés sur les CSP (Configuration Service Provider). Cela permet de cibler des réglages précis non exposés dans les profils standards d'Intune, tout en restant pris en charge par Windows.

Utilisation des scripts Powershell

Microsoft Intune permet de déployer des scripts Powershell dans le contexte SYSTEM ou dans le contexte USER ce qui permet de pousser des configurations dans l'un ou l'autre des contextes.

Utilisation des remédiations

Les licences Windows Enterprise permettent l'utilisation des remédiations dans Microsoft Intune. Cette fonctionnalité offre la possibilité de déployer des scripts de configuration afin de détecter et corriger automatiquement des écarts de conformité sur les appareils gérés.

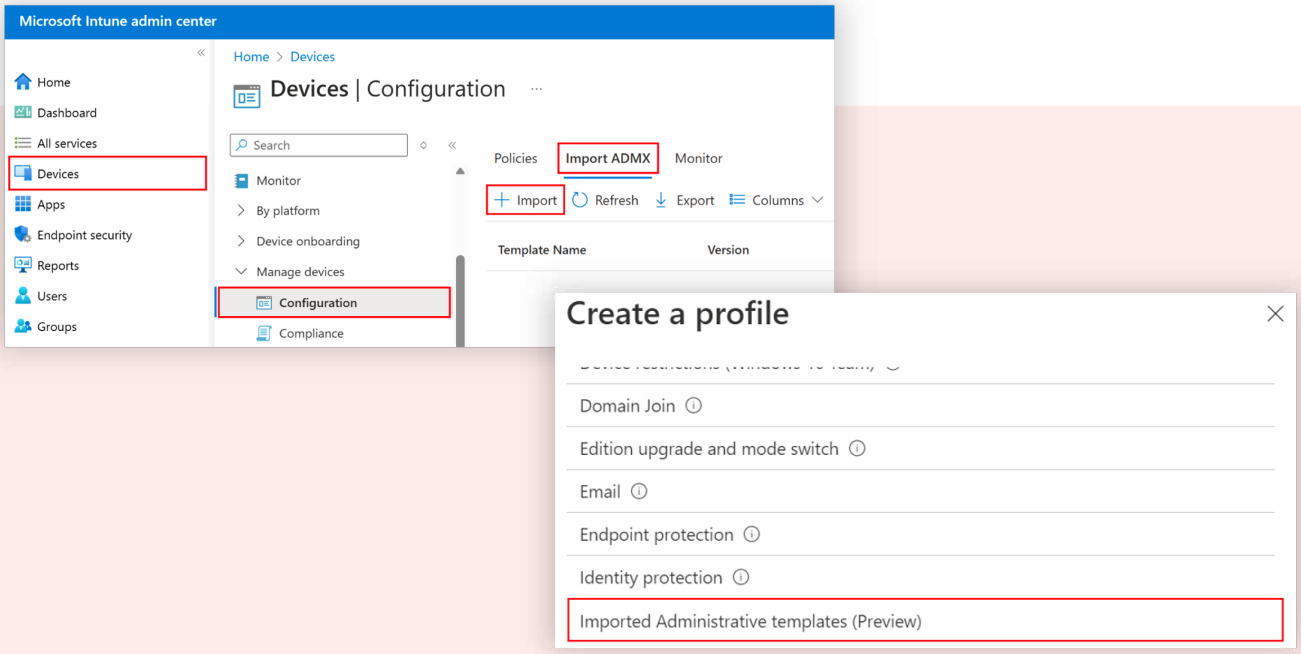
Cela se base sur un script de découverte et un script de correction, on peut imaginer donc le script de découverte qui contrôle une valeur de clé de registre et le script de correction qui vient corriger cette valeur si celle-ci n'est pas correcte et ceux à une périodicité configurable par l'administrateur.

Il est également possible d'exécuter cette remédiation à la demande via le portail Microsoft Intune.

Imported Administratives Templates

Pour gérer et configurer des **logiciels tiers** comme Mozilla Firefox, il est possible d'importer directement les fichiers ADMX fournis par l'éditeur dans Microsoft Intune. Cela permet de créer des profils de configuration spécifiques pour appliquer les paramètres souhaités. La plateforme autorise l'import de jusqu'à 20 fichiers ADMX.

Microsoft Intune propose également la fonctionnalité **Group Policy Analytics**, utile dans le cadre d'une migration depuis un environnement Active Directory avec des GPO. En important les stratégies de groupe au format XML, cette fonctionnalité permet d'identifier les correspondances disponibles dans les stratégies Intune, facilitant ainsi l'évaluation et la transition vers une gestion moderne.



Sécurisation et gestion de la conformité

Sécurisation et hardening

Grâce à Microsoft Intune, il est possible d'activer des fonctionnalités de sécurité importantes et recommandées comme :

- **Le chiffrement Bitlocker / Personnal Data Encryption** : pour protéger les données contenues sur le disque dur local et la session de l'utilisateur.
- **Windows Hello For Business** : pour protéger l'identité de l'utilisateur en mettant en place une authentification passwordless grâce notamment à la biométrie ou à un code PIN.
- **Gestion du compte Administrateur local avec LAPS** : pour protéger et sécuriser l'utilisation du compte administrateur BUILT-IN de Windows grâce notamment à un mot de passe fort.

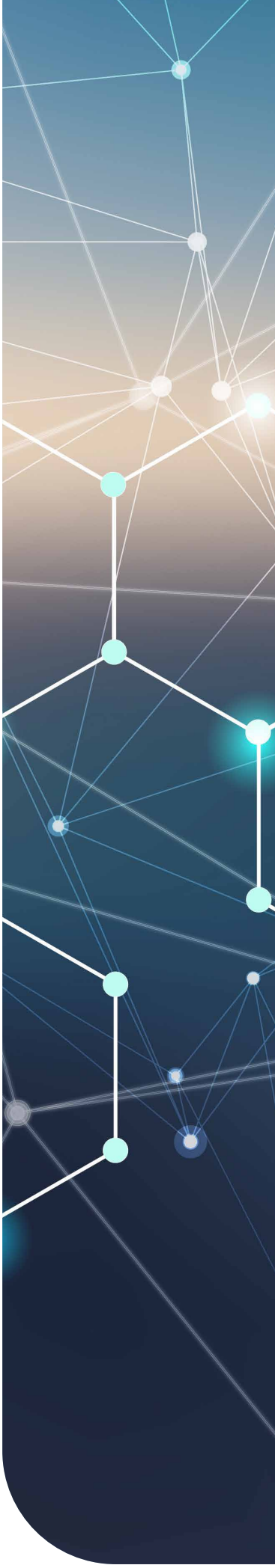
Et aussi mettre en place du Hardening conformément aux bonnes pratiques du CIS par exemple. Ces règles de hardening sont souvent poussées par les équipes RSSI et peuvent parfois nécessiter quelques « mitigations » pour s'adapter au contexte terrain. Pour mettre en place tout cela, il est possible d'utiliser :

Le Blade «Endpoint Security» dans Microsoft Intune

C'est dans cette section que se configure la majorité des fonctionnalités de sécurité mentionnées précédemment, ainsi que d'autres comme le pare-feu Windows. Elle permet également la configuration de l'antivirus Microsoft Defender ATP, sous réserve de disposer des licences nécessaires (notamment pour les règles ASR et l'EDR).
Certaines fonctionnalités avancées, comme Endpoint Privilege Management, peuvent également être activées, sous réserve de licence, et apportent une valeur ajoutée en matière de contrôle des droits utilisateurs.

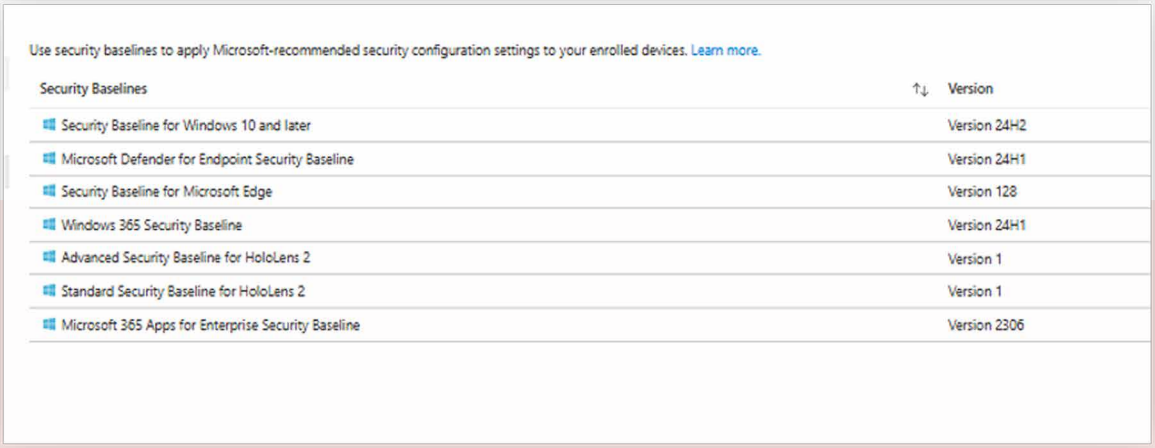
Les setting Catalog / scripts / CSP

Il s'agit aujourd'hui de la méthode recommandée pour appliquer des stratégies dans Intune. Les scripts PowerShell restent utiles pour certains réglages plus anciens ou spécifiques, tandis que les CSP / OMA-URI permettent d'accéder à des paramètres non exposés dans l'interface standard.



Security Baseline

Microsoft propose également des Security Baselines, qui regroupent un ensemble de bonnes pratiques et de recommandations officielles pour la configuration sécurisée des environnements Windows.



De nombreuses organisations s'appuient sur des recommandations pour configurer efficacement les fonctionnalités de sécurité. Les **stratégies de sécurité** proposées dans Intune sont préconfigurées et prêtes à être déployées.

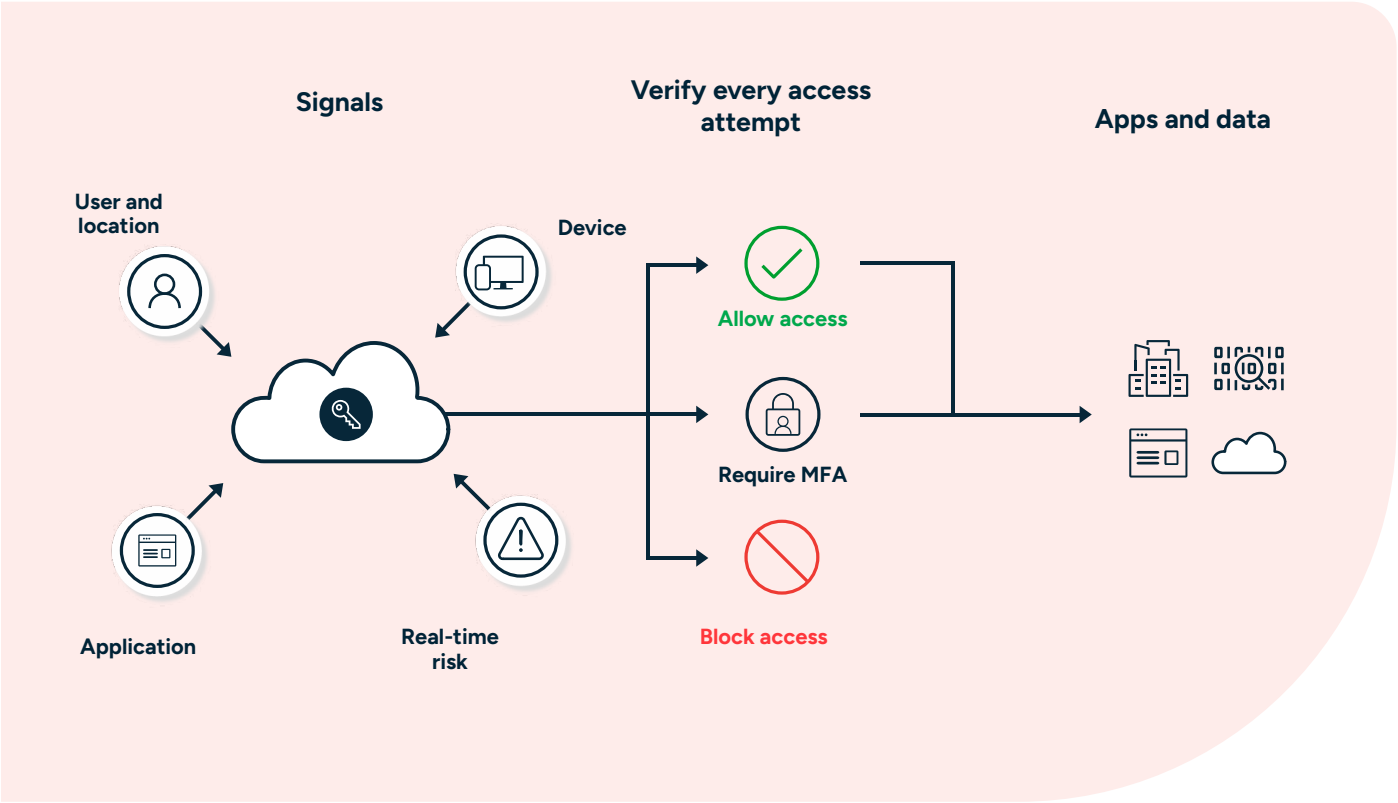
Par défaut, les paramètres appliqués sont parmi les plus restrictifs, mais chaque règle reste personnalisable afin de s'adapter aux besoins et aux contraintes de l'environnement cible. Ces **Security Baselines** constituent un point de départ pertinent pour sécuriser rapidement un parc Windows, en particulier dans le cadre d'un déploiement initial.

Pour avoir un aperçu des settings contenues dans ces règles, rendez-vous ici.

Gestion de la conformité et accès conditionnel

Une stratégie de conformité Intune couplée à une **règle d'accès conditionnel**, permet à une entreprise de s'assurer que tous les postes de travail Windows utilisés par leurs employés respectent les règles fixées dans ces stratégies de conformité pour accéder aux ressources de l'entreprise.

Si le poste n'est pas conforme à ces règles, il peut se voir refuser l'accès aux ressources ou demander une authentification MFA par exemple pour y accéder. On parlera dans ce cas de « **Device-based Conditionnal Access Policy** ».



Il existe deux types de **règles de conformité** :

Les règles de conformité « by design » fournies par Microsoft

Elles permettent de contrôler automatiquement plusieurs paramètres essentiels de sécurité sur les postes.

Ces règles vérifient notamment l'état du **chiffrement BitLocker**, l'activation du pare-feu et de l'antivirus, ou encore la version de Windows installée sur le poste. Elles offrent une base solide pour assurer un niveau de conformité minimal sur l'ensemble du parc.

Les règles de conformité « custom »

Il est également possible de créer des règles de conformité personnalisées (« custom »), qui apportent une flexibilité accrue. Grâce à l'utilisation d'un **script PowerShell** de découverte renvoyant des résultats au format JSON, il devient possible de cibler des contrôles très spécifiques.

Par exemple, la présence d'un paramètre précis dans le registre, la détection d'un proxy Zscaler, ou encore la vérification de la configuration d'un mot de passe BIOS peuvent être intégrés dans une stratégie de conformité sur mesure, répondant ainsi aux besoins spécifiques de chaque environnement.

Il est possible de contrôler la conformité du **Windows Subsystem for Linux (WSL)** au sein de Microsoft Intune, si celui-ci est utilisé dans l'environnement de l'organisation.

En cas de non-conformité, une notification par e-mail peut être configurée afin d'informer l'utilisateur de la situation, en précisant les causes de la non-conformité ainsi que les éventuelles actions correctives à entreprendre.

Les règles de conformité sont également disponibles pour d'autres systèmes d'exploitation, notamment macOS, iOS et Android.

Pour plus d'informations, c'est par ici.

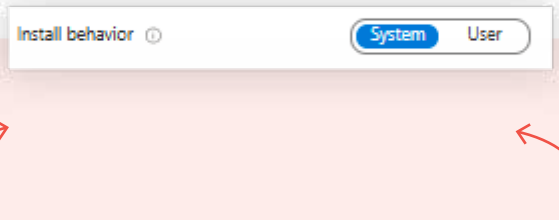
Déploiement des applications

Une fois le poste de travail provisionné, configuré et sécurisé, le **déploiement du socle applicatif** peut être envisagé. Microsoft Intune prend en charge différents types d'applications sur Windows, qu'il s'agisse d'installateurs MSI, EXE, d'applications du Microsoft Store ou de packages Win32.

Une fois les applications ajoutées dans Intune, leur déploiement peut être ciblé sur des groupes d'utilisateurs ou de périphériques, selon les besoins de l'organisation.

Type d'application	Particularité
Win32App	Empaquetage d'une application au format EXE / MSI dans un format intunewin qui offre plusieurs avantages comme : Logique de détection / Gestion des dépendances / Personnalisation et flexibilité des applications. **La taille de l'application Windows ne doit pas être supérieure à 30 Go par application.** Vous devez mettre à jour l'application.
Office 365	Inclut des outils comme Word, Excel, et Outlook. Ces applications peuvent être **configurées pour répondre aux besoins spécifiques** de l'organisation grâce à l'assistant de configuration directement intégrée. Office 365 se met à jour automatiquement selon votre stratégie.
LOB : Appx / MSIX / MSI	Ce sont notamment **des applications développées spécifiquement** pour votre organisation. Vous devez mettre à jour l'application.
Microsoft Store App	Les applications sont **installées directement depuis le Microsoft Store**. Les mises à jour sont automatiques ce qui simplifie leur gestion.
Web Apps	Ces applications sont **essentiellement des liens vers des sites web ou des services en ligne**. Elles ne nécessitent pas d'installation sur l'appareil et sont accessibles via un navigateur. Un raccourci vers l'application web est placé dans le menu Démarrer.
Enterprise App Catalog	Applications Win32app **préconfigurées conçues par Microsoft**. Le catalogue contient à la fois des applications Microsoft et des applications tierces. **Intune add-on as part of the Intune Suite.** La mise à jour des applications est automatique. La liste est disponible ici : Gestion des applications d'entreprise Microsoft Intune | Microsoft Learn

Il est également possible de déployer ces applications dans deux contextes distincts :



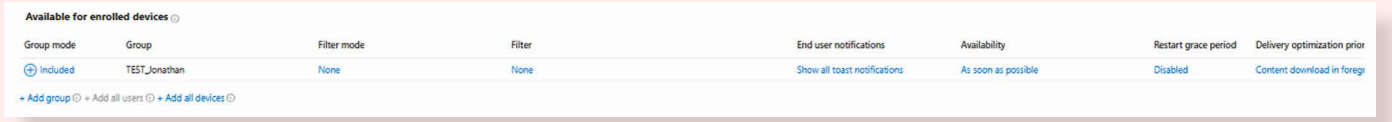
SYSTEM CONTEXT

Lorsqu'une application est déployée dans le **contexte System**, elle est installée directement sur l'appareil par Intune avec les autorisations maximales.

USER CONTEXT

Lorsqu'une application est déployée dans le **contexte utilisateur**, elle est installée pour cet utilisateur lorsque celui-ci se connecte à l'appareil. Notez que l'installation de l'application n'aboutit pas tant que l'utilisateur ne se connecte pas à l'appareil. Elle s'installe avec les autorisations de l'utilisateur (non administrateur).

Il est également possible de mettre en place et maintenir un **portail de déploiement applicatif** directement via l'application « Portail d'Entreprise ».

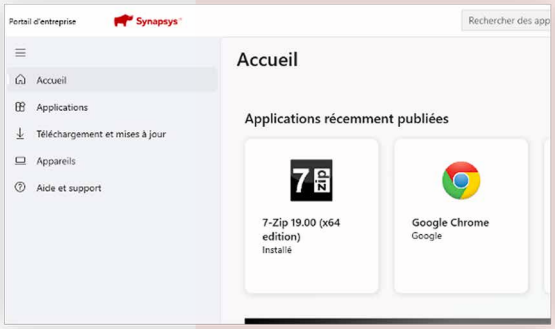


Pour ce type de déploiement, il convient de sélectionner le mode « Available for enrolled devices », qui rend l'application disponible à l'installation depuis le portail d'entreprise. Ce déploiement peut être ciblé sur un groupe spécifique ou étendu à l'ensemble des utilisateurs en sélectionnant l'option « All Users ».

L'application devient ensuite disponible dans le **Portail d'entreprise**, où elle peut être installée librement par l'utilisateur final.

Il est possible d'affiner le ciblage des déploiements à l'aide des Assignment Filters. Ces filtres permettent d'appliquer des conditions spécifiques, comme limiter le déploiement à des appareils d'une certaine marque (ex. : HP) ou à un système d'exploitation donné (ex. : uniquement Windows 11).

Pour personnaliser davantage l'expérience de déploiement des applications Win32, l'outil **PSAppDeployToolkit** peut être utilisé. Il s'agit d'un framework PowerShell bien connu permettant de gérer l'installation, la mise à jour ou la désinstallation des applications avec des interfaces utilisateur personnalisées : en savoir plus.



Enfin, les applications Win32 App sont compatibles avec la **Delivery Optimization**, une fonctionnalité native de Windows permettant d'optimiser les téléchargements en utilisant des sources alternatives telles que d'autres appareils sur le réseau ou un serveur de cache local. Cette technologie permet de réduire la consommation de bande passante et d'accélérer les installations, tout en étant pleinement compatible avec Windows Autopilot, dans le cadre de déploiements à grande échelle.

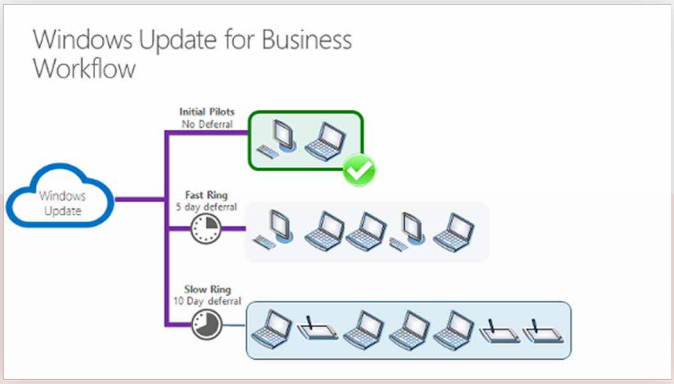
Gestion des mises à jour de sécurité et des fonctionnalités

Windows Update for Business

La gestion des mises à jour de sécurité et de fonctionnalités pour les PC Windows gérés par Intune se fait au travers de **Windows Update for Business**.

Windows Update for Business (WUfB) est un **service cloud gratuit** qui permet aux entreprises de gérer les mises à jour de Windows 10 et Windows 11 sans nécessiter d'infrastructure dédiée.

Windows Update for Business permet aux administrateurs de gérer les mises à jour de Windows 10 (qui arrive en fin de support en Octobre 2025) et Windows 11 de manière centralisée, sans nécessiter d'approbation individuelle comme un WSUS standard ou un MECM (si pas d'utilisation d'ADR).



Voici quelques détails supplémentaires :

> **La gestion de l'installation des cumulatives updates et l'expérience utilisateurs** se paramètrent dans un « Update Ring » , ainsi il est possible de définir :

- Quand les mises à jour de sécurité et de fonctionnalités s'installent (Update Deferral period)
- Les paramètres d'expérience utilisateur
- La deadline pour le redémarrage après l'installation des mises à jour

> **Le profil de mise à jour des fonctionnalités** (Feature Updates profile) permet de figer une version spécifique de Windows (build) sur un parc d'appareils, ou de planifier le passage d'une version à une autre, comme par exemple de la build 24H2 à 25H2.

> **En cas de vulnérabilité critique** (type 0-day) nécessitant un déploiement rapide des correctifs, une Expedite Policy peut être utilisée. Cette stratégie permet d'outrepasser les périodes de report (deferral) afin d'appliquer les mises à jour de sécurité sans délai sur les appareils ciblés.

L'expérience utilisateur est optimisée grâce à Windows Update for Business, qui simplifie la gestion des mises à jour tout en minimisant les interruptions. Les appareils récupèrent directement les mises à jour depuis Windows Update via Internet, sans passer par une infrastructure locale.

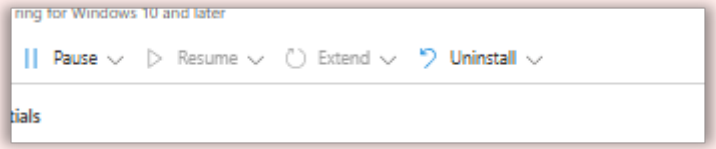
La fonctionnalité **Delivery Optimization** peut être utilisée pour réduire la charge réseau en tirant parti de sources alternatives comme d'autres appareils du réseau, à l'image de ce qui est possible pour le déploiement d'applications.

En matière de **rapports et de suivi**, Microsoft Intune met à disposition des outils permettant de surveiller en temps réel l'état des mises à jour sur les appareils gérés. Ces rapports fournissent des informations sur les mises à jour installées, les échecs éventuels, ainsi que sur les niveaux de conformité, facilitant ainsi la supervision et la prise de décision pour les équipes IT.

Bon à savoir !

En cas de souci avec une mise à jour de sécurité ou de fonctionnalités, il est possible de mettre en pause le ring pendant 30 jours ou lancer une désinstallation de la mise à jour problématique.

Il est bien entendu recommandé de déployer les mises à jour en décalant par ring vos types de population. (Utilisation du Quality Update Deferral Period).



Hot patching

Le hotpatching sur Windows 11, géré via Intune, permet l'application de mises à jour de sécurité sans nécessiter de redémarrage du système.

Cette technologie vise à réduire les interruptions tout en assurant un niveau de sécurité élevé. Elle est disponible à partir de la version Windows 11 Enterprise 24H2 et ultérieures.

Le cycle de publication prévoit **quatre redémarrages obligatoires** par an, correspondant à des mises à jour majeures, tandis que les autres correctifs de sécurité sont appliqués de manière transparente, sans redémarrage.

Pour activer cette fonctionnalité, il faudra créer une « **Windows Quality Update Policy** ».

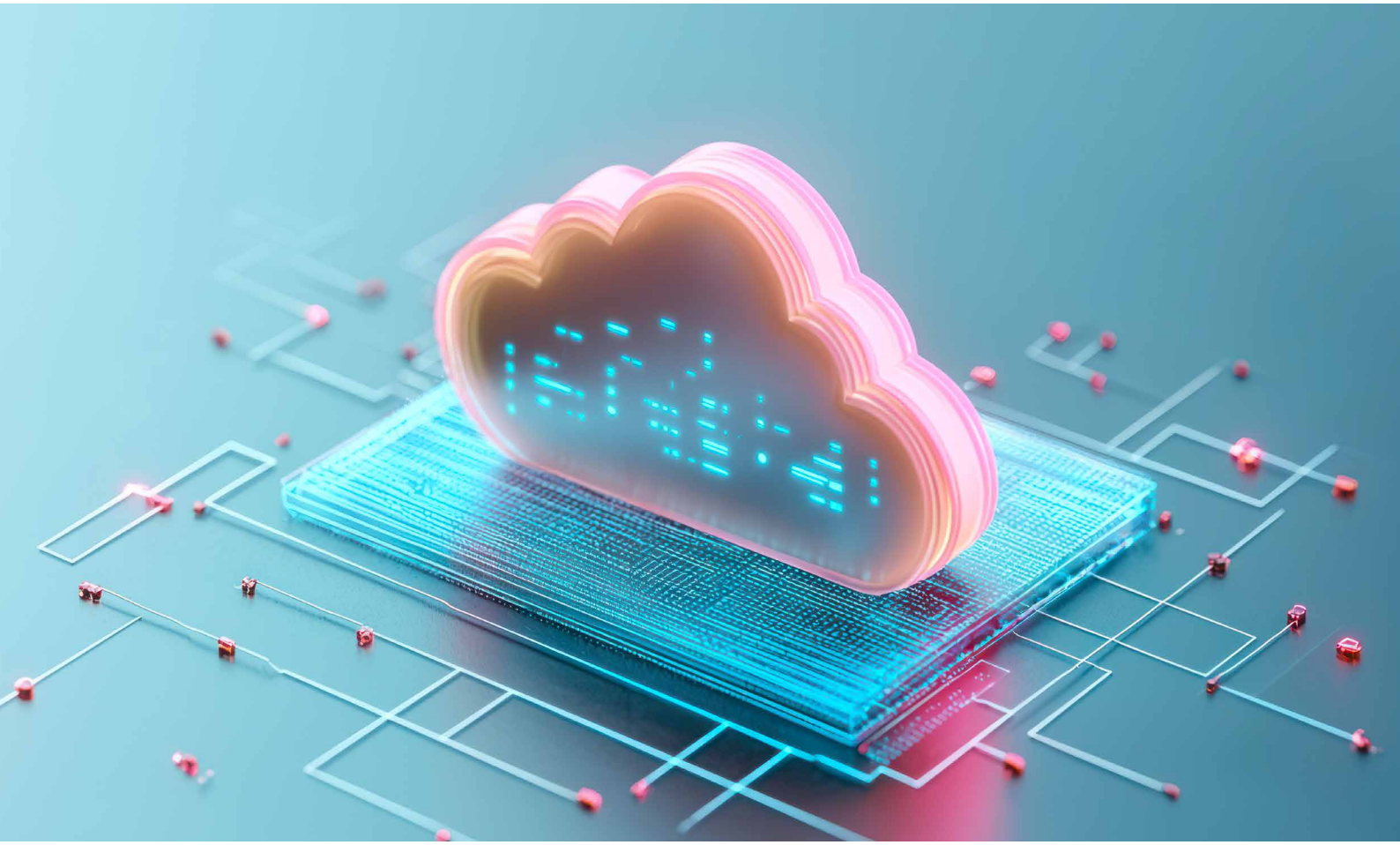
Quarter	Baseline updates (requires restart)	Hotpatch (no restart required)
1	January	February and March
2	April	May and June
3	July	August and September
4	October	November and December

Autopatch

Windows Autopatch est un **service cloud disponible** avec les licences Microsoft 365 Business Premium ainsi que Windows 11 Enterprise E3 ou E5. Il va au-delà de Windows Update for Business en automatisant la gestion des mises à jour pour Windows, Microsoft 365 Apps for Enterprise, Microsoft Edge et Microsoft Teams.

L'objectif est d'assurer un niveau de sécurité renforcé et une continuité de service optimale à l'échelle de l'organisation.

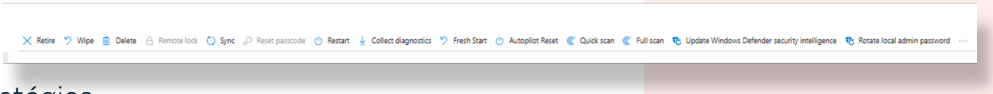
Plus d'informations disponibles ici.



Gestion à distance et accès aux ressources de l'entreprise

Gestion à distance

Quand un poste Windows est enrôlé dans Intune, il est possible de lancer plusieurs actions à distance comme :

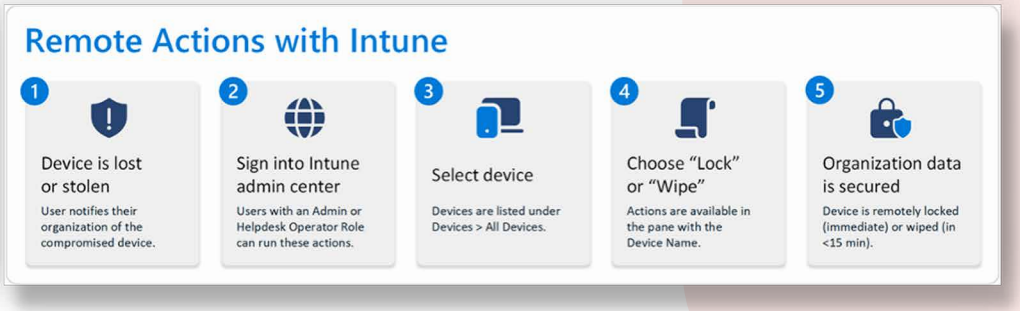


- Une remise à zéro
- Un renommage du poste
- Une synchronisation des stratégies
- Un redémarrage
- Ou encore un scan antivirus

En cas de vol ou de compromission d'un poste de travail Windows, une **action de type Wipe** peut être déclenchée à distance pour effacer les données de l'appareil.

La plateforme Microsoft Intune propose plusieurs actions à distance permettant de gérer les appareils de manière centralisée. La liste complète de ces actions est disponible ici.

Concernant la **prise en main à distance**, plusieurs solutions sont compatibles avec Intune, notamment Remote Help et TeamViewer. Chaque outil présente des avantages, des limites et des coûts spécifiques, et peut être sélectionné en fonction des besoins de l'organisation.



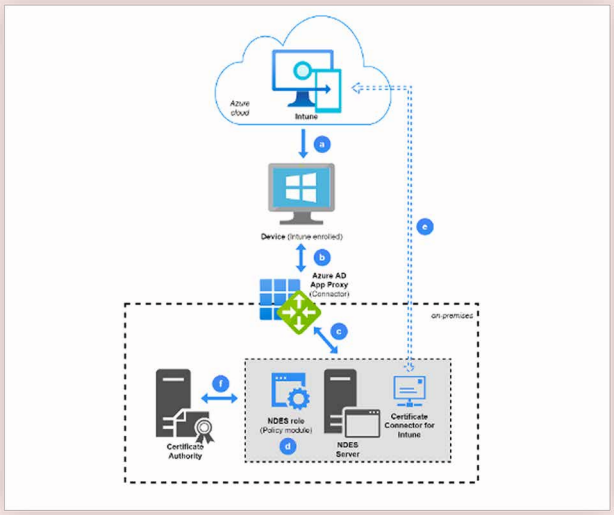
Accès aux ressources de l'entreprise

Le déploiement de **configurations spécifiques** telles qu'un SSID Wi-Fi ou un profil VPN est pris en charge nativement par Microsoft Intune.

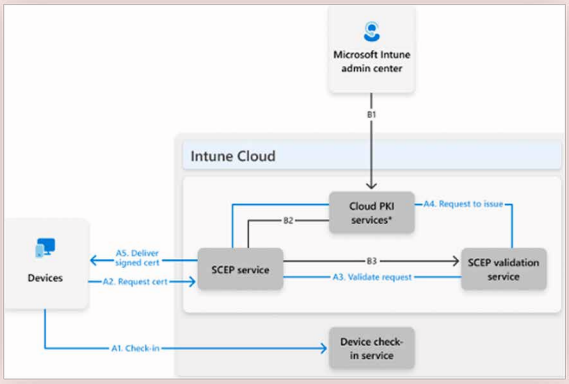
Dans le cas où une **authentification par certificat** est requise, il est également possible de déployer des certificats issus d'une PKI interne.

Deux méthodes principales permettent de réaliser ce type de déploiement, en fonction de l'infrastructure existante et des besoins en sécurité.

L'utilisation d'un serveur SCEP / Ndes avec un connecteur spécifique pour Intune.



L'utilisation de la cloud PKI, service dernièrement proposé par Microsoft



Les deux approches impliquent des coûts. D'un côté, une **infrastructure PKI interne** engendre des frais liés à la gestion des serveurs, à l'infogérance et à la maintenance. De l'autre, une solution de PKI cloud repose sur un **modèle de service payant**, souvent plus rapide à mettre en place et proposant des fonctionnalités intégrées telles que le reporting.

Le choix entre ces deux options dépend des contraintes techniques, des exigences de sécurité et du budget alloué.

Gestion des PC spéciaux

La force de Microsoft Intune est qu'il peut s'adapter et traiter tous les cas d'usages spécifiques qu'une entreprise peut avoir comme :

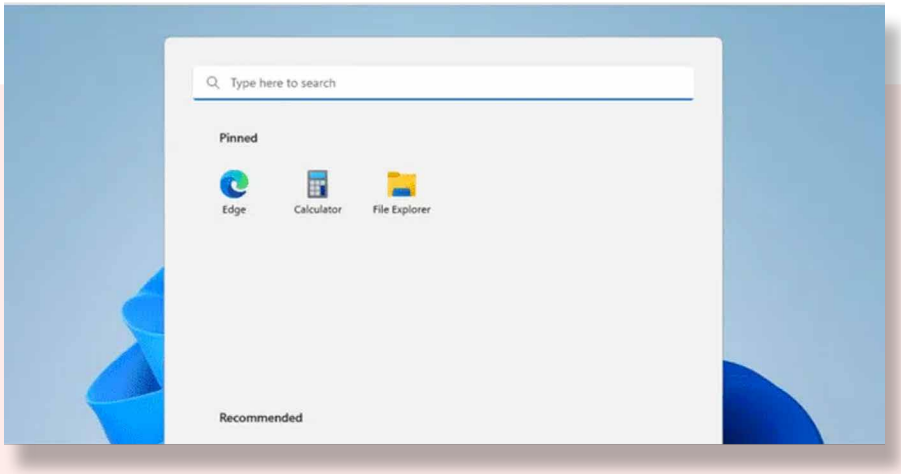
- **L'utilisation du mode Kiosk** pour des PC destinés à être localisé dans des points d'informations par exemple.
- **L'utilisation du mode shared** pour des PC destinés à être en prêt ou dans des espaces de travail en libre-service.

Kiosk Mode

Microsoft prend en charge le mode Kiosk en mode « **Single App** » ou « **Multi App** ».

Cela offre plusieurs avantages comme :
- Une sécurité renforcée : l'utilisateur n'a accès qu'aux applications autorisées empêchant toutes modifications non souhaitées.
- Une expérience utilisateur simplifiée
- Un déploiement rapide et une gestion centralisée pour les administrateurs
- Utilisation d'une licence Intune Device moins onéreuse

Pour en savoir plus sur la configuration possible, c'est ici.

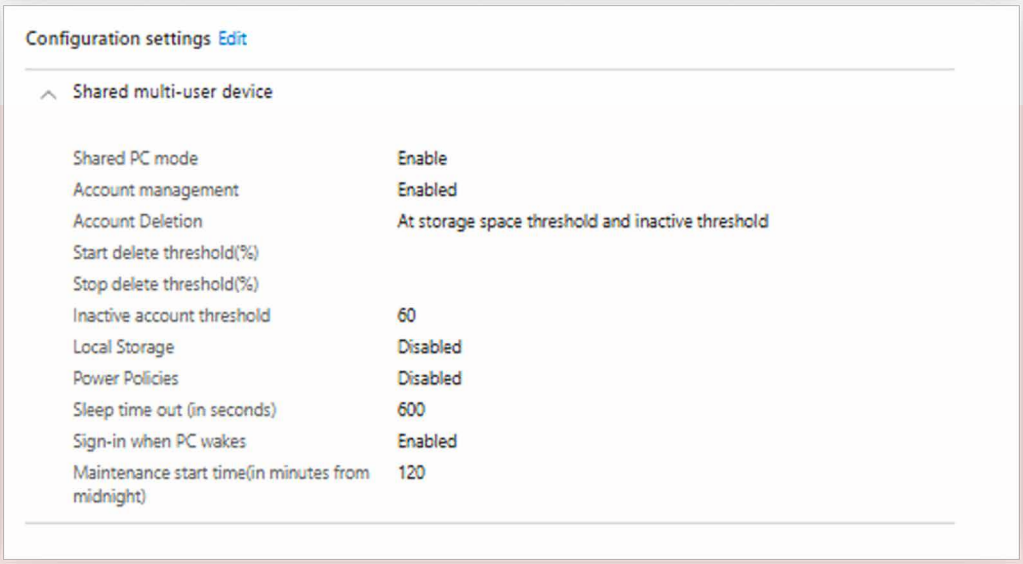


Shared Device

Le mode Shared Device sous Microsoft Intune offre plusieurs avantages pour les environnements où plusieurs utilisateurs doivent accéder à un même appareil :

- **Optimisation des ressources et des coûts** : maximiser l'utilisation des appareils sans nécessiter de configurations individuelles.
- **Suppression automatique des comptes** : suppression des comptes inactifs ou invités après chaque session, garantissant un environnement propre et sécurisé.
- **Contrôle des fonctionnalités** : les administrateurs peuvent restreindre l'accès aux paramètres système, aux fichiers locaux et aux options d'alimentation.

Pour en savoir plus, cliquer ici.



Reporting

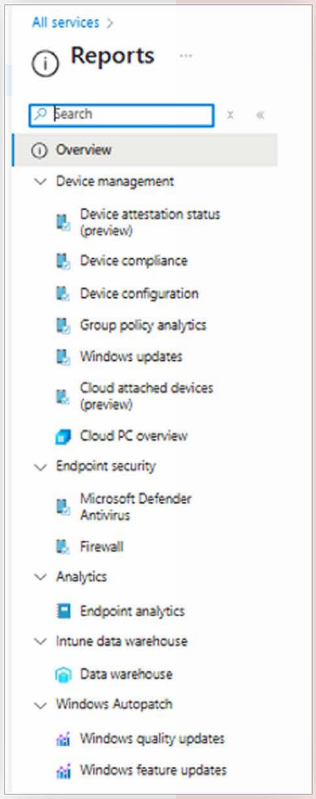
La fonctionnalité de reporting intégrée à Microsoft Intune permet de surveiller et d'analyser plusieurs aspects liés à la gestion des postes de travail, notamment :

- L'état des appareils
- La bonne application des configurations
- La bonne installation des mises à jour
- Leur état de conformité

Ces données sont regroupées dans différentes catégories, facilitant leur consultation et leur exploitation.

En complément, la **section Endpoint Analytics** fournit des indicateurs sur la santé et la performance du parc, permettant notamment d'identifier les problèmes liés aux temps de démarrage ou aux applications instables.

Enfin, l'utilisation de **Microsoft Graph API via PowerShell** permet d'extraire des informations détaillées à des fins d'analyse avancée. Ces données peuvent être intégrées dans des tableaux de bord Power BI pour un reporting personnalisé.



Conclusion

La gestion des postes de travail Windows via Microsoft Intune constitue une approche moderne et adaptable, permettant d'assurer la sécurité, la conformité et l'efficacité opérationnelle, tout en maintenant une expérience utilisateur cohérente, quel que soit le lieu de travail.

Les éléments abordés dans ce document fournissent les bases nécessaires à une exploitation optimale d'Intune pour une gestion centralisée, sécurisée et évolutive du poste de travail.

Dans une stratégie de modernisation de l'environnement utilisateur, Intune s'inscrit comme un composant clé, capable de répondre aux exigences actuelles en matière de mobilité, de sécurité et d'automatisation.

Jonathan Fievet

Ingénieur Modern Workplace chez Synapsys

Synapsys

A propos de Synapsys

Synapsys est un acteur de référence spécialisé dans la transformation des infrastructures IT. Depuis plus de 13 ans, nous accompagnons nos clients tout au long du cycle de vie des projets d'infrastructure à travers nos expertises en Digital Workplace, Cloud, DevOps, Cybersécurité, Data/IA et Transformation des SI.

Synapsys propose à ses clients un service technologique de qualité, grâce à l'esprit collectif et engagé de ses 180 talents répartis à Paris, Lille, Lyon et Kuala Lumpur.

Nous sommes fiers d'être considérés comme un partenaire de confiance et plébiscités pour la réalisation de projets de transformation structurants. Nos clients grands comptes nous sollicitent pour bâtir des infrastructures agiles et résilientes afin de relever les défis de transformation digitale de demain.

Convaincus que tout projet doit apporter le progrès et toute collaboration, la confiance, nous avons à cœur de proposer une vision de l'entreprise inclusive et équitable. Nous faisons du développement des hommes un véritable modèle d'entreprise qui guide nos orientations stratégiques, notre culture et notre mode de fonctionnement.

Chez Synapsys, c'est la force du collectif, l'engagement, l'équité et l'authenticité qui priment. Nous mettons tout en œuvre pour que chacun ait l'opportunité de se développer professionnellement dans un climat de confiance autour d'un projet commun.

www.synapsys-groupe.com

Crédit images : Synapsys & Adobe Stock