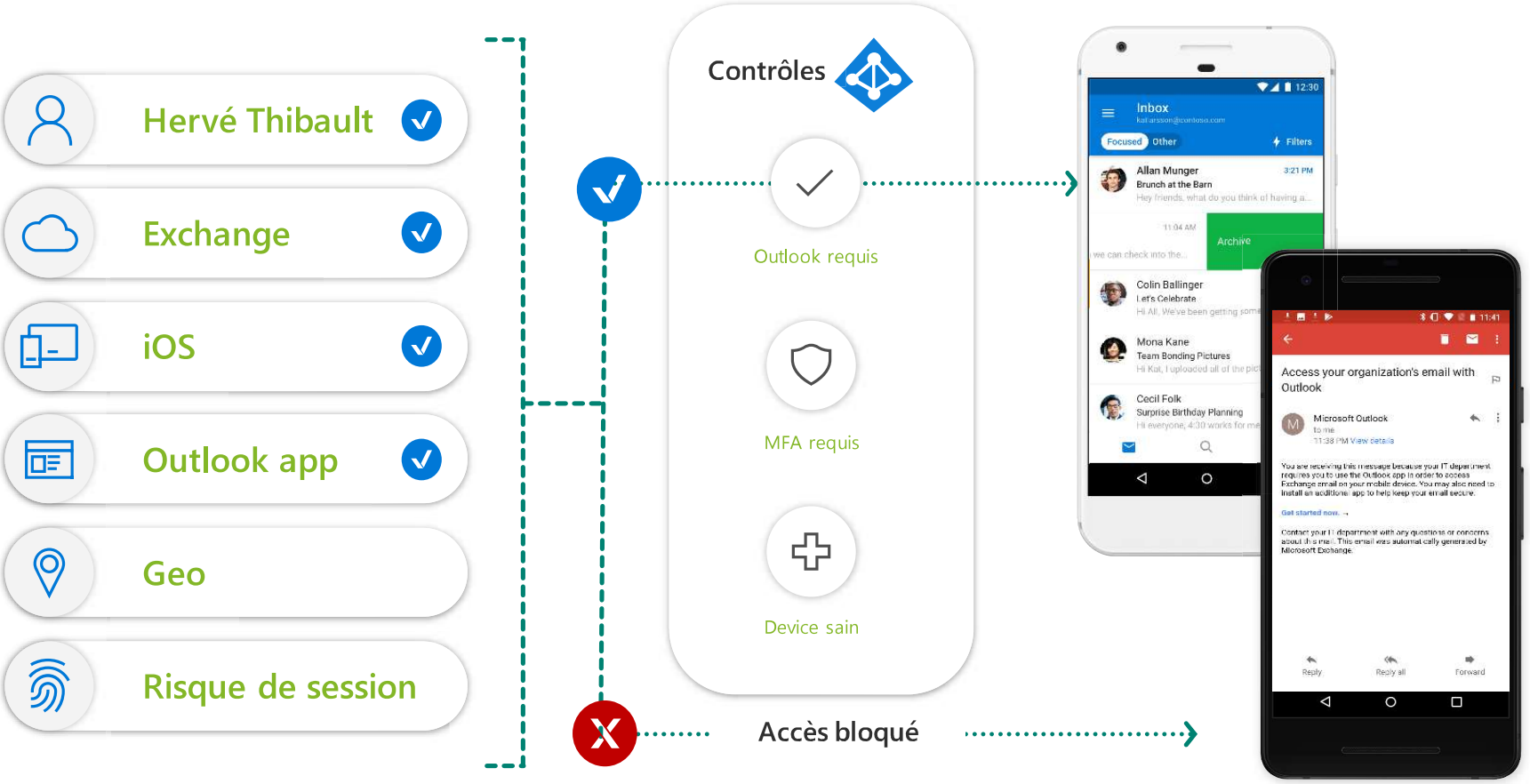
Accès conditionnel avec Azure AD Premium

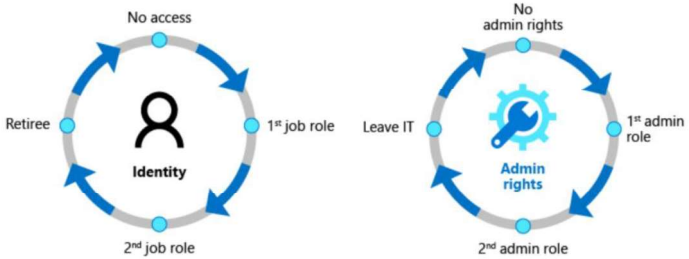
Autoriser l'accès à Exchange Online depuis Outlook uniquement



Microsoft

Modern Workplace : Identity Gouvernance

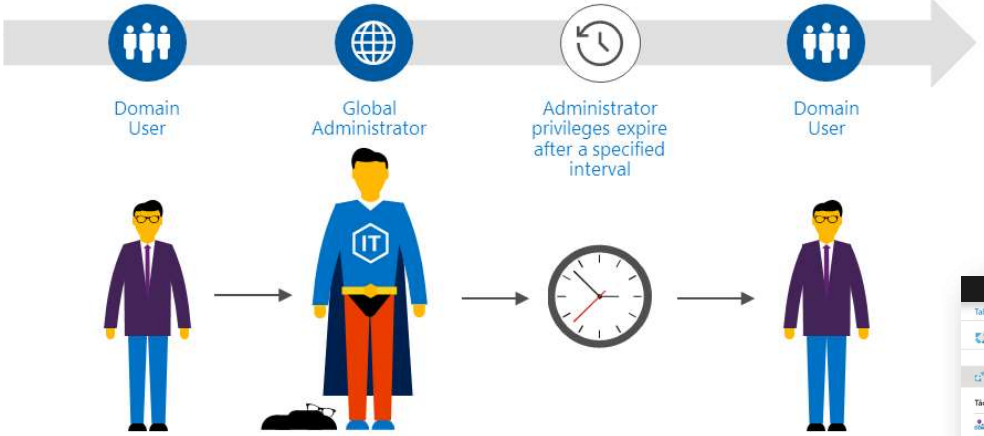
- Gouverner le cycle de vie des identités
- Gouverner le cycle de vie des accès
- Sécuriser l'administration

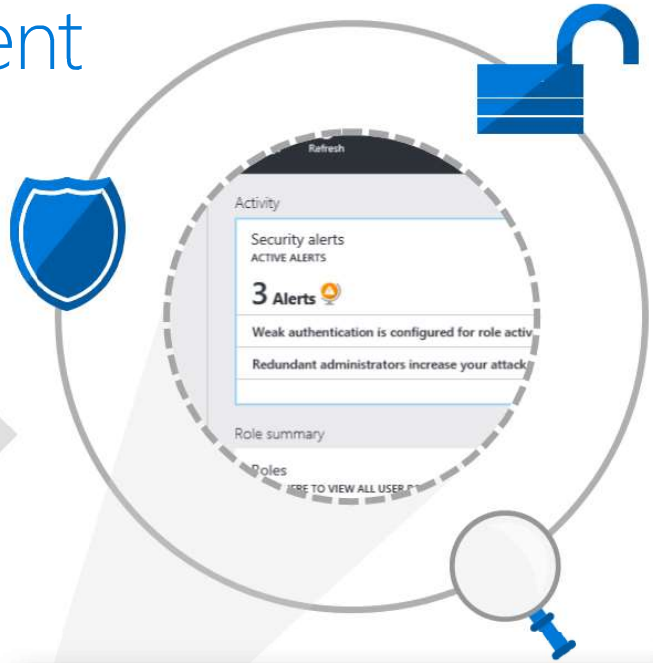


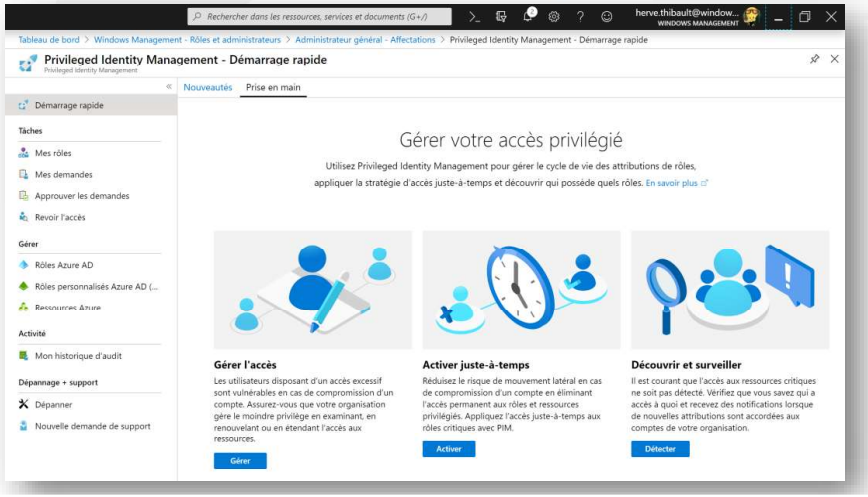
Comme pour tout projet, la gouvernance est clé !

Privileged Identity Management

- Just In Time Administration (JITA)
- Just Enough Administration (JEA)



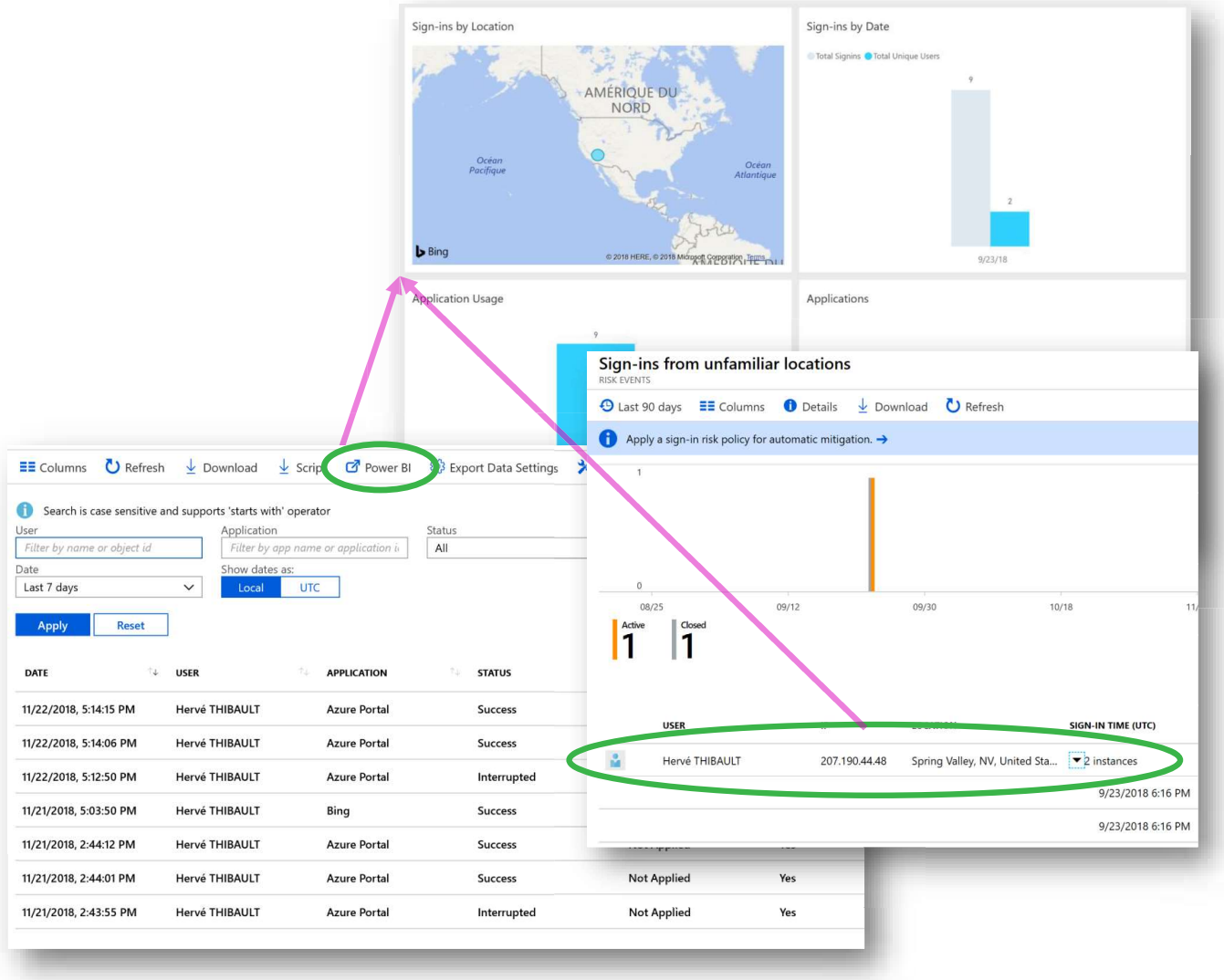




Rapports de sécurité & d'activité

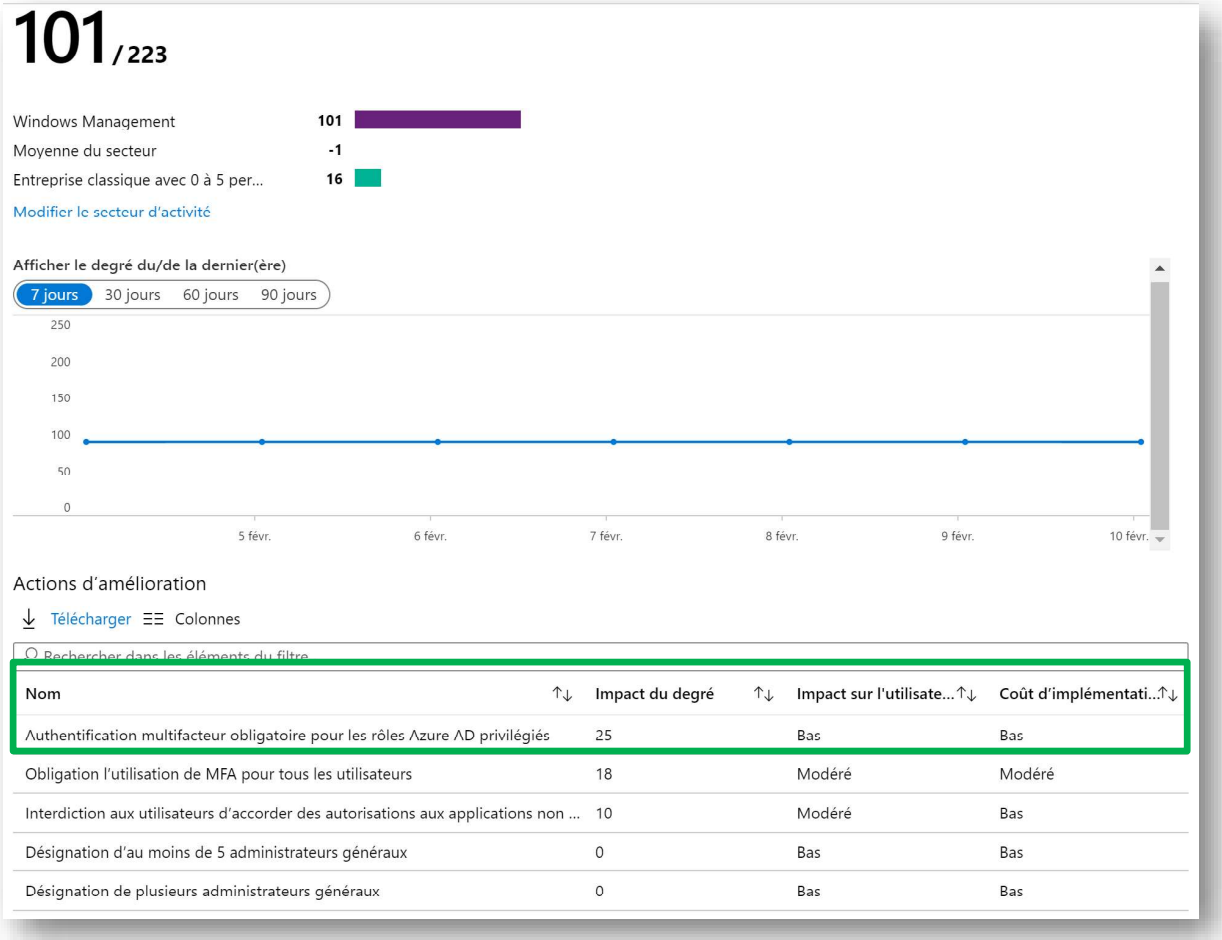
- **Rapports de sécurité** : Identification des utilisateurs "à risque", des connexions "suspectes" (@IP anonymes, endroits inhabituels ou "impossibles", devices compromis, …)

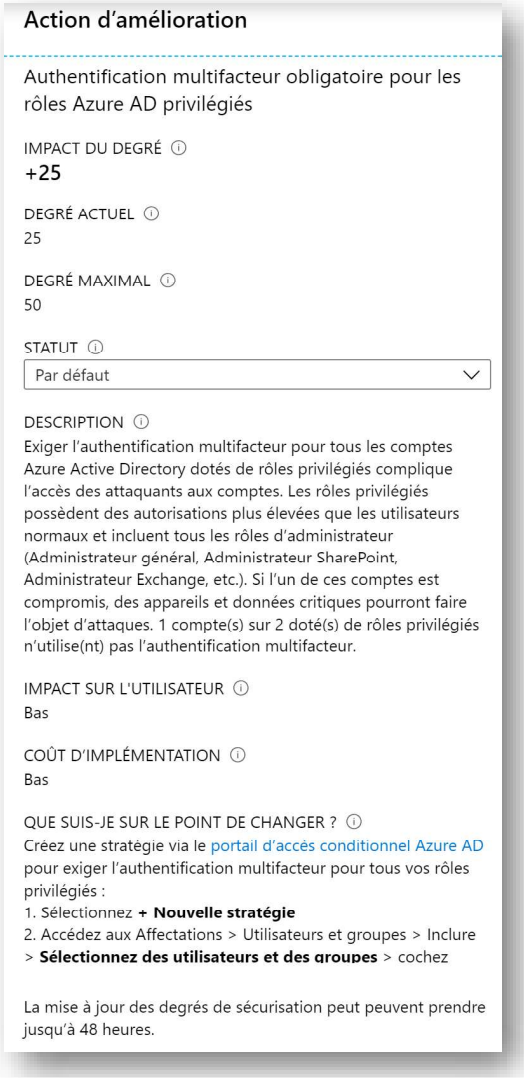
- **Rapports d'activité** : changements de groupe, reset de mot de passe, connexions authentifiées, …



Secure Score

Identifier les axes d'amélioration de la sécurité en un coup d'œil

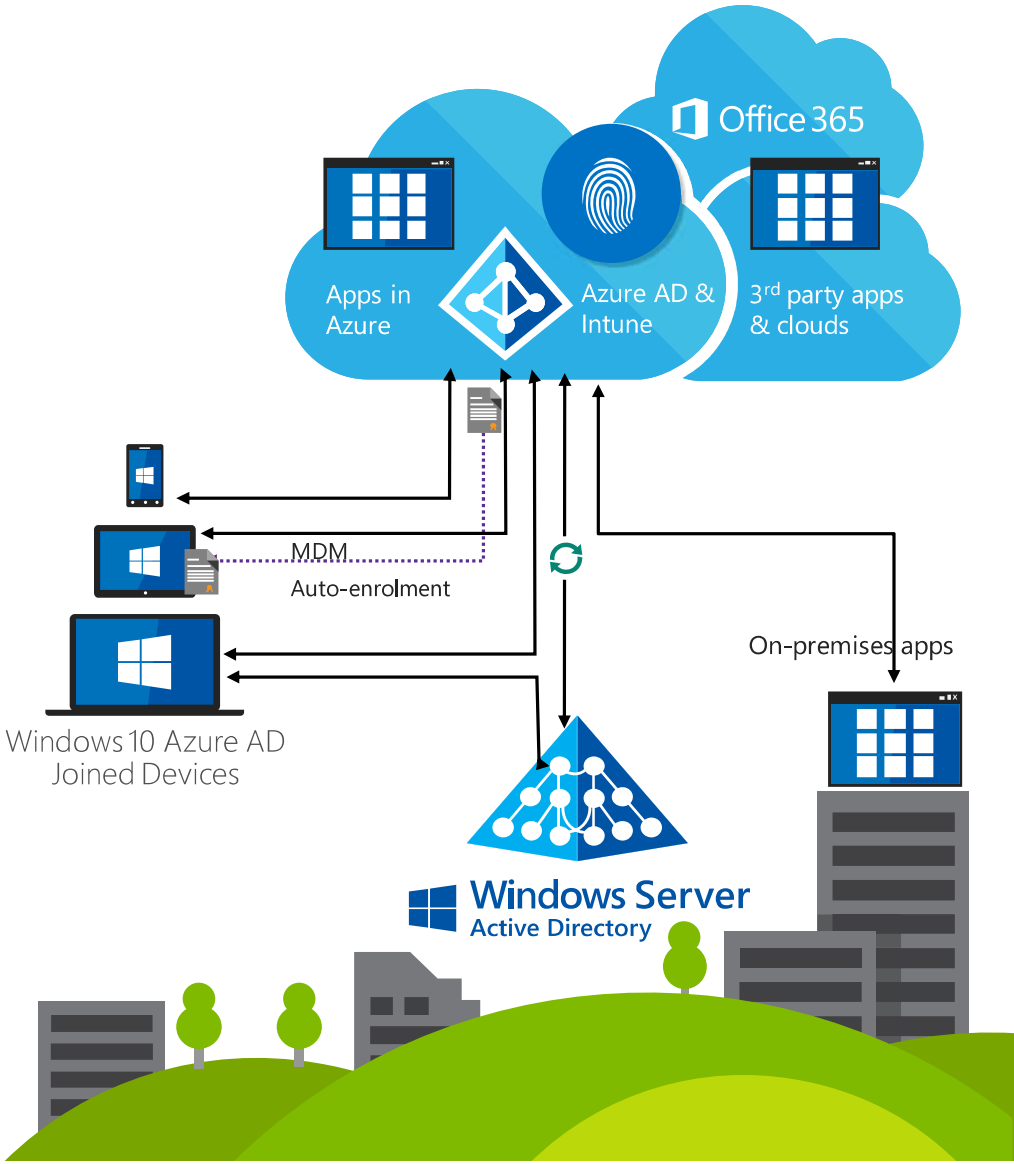




Azure AD Join & Windows 10

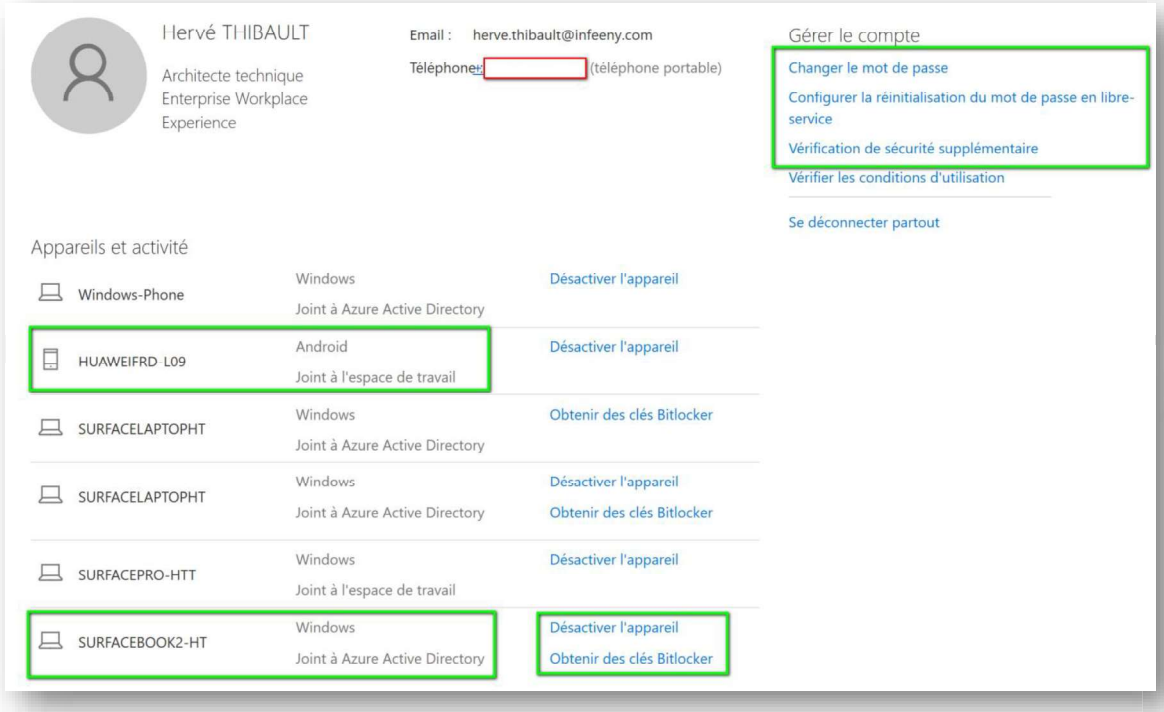
- Azure AD Join permet de connecter un appareil Windows 10 device dans l'Azure Active Directory de votre organisation.
- Les utilisateurs peuvent se connecter à Windows avec les identifiants stockés dans le cloud et profiter de la nouvelle experience moderne de Windows.

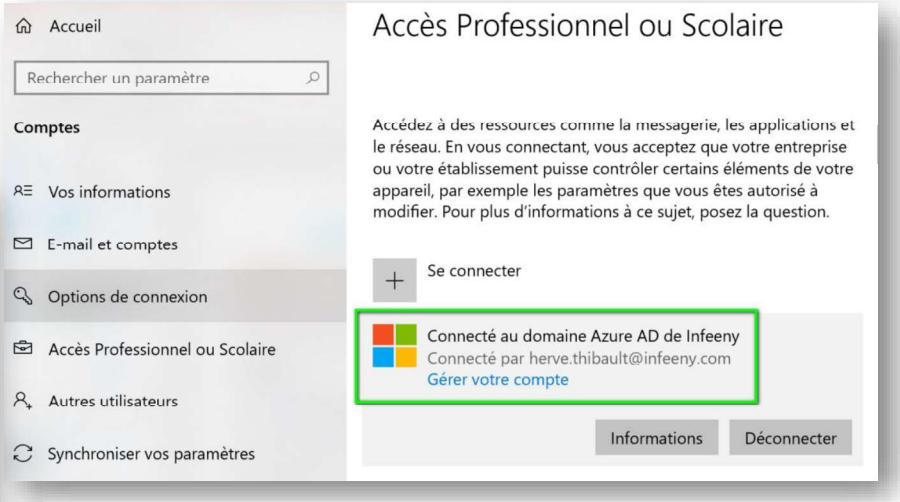
- SSO
- Accès Education / Business Store
- Enrôlement automatique dans un MDM
- Support d'environnement hybride

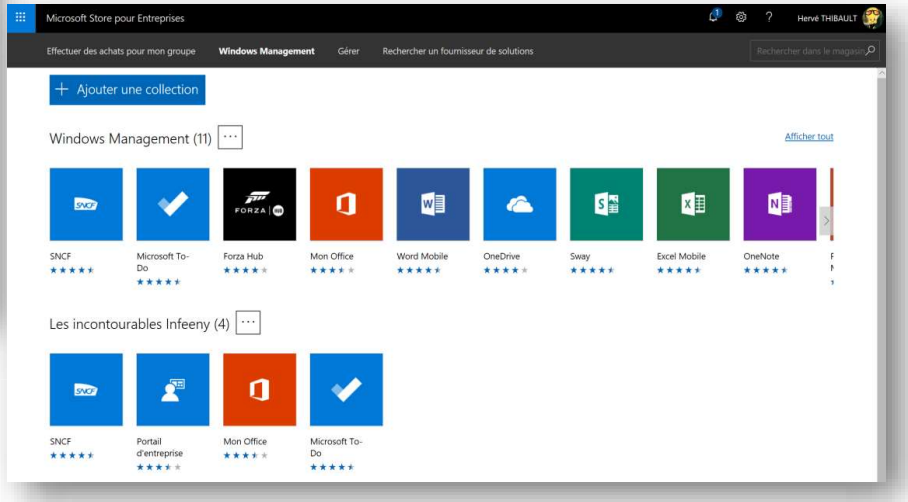


Microsoft

Azure AD Join & Windows 10







Microsoft

En synthèse

Azure Active Directory Premium :

- **Des utilisateurs** : Créés dans le cloud, importés depuis un fichier, synchronisés depuis un annuaire LDAP
- **Des groupes** : Pour donner accès à des applications (Cloud ou on-premise)
- **Une identité sécurisée** (MFA, rapports d'activité, protection de l'identité, …)

- Mais … pas de stratégies systèmes (GPOs)
  - Il faut utiliser **Microsoft Intune** (ou autre solution de MDM) !

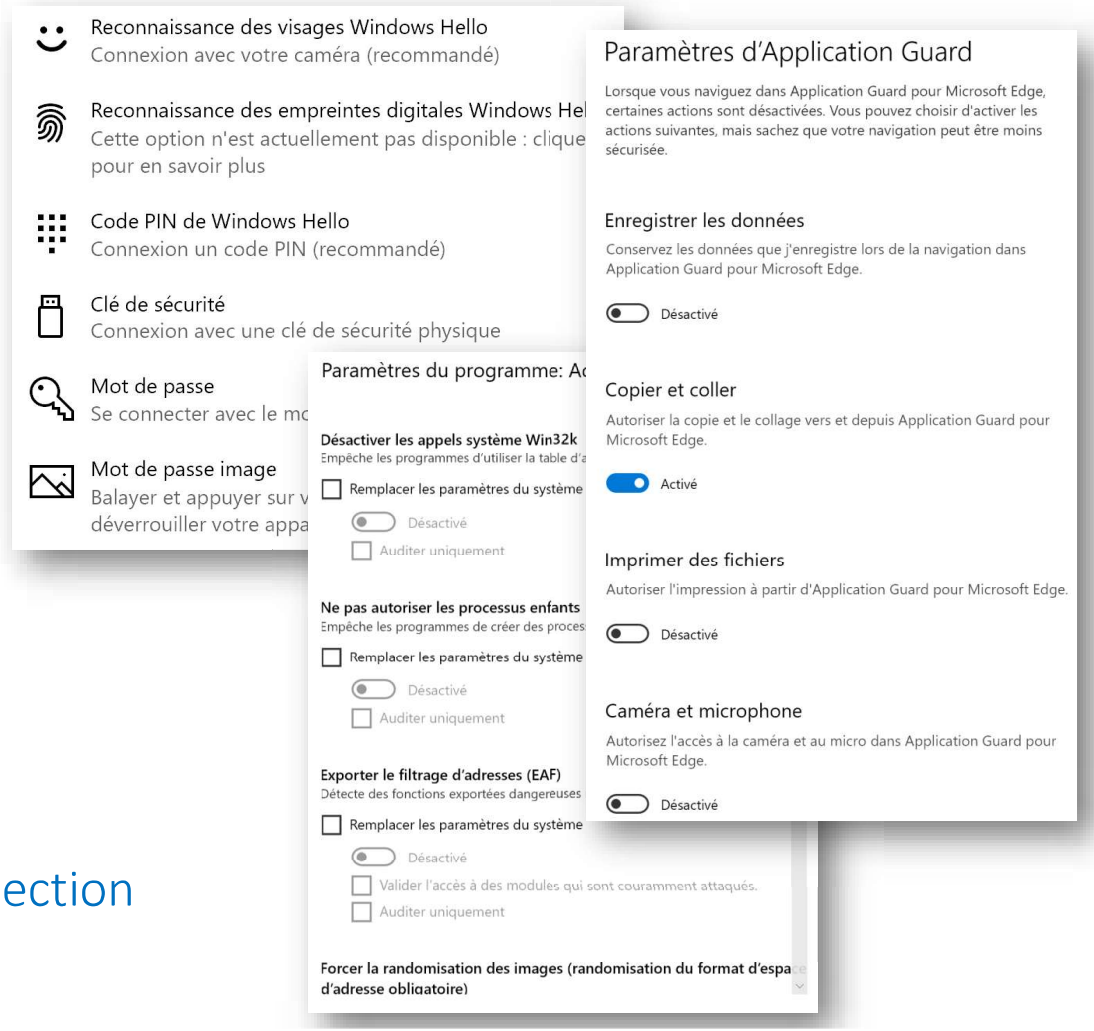
Microsoft

Modern Management

Secure Device, OS & Applications

Windows 10

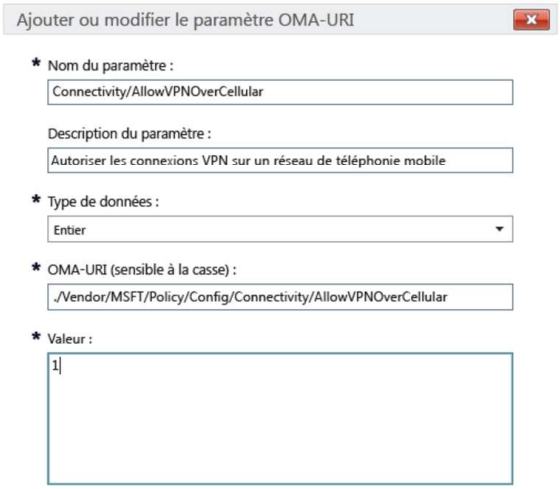
UEFI/secure Boot
Device Health Attestation
BitLocker
Applocker
Exploit Guard
Credential Guard
Application Guard
Windows Hello (clé de sécurité Fido2)
Windows Sandbox
Windows Defender Advanced Threat Protection



Gestion MDM dans Windows 10 – OMA-URI

- OMA-URI = Open Mobile Alliance - Uniform Resource Identifier : Paramètres standards utilisés par de nombreux fabricants d'appareils mobiles pour contrôler les fonctionnalités des appareils
- Permet de contrôler les fonctionnalités des appareils Windows 10 sans GPO Active Directory ou GPO locales
- Via WCD, SCCM, Intune, Airwatch, …
- Librairie de référence des paramètres qui peuvent être utilisés avec Windows 10 : https://docs.microsoft.com/fr-fr/windows/client-management/mdm/configuration-service-provider-reference

- **Nom du paramètre** : Affectez un nom unique au paramètre OMA-URI pour mieux l'identifier dans la liste des paramètres.
- **Description du paramètre** : Si vous le souhaitez, entrez une description du paramètre.
- **Type de données** : Choisissez parmi :
  - **Chaîne**
  - **Chaîne (XML)**
  - **Date et heure**
  - **Entier**
  - **Virgule flottante**
  - **Booléen**
- **OMA-URI (sensible à la casse)** : Spécifiez l'identificateur OMA-URI pour lequel vous voulez fournir un paramètre.
- **Valeur** : Spécifiez la valeur à associer à l'identificateur OMA-URI que vous avez entré.



Microsoft