Hes·so VALAIS WALLIS

Haute Ecole de Gestion
Hochschule für Wirtschaft

Filière Informatique de gestion
Studiengang Wirtschaftsinformatik

Travail de Bachelor 2021

Microsoft Security

Étudiant : **Kevin Coppey**

Professeur : **Xavier Barmaz**

Déposé le : **22 novembre 2021**

i. Résumé

Au début de l'année 2020, le monde a connu une crise sans précédent causée par la pandémie Covid-19. Cet événement a touché la Suisse, mais également le monde entier. En mars 2020, le Conseil Fédéral a pris la décision d'instaurer la pratique du télétravail comme usuelle. C'est ainsi qu'une moyenne de 34,1% de télétravailleurs a été atteinte en Suisse en 2020 (Bilan, 2021).

Dans cette optique, la plupart des entreprises ont dû proposer, bien souvent dans l'urgence, une alternative au travail traditionnel sur site.

Étant donné que la majorité des entreprises base leurs systèmes d'exploitation sur Windows, selon la dernière étude de StatCounter Global Stats (2021), il est intéressant de se poser les questions suivantes : « Comment protéger les appareils Windows nomades à l'intérieur et en dehors de la structure d'une entreprise ? », « Quels sont les outils que Microsoft met à notre disposition pour garantir une protection maximale » et « Quels sont les infrastructures à privilégier par les entreprises dans un cadre de protection des appareils clients ? ».

Microsoft propose, depuis plusieurs années, une alternative à l'installation sur site de toute l'infrastructure avec son service nommé « Azure ». Cette alternative utilise la technologie de l'informatique en nuage pour proposer à ses clients un service accessible dans le monde entier.

Ainsi, ce travail consiste à déterminer quelle est la meilleure solution entre une architecture sur site, en nuage, ou hybride dans le cadre d'un potentiel usage nomade.

Le recensement de toutes les solutions permettant une gestion des points de terminaison ainsi que l'analyse dûment réalisée, nous permettent d'affirmer que les réponses aux questions posées plus haut se trouve dans le Cloud.

Par conséquent, nous invitons le lecteur à prendre connaissance, à travers ce travail de Bachelor, des éléments qui impliquent ce choix et l'utilisation qui en résulte.

Mots-clés : sécurité Microsoft, endpoints security, Cloud, télétravail, Azure.

ii. Avant-propos

La formation dans la filière d'Informatique de gestion à la Haute École Spécialisée de Suisse Occidentale Valais/Wallis se conclue par un travail de Bachelor validant les trois ans d'études. Celui-ci nécessite un total de 360 heures. Il est constitué d'un rapport écrit, dans lequel nous retrouvons un état de l'art de la situation actuelle, d'une hypothèse à envisager ainsi qu'une partie pratique qui accompagne l'analyse. Une défense orale vient s'ajouter à la partie écrite afin de permettre à l'étudiant de présenter son projet et ses conclusions.

La réalisation de ce travail se base sur les solutions de sécurité proposées par Microsoft afin de déterminer quelle est la solution la plus adéquate à suivre en 2021 en ce qui concerne le choix d'une infrastructure sur site, Cloud ou encore en choisissant un mix des deux précédentes. Nous posons une hypothèse pour trouver cette solution.

Le projet ci-présent a été proposé et est suivi par le Professeur Xavier Barmaz de la Haute école spécialisée de Suisse Occidentale, dans la filière d'informatique de gestion.

Depuis ma découverte pour la sécurité informatique en 2020 grâce au module 634-2 dédié à l'enseignement des tenants et aboutissants d'une protection informatique, j'ai décidé d'orienter ma recherche de carrière dans ce domaine. C'est dans cette logique qu'un travail de Bachelor relatif au domaine me permet de mettre en application les notions que j'ai pu acquérir durant ma formation. De plus, le domaine de la cybersécurité, en constante expansion, me paraît un choix de carrière judicieux. Ainsi, ce document se présente autant comme un défi que comme un passeport pour le monde professionnel.

La principale difficulté rencontrée est sans doute la rigueur demandée lors du recensement des solutions dans l'état de l'art ainsi que le choix des critères nécessaires à la réalisation de la matrice de comparaison.

Une bonne connaissance du système d'exploitation de Microsoft, de la plateforme cloud « Azure », du fonctionnement des réseaux informatiques ainsi qu'un intérêt pour la cybersécurité sont des compétences cruciales dans la réalisation de ce document.

iii. Remerciements

Nous tenons principalement à remercier le Professeur Xavier Barmaz pour ses précieux conseils et sa haute disponibilité. Grâce à ses directives, sa rigueur et ses remarques, le processus de réalisation de ce document s'est déroulé convenablement.

Nous remercions l'ensemble du personnel administratif de la HES-SO Valais/Wallis et, plus particulièrement, Madame Catherine Tacchini pour ses indications.

Également, nous souhaitons saluer amis et membres de la famille pour leur soutient tant moral et matériel particulièrement important. Madame Oumayma Ouahouda et Madame Lara Dalla Pieta ont été d'une aide précieuse en ce qui concerne la relecture du document.

iv. Table des matières

v. Liste des figures

vi. Liste des tableaux

vii. Liste des abréviations

AAD	:	De l'anglais « Azure Active Directory ».
AADJ	:	De l'anglais « Azure Active Directory Joined ».
AD	:	De l'anglais « Active Directory ».
AD DS	:	De l'anglais « Active Directory Domain Services ».
API	:	De l'anglais « Application Programming Interface ».
BYOD	:	De l'anglais « Bring your own device ».
CC	:	De l'anglais « Computer Configuration ».
CISA	:	Cybersecurity and Infrastructure Security Agency.
CPU	:	De l'anglais « Central Process Unit ».
CSP	:	De l'anglais « Configuration Service Provider ».
CVE	:	De l'anglais « Common Vulnerabilities and Exposures ».
DNS	:	De l'anglais « Domain Name System ».
EMET	:	De l'anglais « Enhance Mitigation Expérience Toolkit ».
EMS	:	Microsoft Enterprise Mobility + Security.
FBI	:	Federal Bureau of Investigation.
HES-SO	:	Haute école spécialisée de Suisse occidentale.
GPO	:	De l'anglais « Group Policy Object ».
HVCI	:	De l'anglais « Hypervisor-Pretected Code Integrity ».
IaaS	:	De l'anglais « Infrastructure as a Service ».
IP	:	De l'anglais « Internet Protocol ».
MDE	:	Microsoft Defender for Endpoint.
MEM	:	Microsoft Endpoint Manager.
MEMAC	:	Microsoft Endpoint Manager Admin Center.

NIS	:	De l'anglais « Network Inspection System ».
OEM	:	De l'anglais « Original Equipement Manufacturer ».
OU	:	De l'anglais « Organizational Unit ».
PaaS	:	De l'anglais « Platform as a Service ».
PIN	:	De l'anglais « Personal Identification Number ».
RAM	:	De l'anglais « Random Access Memory ».
RSSI	:	De l'anglais « Received Signal Strength Indication ».
SaaS	:	De l'anglais « Software as a Service ».
SAM	:	De l'anglais « Security Account Manager ».
SCCM	:	System Center Configuration Manager.
SSO	:	De l'anglais « Single Sign-On ».
TCP	:	De l'anglais « Transmission Control Protocol ».
TPM	:	De l'anglais « Trusted Platform Module ».
UC	:	De l'anglais « User Configuration ».
UDP	:	De l'anglais « User Datagram Protocol ».
UEFI	:	De l'anglais « Unified Extensible Firmware Interface ».
URL	:	De l'anglais « Uniform Resource Locator ».
USB	:	De l'anglais « Universal Serial Bus ».
VBS	:	De l'anglais « Virtualization-based Security ».
VPN	:	De l'anglais « Virtual Private Network ».
XML	:	De l'anglais « Extensible Markup Language ».

Introduction

Depuis l'essor de la pandémie Covid-19, le monde a dû s'adapter. C'est pourquoi, nous avons vu une montée du télétravail et de l'utilisation du terme « BYOD » dans notre quotidien.

Des questions propres à la sécurité des appareils en dehors de l'environnement interne de l'entreprise se sont alors posées. Comment faire pour garantir le même degré de sécurité à distance ? Peut-on continuer à développer un environnement dit « On-Premise » tout en garantissant la sécurité des appareils nomades ?

Bien avant la pandémie, en 2008, Microsoft a annoncé son ambition de créer une plateforme de « cloud computing » que l'on connaît aujourd'hui sous le nom de « Azure ». Celle-ci propose aux particuliers comme aux professionnels une utilisation de ses services de manière partielle ou totalement décentralisée. En d'autres termes, l'utilisateur loue les services de Microsoft pour bénéficier de l'infrastructure qu'il lui plaît, sans avoir besoin de monter une solution en interne.

Par conséquent, dans ce document, nous développons les trois infrastructures (On-Premise, Cloud et Hybride) afin de donner une ligne directrice au lecteur de ce travail dans son choix.

Ce faisant, un état de l'art pour la sécurité native des clients et de ces infrastructures est réalisé afin de décrire ce qu'il se passe actuellement sur le marché de la sécurité Microsoft.

Lorsque les solutions sont recensées, nous passons à la partie analyse. Cette dernière appose des critères pour déterminer quelle solution nous retenons selon l'hypothèse retenue.

La partie d'application de ce document suit directement la partie analyse. En effet, lorsqu'un choix est effectué entre On-Premise, Cloud ou Hybride, nous mettons en application le résultat de notre analyse via des cas d'utilisation représentés sous la forme de guide.

Pour aller plus loin dans le sujet, nous proposons une stratégie de migration vers un environnement Cloud. De plus, nous comparons également les solutions de protection de Microsoft avec ses concurrents sur le marché.

1. État de l’art

Dans cette partie de ce travail de Bachelor, nous nous intéressons à recenser les solutions existantes pour chaque type d’infrastructure.

La première étape que nous présentons est la description des solutions proposées nativement par Microsoft concernant la sécurité d’une machine cliente fonctionnant sur Windows.

La deuxième étape s’intéresse aux solutions sur site, aussi appelées « On-Premise ». Celles-ci partent du principe que le serveur qui gère le service atteignable appartient à l’entreprise dans laquelle nous travaillons (IONOS, 2020).

Pour la troisième étape de cette rubrique, nous décrivons les solutions dites « Cloud » permettant, selon Bastien L., de livrer des ressources et des services à la demande par internet (Bastien L., 2017b).

La dernière partie de cette rubrique propose un mix entre les services utilisés dans un cadre On-Premise et Cloud afin de tirer le meilleure parti des deux infrastructures.

1.1. Solutions natives à la sécurité Windows Client-Side (Laptop)

Microsoft propose, avec son système d'exploitation Windows, des solutions de sécurité permettant de lutter contre les menaces externes exercées par des potentiels pirates informatiques.

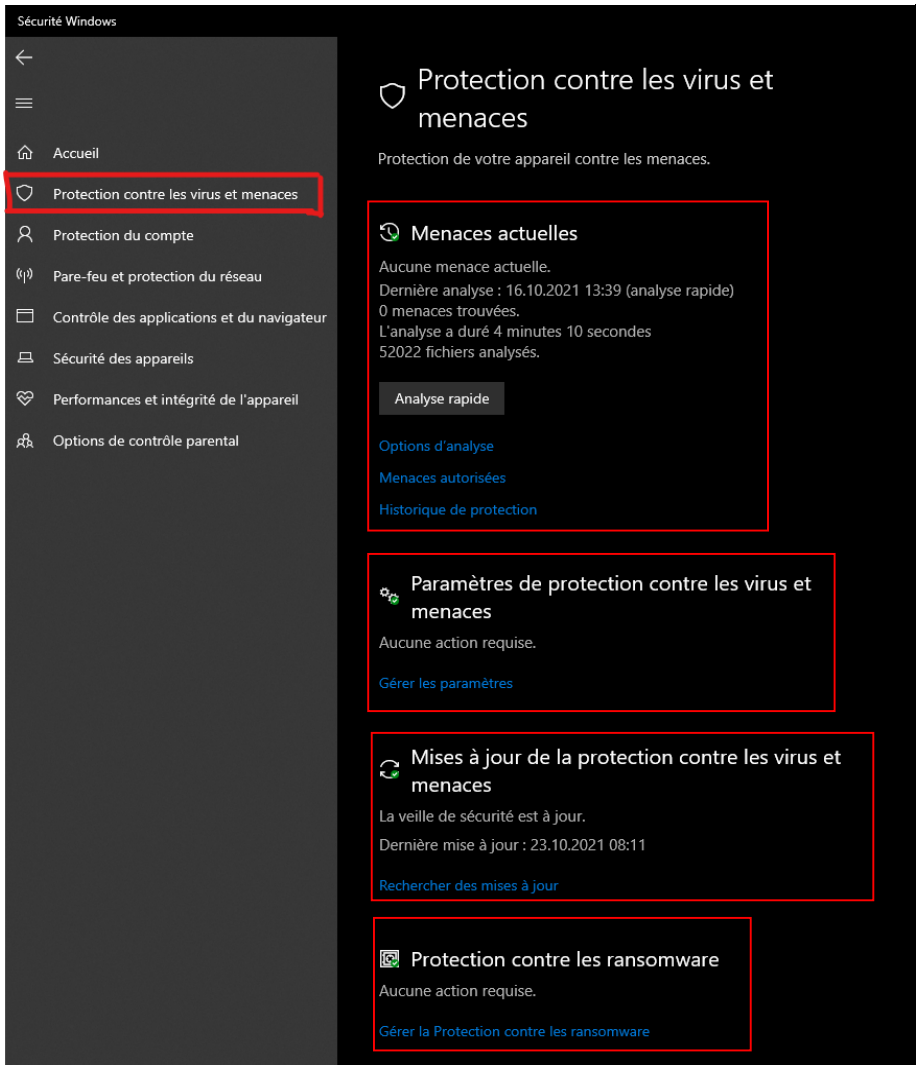
Selon McFarland (2021), les versions récentes de Windows disposent de plusieurs fonctionnalités se révélant intéressantes dans un contexte professionnel. Le but étant de garantir à ses utilisateurs un environnement fiable en proposant tout un panel d'outils de sécurité afin d'améliorer la confiance accordée à Microsoft chez l'utilisateur.

Ainsi, nous décrivons les solutions présentes dans la suite « Sécurité Windows » :

1) Protection contre les virus et les menaces
2) Protection des comptes
3) Pare-feu et protection du réseau
4) Contrôle des applications et du navigateur
5) Sécurité des appareils

1.1.1. Protection contre les virus et menaces

Figure 1 - Sécurité Windows Menu Protection contre les virus et menaces (Source : Auteur)



Windows/Paramètres/Sécurité Windows/Protection contre les virus et menaces

Sur le marché de l'antivirus, nombreux sont les acteurs qui essaient de se démarquer de la concurrence. Selon Paul Thurrott (2006), Microsoft se joint également à la partie en proposant depuis 2006, une solution de sécurité nommée « Windows Defender ».

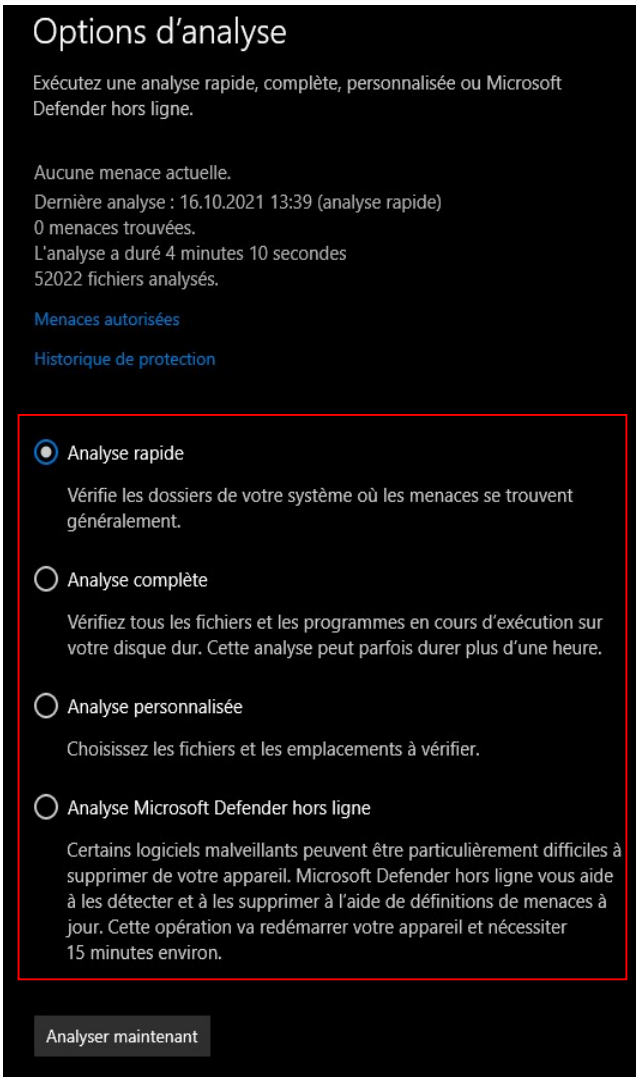
Depuis, Microsoft a amélioré son service pour constituer un des piliers centraux de la sécurité de son système d'exploitation en créant la solution « Sécurité Windows » présente sur toutes les machines récentes. A noter que celles-ci considèrent l'antivirus Microsoft Defender comme étant la solution par défaut. Dans le cas où un autre anti-malware est installé, la Sécurité Windows va désactiver Microsoft Defender, tout en fonctionnant de la même manière qu'avec ce dernier (Microsoft, s.d.-f).

La section « Protection contre les virus et menaces » permet de consulter les informations et les paramètres relatifs à la protection antivirus à partir de Microsoft Antivirus Defender et des produits antivirus tiers.

Nous passons maintenant à la description des fonctionnalités proposées par ce service de protection.

1.1.1.1. Menaces actuelles

Figure 2 - Sécurité Windows Menu Menaces actuelles
(Source : Auteur)



Windows/Paramètres/Sécurité Windows/Protection contre les virus et menaces/Menaces actuelles/Option d'analyse

La rubrique « Menaces actuelles » permet de lancer une analyse rapide ou complète du système afin de détecter des éventuels malwares.

L'analyse rapide vérifie les dossiers systèmes dans lesquels se trouvent généralement les menaces. Cette option permet de bénéficier d'un test rapide.

En revanche, l'analyse complète permet de bénéficier d'une analyse en profondeur de tous les fichiers et programmes présents sur la machine. Dépendant du nombre et du poids de ceux-ci, ce type d'analyse peut durer bien plus longtemps.

Accessoirement, l'utilisateur a la possibilité de lancer une analyse personnalisée en choisissant directement les emplacements du ou des disques durs à vérifier.

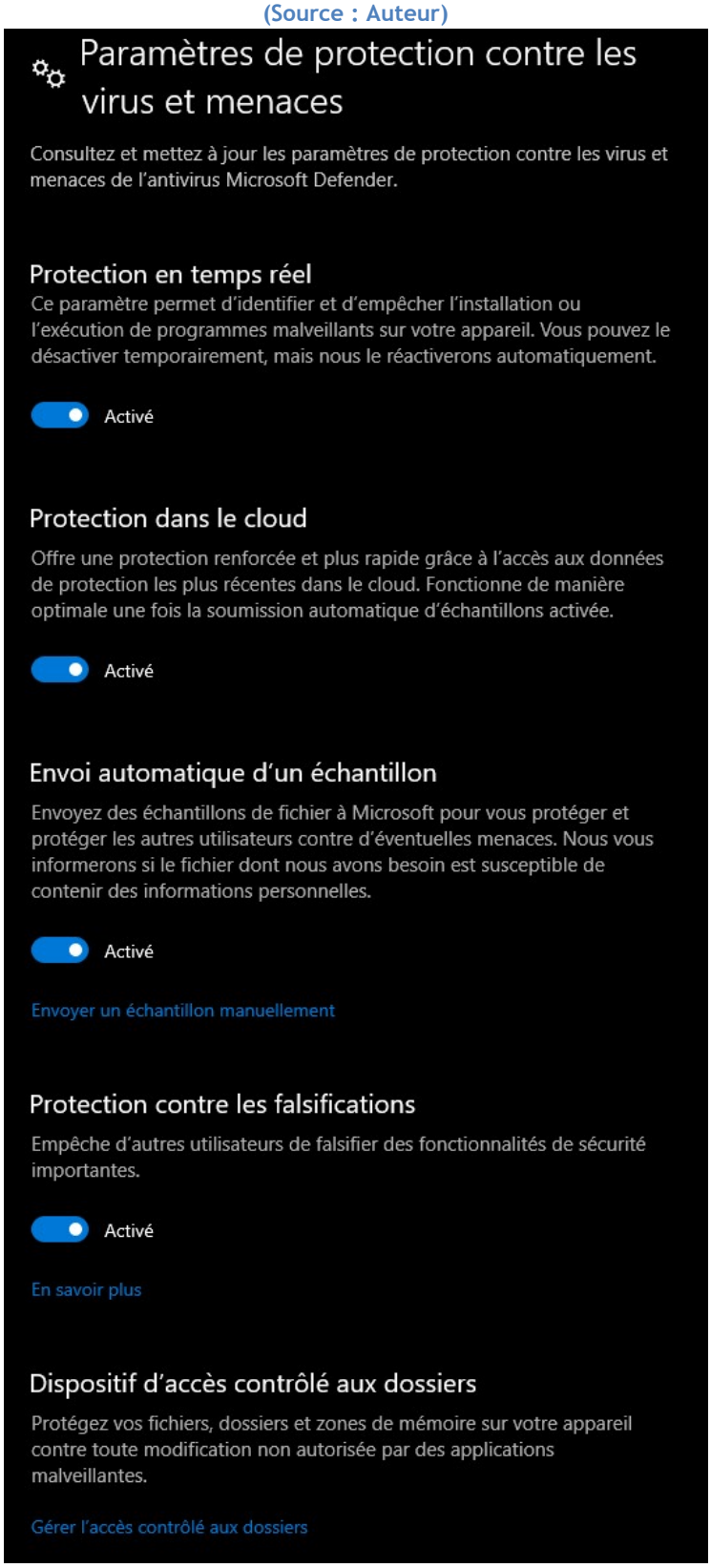
La dernière possibilité est de lancer une analyse Microsoft Defender hors ligne. Celle-ci peut être déclenchée à tout moment. Microsoft recommande d'utiliser cette option lorsqu'il y a une suspicion de logiciels malveillants sur la machine cliente ou lors d'un soupçon de non-détection d'un malware. L'utilisation de Microsoft Defender hors ligne permet également de se débarrasser des malwares les plus persistants en appliquant un nettoyage supplémentaire (Microsoft, s.d.-e).

Les résultats des analyses sont présents dans l'historique des menaces sous la même rubrique.

1.1.1.2. Paramètres de protection contre les virus et menaces

Cette rubrique permet de personnaliser les paramètres de l'antivirus Microsoft Defender.

Figure 3 - Sécurité Windows Menu Paramètres de protection contre les virus et menaces 1
(Source : Auteur)



Windows/Paramètres/Sécurité Windows/Protection contre les virus et menaces/Paramètres de protection contre les virus et menaces/Gérer les paramètres

La protection dans le cloud permet de bénéficier de la puissance de calcul des serveurs de Microsoft pour identifier les menaces, même bien avant leur détection par le système.

La troisième fonctionnalité présente dans cette rubrique est l'envoi automatique d'un échantillon. Celle-ci permet, lorsqu'elle est activée, d'envoyer automatiquement des échantillons de fichier à Microsoft. La société garantit un avertissement à l'utilisateur si des métadonnées sont susceptibles de contenir des informations personnelles (*Windows 10 Famille*, 2021).

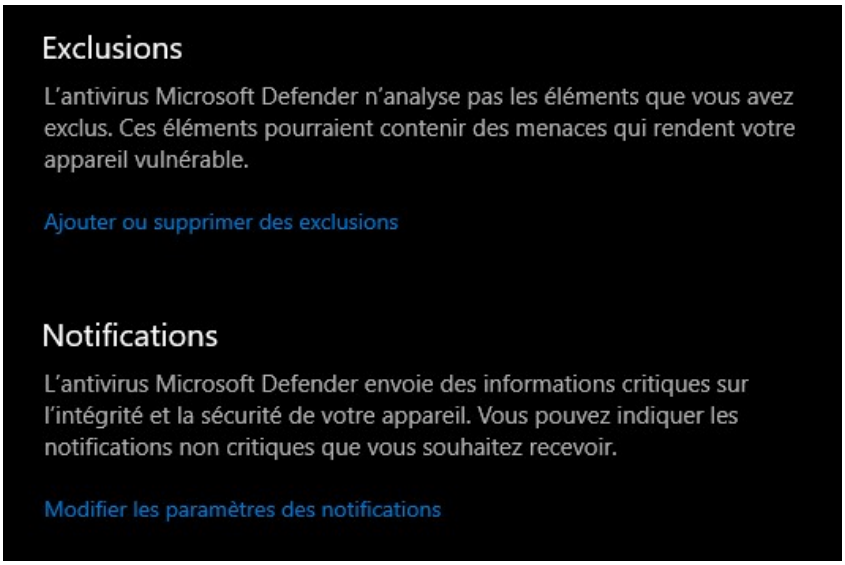
Il est également possible d'envoyer un échantillon manuellement en sélectionnant l'option « Envoyer un échantillon manuellement » qui nous redirige vers un site internet pour faire notre soumission.

La protection contre la falsification est utile pour empêcher des applications de modifier des paramètres importants de Microsoft Defender comme la protection en temps réel citée plus haut. Cela permet d'empêcher une application de désactiver l'antivirus par exemple.

Comme toute solution antivirus, Microsoft Defender dispose d'une fonctionnalité d'exclusion permettant d'empêcher l'analyse d'éléments ou zones de mémoire de la machine de l'utilisateur. Pour ce faire, il suffit d'indiquer le chemin système à exclure.

Et dernièrement, il est possible de modifier les paramètres de notification sur la sécurité que l'utilisateur souhaite recevoir.

Figure 4 - Sécurité Windows Menu Paramètres de protection contre les virus et menaces 2
(Source : Auteur)



Windows/Paramètres/Sécurité Windows/Protection contre les virus et menaces/Paramètres de protection contre les virus et menaces/Gérer les paramètres

1.1.1.3. Mises à jour de la protection contre les virus et menaces

Figure 5 - Sécurité Windows Menu Mises à jour de la protection contre les virus et menaces
(Source : Auteur)

Windows/Paramètres/Sécurité Windows/Protection contre les virus et menaces/Mise à jour de la protection contre les virus et menaces/Rechercher des mises à jour

Afin de garantir une protection du système accrue, Microsoft propose des mises à jour régulières permettant de lutter contre les failles de sécurités. En effet, les hackers sont très actifs dans leurs découvertes afin de les exploiter. C'est pourquoi, Microsoft a la nécessité de toujours proposer des correctifs de sécurité.

Par conséquent, Windows alerte l'utilisateur à chaque fois qu'une nouvelle mise à jour est disponible. Il est cependant également possible de lancer une recherche manuellement.

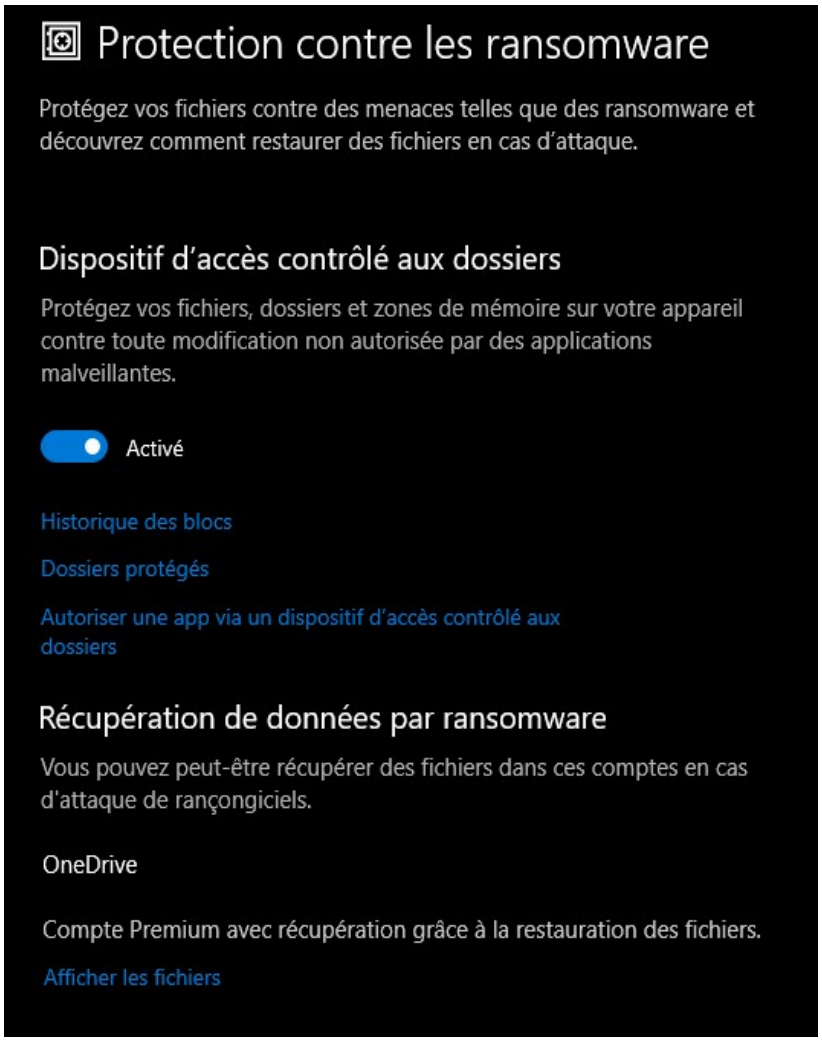
1.1.1.4. Protection contre les ransomware

Selon une étude de l'organisme Sophos (2021), 37% des entreprises ayant répondu au sondage, constituant un échantillon de 5'400 entités, ont subi une attaque par rançongiciel.

Microsoft réagit à ce pourcentage en proposant sa propre protection native sur tous les appareils Windows contre les ransomware via l'option « Protection contre les ransomware ».

L'option « Dispositif d'accès contrôlé aux dossiers » permet d'empêcher une application de procéder à la modification d'un ou plusieurs fichiers, dossiers ou plus généralement des zones de mémoire de l'appareil. Cette fonctionnalité est particulièrement utilisée comme mesure de défense contre les ransomwares qui chiffre les fichiers.

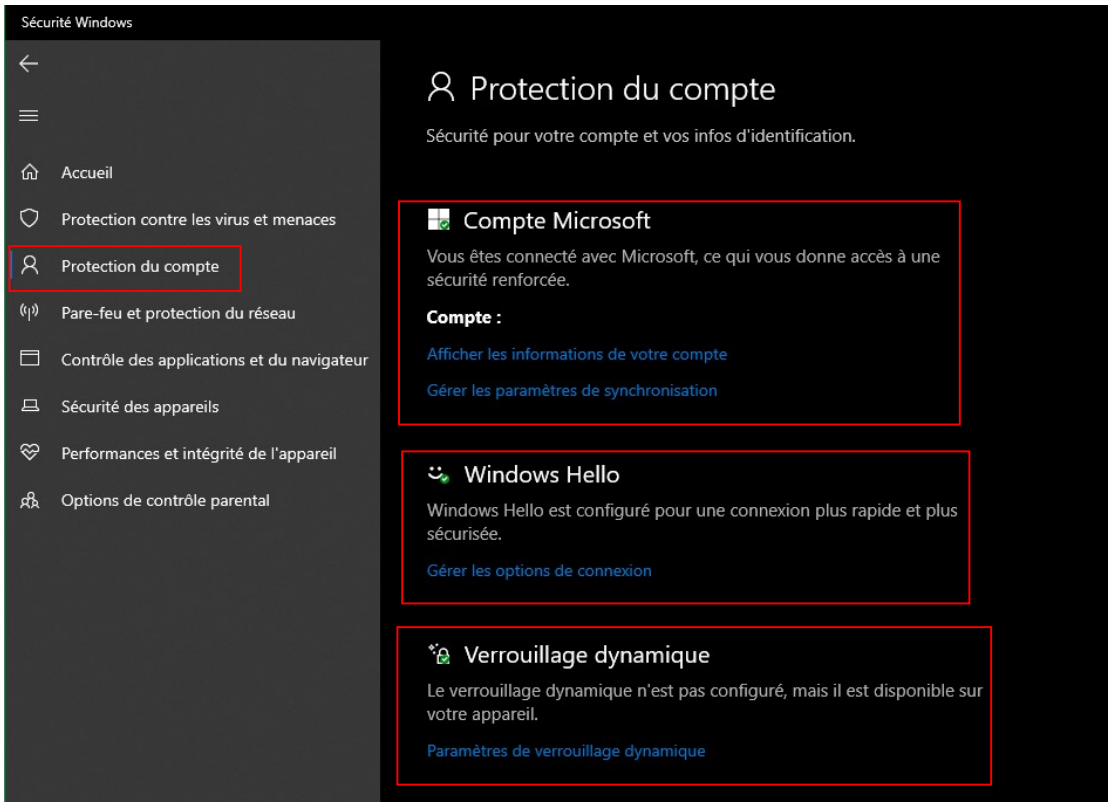
Figure 6 - Sécurité Windows Menu Protection contre les ransomware (Source : Auteur)



Windows/Paramètres/Sécurité Windows/Protection contre les virus et menaces/Protection contre les ransomware/Gérer la Protection contre les ransomware

1.1.2. Protection du compte

Figure 7 - Sécurité Windows Menu Protection du compte
(Source : Auteur)



Windows/Paramètres/Sécurité Windows/Protection du compte

Afin de rallier tous les services proposés par Microsoft sous une seule identité, il est possible de créer un compte Microsoft. Celui-ci permet d'utiliser les mêmes identifiants de connexion sur tous les services proposés par l'entreprise.

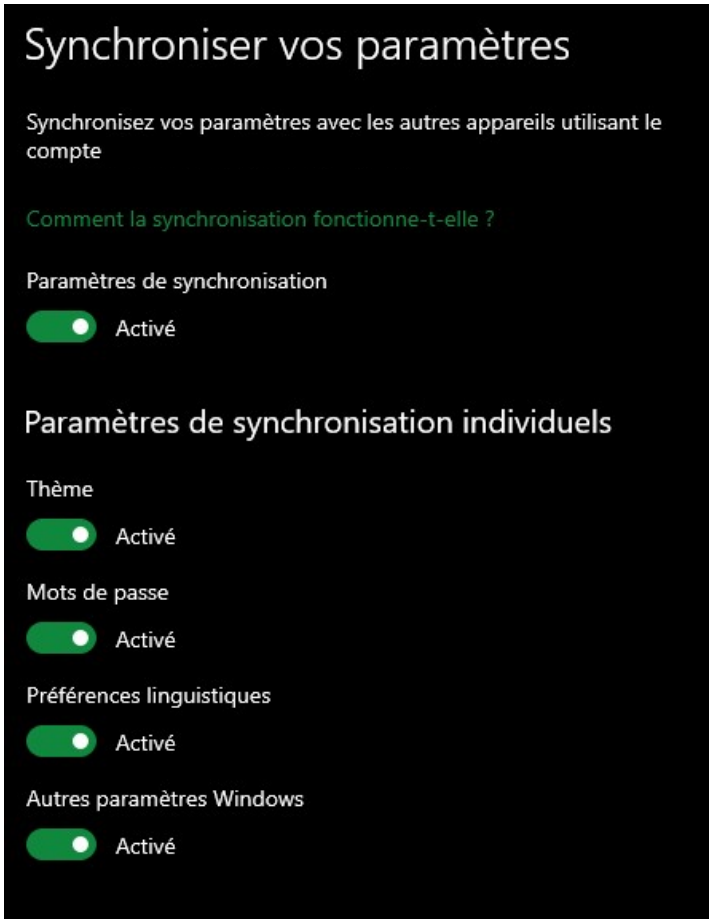
Lors de l'étape de l'ouverture de session Windows, le système d'exploitation demande à l'utilisateur de renseigner ses informations de connexion. Sans cela, il est impossible d'atteindre la session de l'utilisateur.

L'utilisation d'un compte Microsoft permet de sauvegarder certains paramètres de personnalisation de la session afin de les récupérer sur un autre appareil.

Il est néanmoins également possible de créer un compte local qui va stocker les informations de connexion localement dans la base de registre Windows. Cependant, nous ne recommandons pas de passer par cette solution.

Nous détaillons ici les mesures mises en place par Microsoft relatives à la protection du compte de l'utilisateur.

Figure 8 - Paramètres de compte synchronisables
(Source : Auteur)



Windows/Paramètres/Sécurité Windows/Protection du compte/Compte Microsoft/Gérer les paramètres de synchronisation

1.1.2.1. Compte Microsoft/Compte local

Comme expliqué plus haut, Microsoft donne la possibilité de créer un compte pour tous ses services. Plus simplement, un compte créé pour ouvrir sa session Windows est le même que celui utilisé pour son compte Microsoft Office par exemple. Cela permet de tout centraliser grâce à une seule paire d'identifiants (SSO).

Cette paire d'identifiant est constituée de deux éléments :

- Une adresse électronique ou un numéro de téléphone
- Un mot de passe

Il n'est pas obligatoire d'utiliser une adresse électronique créée sur un domaine appartenant à Microsoft. Il est très bien possible de créer un compte Microsoft en utilisant une adresse d'une entreprise tierce.

Le mot de passe doit quant à lui contenir au moins 8 caractères avec au moins deux des catégories suivantes : majuscules, minuscules, chiffres et symboles. Selon Charlotte Empey (2018), employée chez Avast, un bon mot de passe se doit d'être long, de contenir plusieurs types de caractères (nombres, symboles, etc.), d'éviter le leetspeak (ex : DOORBELL qui devient D00R8377) et de ne pas utiliser des mots de passe connus (ex : « qwertz »).

Rien ne diffère dans le processus d'authentification en local. La seule différence est que le compte est local, stocké dans la base de données SAM, et ne permet pas de bénéficier des autres services de Microsoft.

1.1.2.2. Windows Hello

Depuis 2017, Microsoft communique sur sa stratégie « Passwordless ». Celle-ci repose sur le fait de ne plus utiliser de mots de passe car trop contraignants pour un utilisateur.

Cette stratégie repose principalement sur l'utilisation de Windows Hello.

Figure 9 - Sécurité Windows Menu Windows Hello
(Source : Auteur)

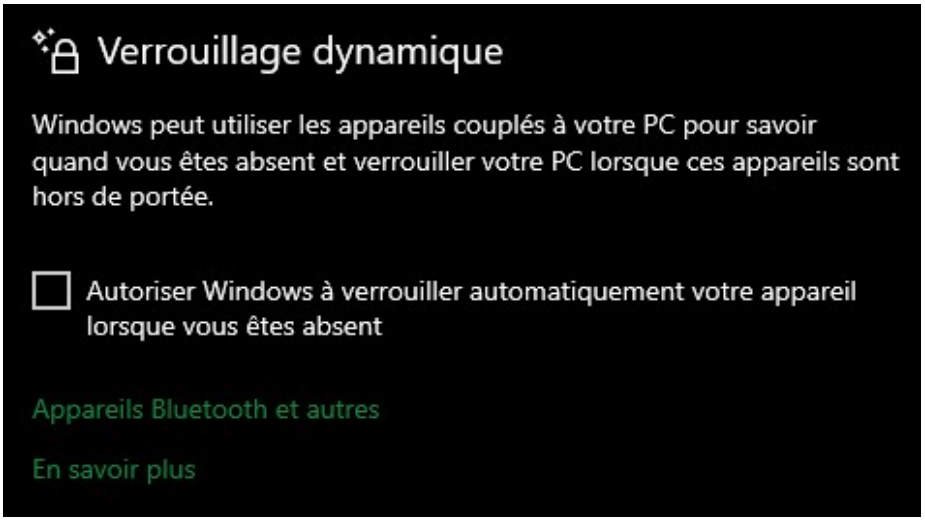
Windows/Paramètres/Sécurité Windows/Protection du compte/Windows Hello

Selon Microsoft, Windows Hello est plus sécurisé qu'un mot de passe et permet d'accéder plus rapidement à sa session à l'aide d'un PIN, de la reconnaissance faciale ou encore grâce à la reconnaissance biométrique par empreinte digitale. Le mode de connexion Windows Hello est propre à un appareil, ce qui veut dire que si un hacker possède notre PIN par exemple, il lui incombe également de se procurer notre appareil. Il est également sauvegardé pour une récupération du compte Microsoft (Microsoft, s.d.-a).

1.1.2.3. Verrouillage dynamique

Le verrouillage dynamique est une technologie disponible depuis Windows 10 version 1703 permettant d'appairer via bluetooth un appareil tiers afin de verrouiller la session lorsque ce dernier ne se trouve plus à proximité. Lorsque la valeur RSSI atteint un certain seuil correspondant à la force du signal, la session Windows va se verrouiller.

Figure 10 - Sécurité Windows Menu Verrouillage dynamique
(Source : Auteur)



Windows/Paramètres/Sécurité Windows/Protection du compte/Verrouillage dynamique

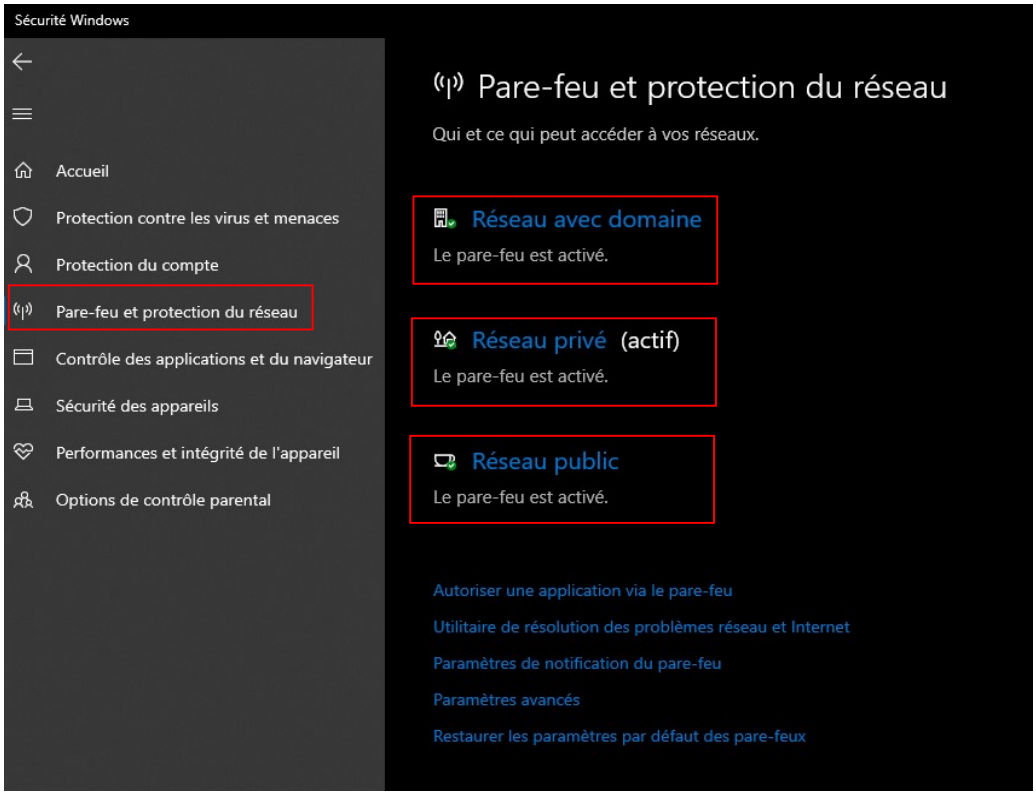
Voici comment le processus fonctionne :

Le signal de valeur d'attribut rssiMin indique la force nécessaire pour que l'appareil soit considéré comme « à portée ». La valeur par défaut -10 permet à un utilisateur de se déplacer dans un bureau ou un espace de travail de taille moyenne sans que Windows ne verrouille l'appareil. RssiMaxDelta a une valeur par défaut de -10, ce qui indique à Windows de verrouiller l'appareil une fois que la force du signal est resserrée de plus de 10 mesures. Les mesures RSSI sont relatives et diminuent à mesure que faiblissent les signaux Bluetooth entre les deux appareils couplés. Par conséquent, une mesure de 0 est plus puissante que -10, qui est plus puissant que -60, qui est un indicateur que les appareils s'éloignent de plus en plus l'un de l'autre (Microsoft, 2019c).

Il est possible d'appairer différents appareils. Le plus commun est de jumeler son téléphone portable avec la machine cliente Windows car il peut être facilement transportable et peut se ranger dans la poche d'un pantalon par exemple.

1.1.3. Pare-feu et protection réseau

Figure 11 - Sécurité Windows Menu Pare-feu et protection du réseau (Source : Auteur)



Windows/Paramètres/Sécurité Windows/Pare-feu et protection du réseau

Dans cette partie du document, nous nous intéressons à la sécurité de l'appareil face aux agressions par internet. Le pare-feu ou firewall en anglais, est un élément essentiel pour contrôler le trafic entrant et sortant du réseau.

Pour rappel, voici une définition donnée par Manuj Aggarwal (2018, p. 57) dans son livre *Network Security with pfSense* : « Un firewall est un appareil ou un logiciel dans le domaine de la sécurité des réseaux informatiques qui utilise une des règles pour contrôler le trafic entrant et sortant ». Ce qui veut dire que seulement le trafic autorisé par un ensemble de règles peut passer outre le pare-feu. Toutes les autres connexions sont rejetées. Il filtre la circulation dans le réseau par l'adresse IP de la source et de la destination et par le protocole de transport (ex : TCP ou UDP).

Le pare-feu est donc une solution idéale pour empêcher un utilisateur d'accéder ou de recevoir des paquets d'informations inconnus ayant un but malicieux.

Par défaut, le pare-feu utilisé est « Microsoft Pare-feu Windows Defender » qui est la solution native de Microsoft. Cependant, il est très bien possible d'en installer un autre venant d'une société tierce étant donnée la compatibilité expliquée plus haut de la solution « Windows Security ».

Microsoft possède une stratégie de firewall sur trois niveaux :

- Réseau avec domaine : Gestion des règles du pare-feu dans un réseau d'entreprise.
- Réseau privé : Gestion des règles du pare-feu dans un réseau privé (ex : Domicile privé).
- Réseau public : Gestion des règles du pare-feu dans un réseau public (ex : Restaurant).

Selon le réseau sur lequel l'appareil est connecté, « Windows Defender » va appliquer les règles configurées par défaut ou par l'utilisateur.

A savoir également qu'il est très bien possible de désactiver la protection à tout moment. Nous nous permettons d'avertir le lecteur que cette manœuvre doit être faite en toute connaissance de cause.

1.1.4. Contrôle des applications et du navigateur

Selon une récente étude, 75% des organisations à travers le monde ont connu une tentative se rapprochant à une attaque par hameçonnage en 2020 (Rosenthal, 2021).

Le « phishing » ou hameçonnage en français est une pratique d'attaque informatique répandue à notre époque. Une définition est donnée par le Federal Bureau of Investigation (FBI) :

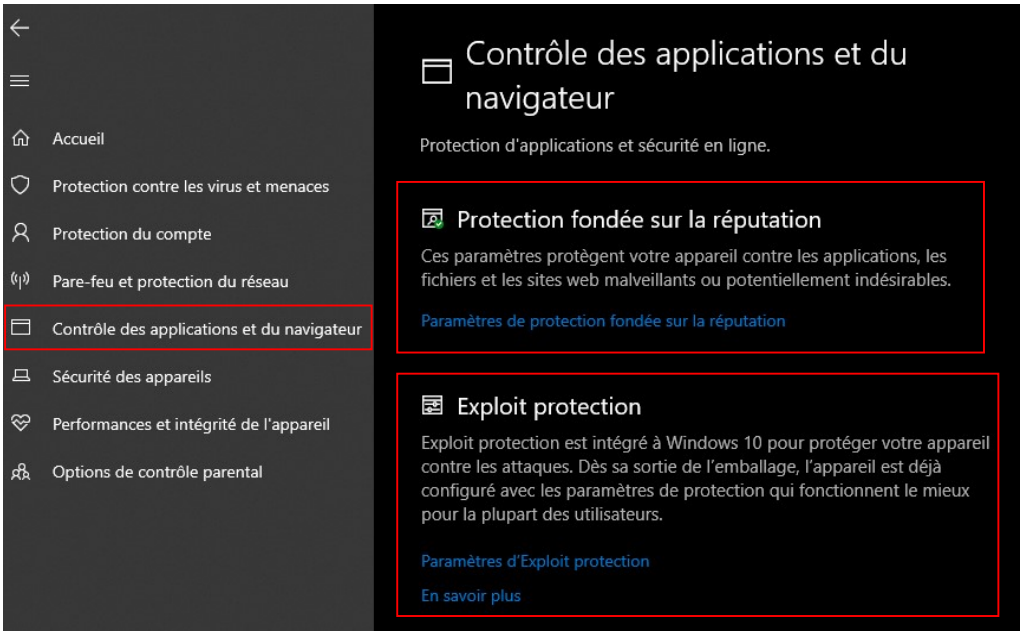
Le phishing est l'action d'envoyer un courrier électronique en prétendant faussement être une entreprise légitime dans le but de tromper le destinataire en lui demandant de divulguer des informations personnelles et sensibles telles que des mots de passe, des numéros de carte bancaire après avoir demandé à l'utilisateur de visiter un site internet spécifique. Le site en question n'est cependant pas authentique et a été créé uniquement dans le but de voler les informations de l'utilisateur (FBI, 2020).

Microsoft a décidé de réagir en proposant, dans sa solution de sécurité Windows, un moyen de lutter contre ces tentatives malveillantes en sécurisant également l'utilisation d'application et la navigation de l'utilisateur. Ce moyen porte le nom de « Microsoft Defender SmartScreen ».

Selon la documentation de Microsoft, « Microsoft Defender SmartScreen » est capable de déterminer si un site est potentiellement dangereux par :

- « Analyse des pages Web visitées, par la recherche de signes indiquant un comportement suspect. Si Microsoft Defender SmartScreen établit qu'une page est suspecte, une page d'avertissement s'affiche pour vous avertir. » (Microsoft, 2021g).
- « Comparaison des sites que vous visitez à une liste dynamique de signalement des sites d'hameçonnage et des logiciels malveillants. En cas de correspondance, Microsoft Defender SmartScreen affiche un avertissement informant l'utilisateur que le site pourrait être malveillant. » (Microsoft, 2021g).

Figure 12 - Sécurité Windows Menu Contrôle des applications et du navigateur (Source : Auteur)

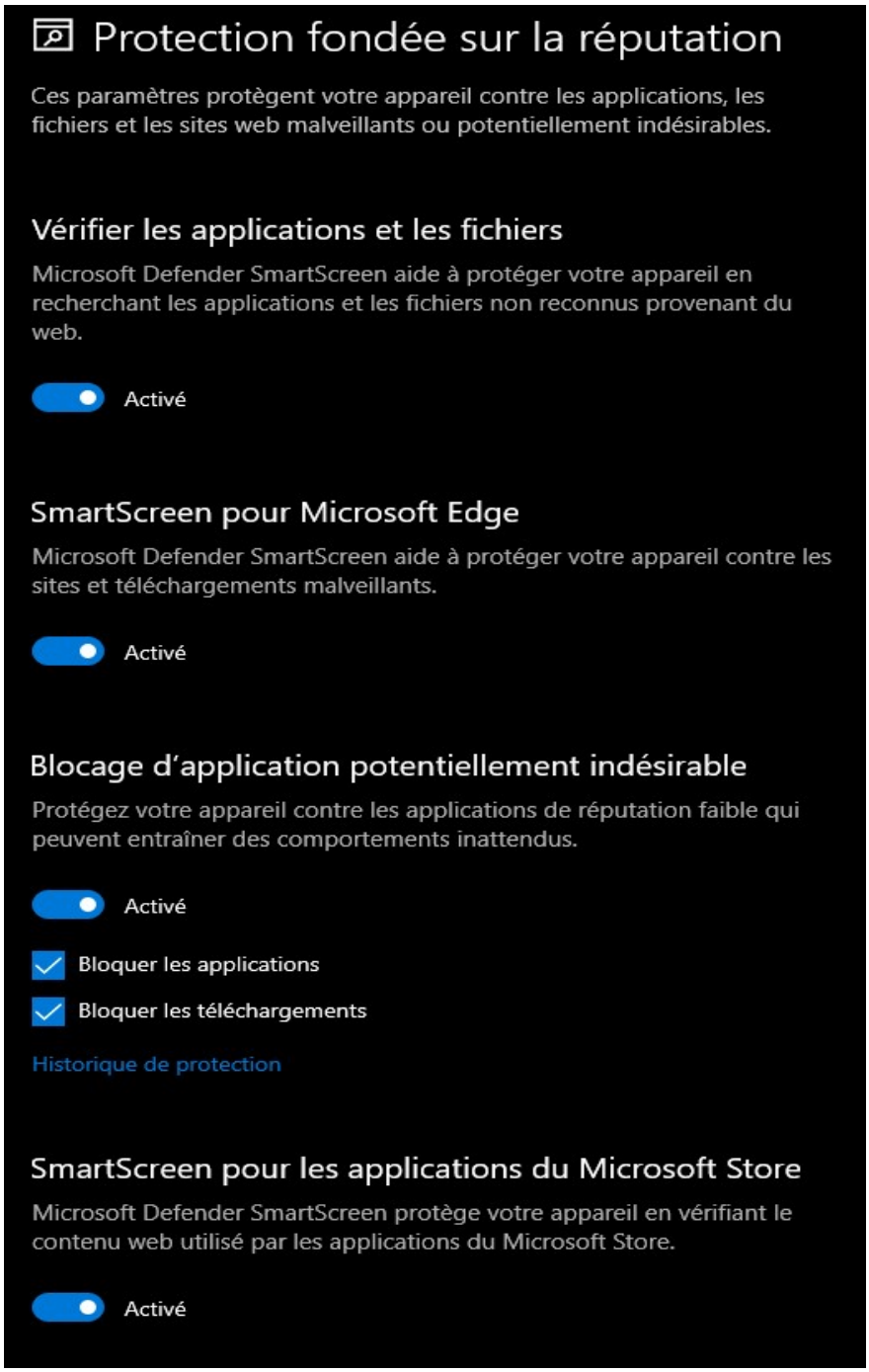


Windows/Paramètres/Sécurité Windows/Contrôle des applications et du navigateur

1.1.4.1. Protection fondée sur la réputation

Cette première section permet de paramétrer la protection de l'appareil « contre les applications, les fichiers et les sites web malveillants potentiellement indésirables » (*Windows 10 Famille*, 2021) grâce à la technologie « Microsoft Defender SmartScreen ».

Figure 13 - Sécurité Windows Menu
Protection fondée sur la réputation
(Source : Auteur)



Windows/Paramètres/Sécurité Windows/Contrôle des applications et du navigateur/Paramètres de protection fondée sur la réputation

Par conséquent, cette solution, si les paramètres sont activés, peut autant vérifier et bloquer la visite des sites internet que contrôler et également stopper les applications analysées comme étant néfastes pour le système.

Il est important de retenir que cette technologie est uniquement nativement disponible pour le navigateur de Microsoft : « Edge ». Il est également possible de l'activer sur d'autres navigateurs de type « Chromium » comme Google Chrome. Pour cela, il est nécessaire de télécharger l'extension officielle sur le chrome web store.

1.1.4.2. Exploit protection

La protection contre les codes malveillants exploitant une faille de sécurité est la nouvelle solution découlant directement de « Enhance Mitigation Expérience Toolkit » (EMET). Celui-ci est un utilitaire permettant de mitiger l'exploitation de faille présente dans des applications. Il n'est cependant plus maintenu à jour par Microsoft depuis le 31 juillet 2018 et est dorénavant remplacé par « Exploit protection » (Microsoft, s.d.-c).

Selon Peter van der Woude (2021), cet « Exploit protection » est donc utilisé pour empêcher la propagation d'une vulnérabilité ayant pour source le système d'exploitation en lui-même ou encore un programme quelconque. Cette mitigation va empêcher la faille de se répandre sur tout le système, voir même d'infecter d'autres appareils connectés.

Les paramètres de configuration se distinguent en deux catégories, les paramètres du programme et les paramètres systèmes.

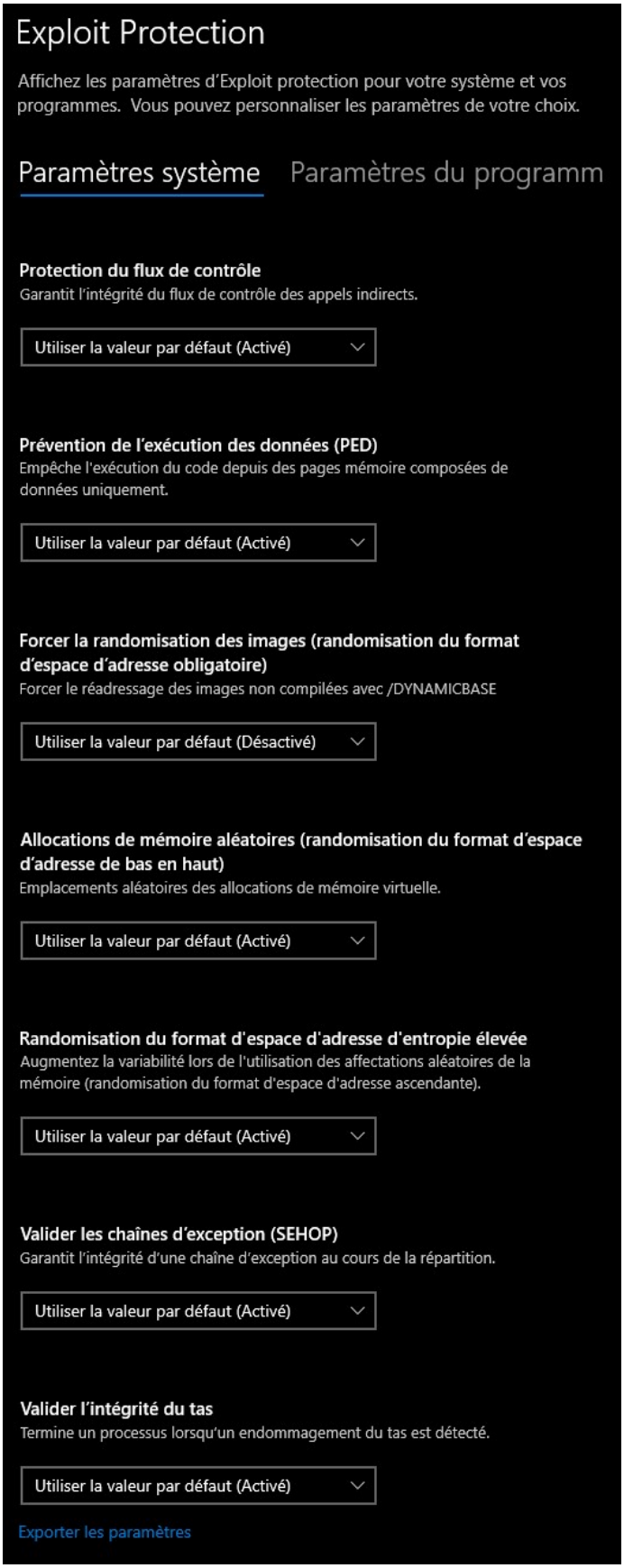
Les paramètres systèmes sont activés par défaut et sont maintenus directement par Microsoft. Il n'est donc pas possible pour un utilisateur d'ajouter une autre configuration que celles déjà proposées.

Les paramètres des applications sont, quant à eux, complètement personnalisables. En effet, il est possible de rajouter des programmes dans la liste, en plus de ceux déjà présents.

Lorsqu'un programme est ajouté, nous pouvons déterminer les paramètres de mitigation que nous souhaitons en fonction de nos besoins.

A noter qu'il est possible d'exporter sous format Extensible Markup Language (XML), la liste de tous les paramètres du programme ou du système.

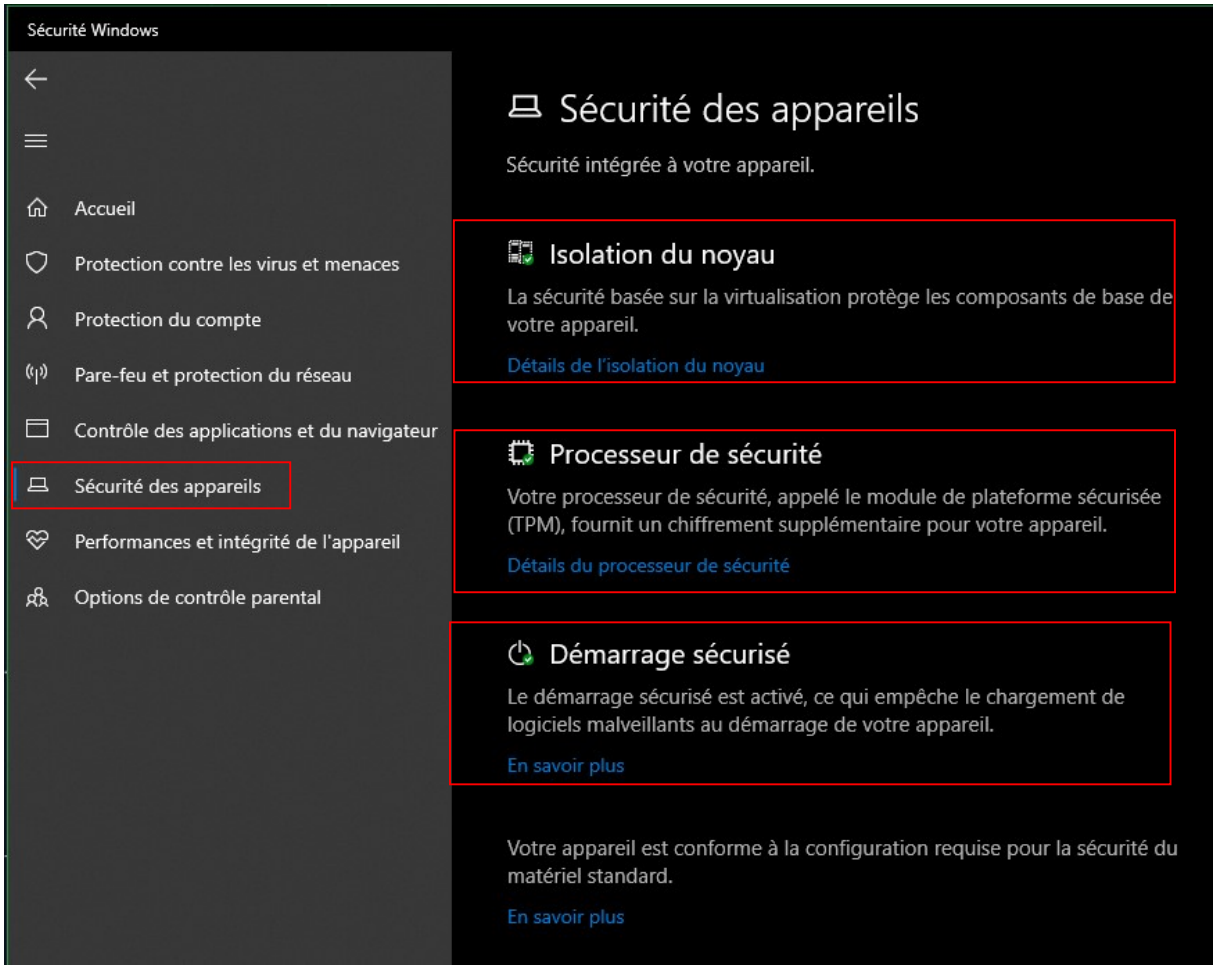
Figure 14 - Sécurité Windows Menu Exploit Protection (Source : Auteur)



Windows/Paramètres/Sécurité Windows/Contrôle des applications et du navigateur/Exploit Protection

1.1.5. Sécurité des appareils

Figure 15 - Sécurité Windows Menu Sécurité des appareils
(Source : Auteur)



Windows/Paramètres/Sécurité Windows/Sécurité des appareils

Depuis toujours, les hackers essaient de tester les limites de la sécurité imposée par les fabricants et les géants de la cybersécurité. En 2010 est découvert un des rootkits les plus connus de nos jours : « Stuxnet ». Celui-ci avait pour but d'endommager le programme nucléaire iranien (Clayton, 2012).

Un employé de chez Avast, donne la définition suivante d'un rootkit :

« Un rootkit est un progiciel conçu pour rester caché sur votre ordinateur tout en permettant l'accès et le contrôle à distance de ce dernier. Les pirates utilisent des rootkits pour manipuler votre ordinateur à votre insu. » (Belcic, 2021).

Ils sont en général indétectables ou très difficilement remarquables étant donné qu'ils évoluent à un niveau très bas.

Le bootkit est également un élément malveillant qui fait partie de la famille des rootkits. Selon Microsoft (2019b), celui-ci a comme spécificité de se lancer au moment où l'ordinateur démarre, avant le chargement du système d'exploitation ou durant celui-ci. Le bootkit permet donc au hacker d'obtenir le niveau de privilège le plus élevé (d'où le terme « root » qui est le terme désignant un compte administrateur sur les environnements Linux).

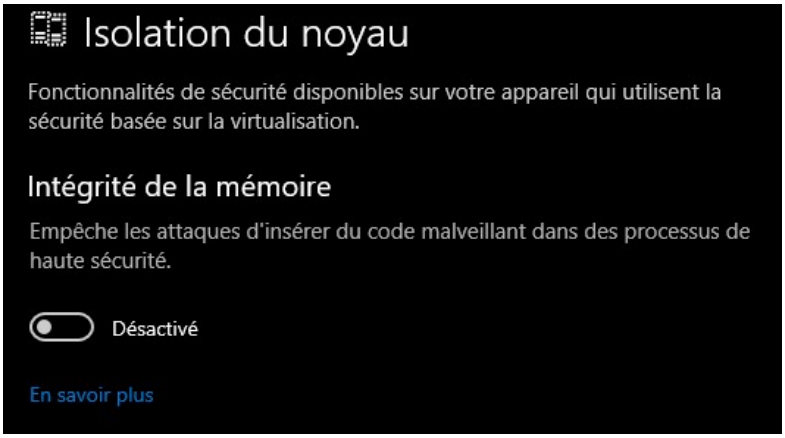
De plus, le rapport de sécurité de Microsoft, nommé « Security Signals » (2021a), annonce que plus de 83% des entreprises sondées ont connu une attaque de type micrologiciel, qui est encore une fois, une attaque visant les composants de bas niveau.

C'est pourquoi Microsoft propose dorénavant des systèmes de sécurité informatique permettant de lutter contre ce genre de malware dans les niveaux les plus bas des appareils.

1.1.5.1. Intégrité de la mémoire

Afin d'empêcher l'exécution de bouts de code malicieux à des niveaux très bas de l'appareil, Windows propose également d'isoler les processus principaux de Windows en les contenant dans un environnement virtuel.

Figure 16 - Sécurité Windows Menu Intégrité de la mémoire
(Source : Auteur)



Windows/Paramètres/Sécurité Windows/Sécurité des appareils/Isolation du noyau

> Le support technique de Microsoft nous soumet une simple analogie pour mieux comprendre :
>
> Pensez-y comme un agent de sécurité à l'intérieur d'un stand verrouillé. Cet environnement isolé (le stand verrouillé dans notre analogique) empêche la fonctionnalité d'intégrité de la mémoire d'être falsifiée par un pirate malveillant. Un programme qui souhaite exécuter un code potentiellement dangereux doit transmettre ce code à l'intégrité de la mémoire dans ce stand virtuel pour pouvoir le vérifier. Lorsque l'intégrité de la mémoire est confortable *[sic]*, le code est sécurisé, il le dirige vers Windows'exécuter *[sic]*. En règle générale, cela [le processus de vérification] se produit très rapidement (Microsoft, s.d.-d).

Plus techniquement parlant, selon la documentation officielle de Microsoft (2021o), l'intégrité de la mémoire (HVCI) et la sécurité basée sur la virtualisation (VBS) coopère pour améliorer le degré de sécurité du noyau Windows. VBS utilise l'hyperviseur natif, qui est le processus de virtualisation de Windows, pour créer une base vierge sur laquelle l'HVCI va se baser pour identifier d'éventuelles modifications.

1.1.5.2. Trusted Platform Module (TPM)

Depuis l'annonce de Windows 11, la nouvelle itération du système d'exploitation de Microsoft, le grand public a pu prendre connaissance du TPM ou module de plate-forme sécurisée. Windows base une partie de sa sécurité sur cet élément, c'est pourquoi il est fortement recommandé par Microsoft de la posséder autant pour Windows 11 que pour Windows 10.

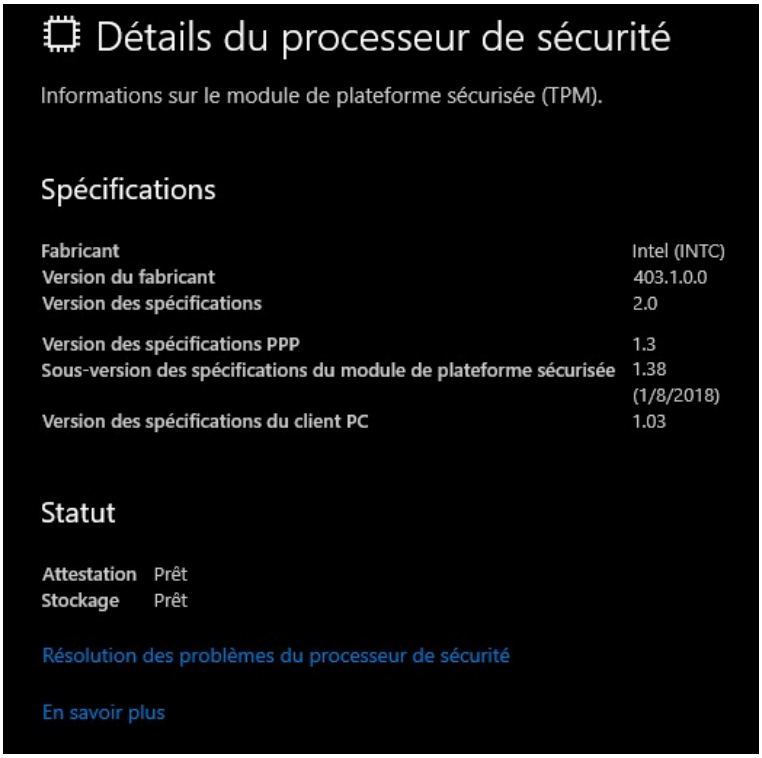
Jumelet et al. (2013, p. 24-25) explique dans leur livre *Sécurité et mobilité Windows 8 pour les utilisateurs nomades : UEFI, BitLocker et AppLocker, DirectAccess, VPN, SmartScreen, Windows Defender*... qu'un TPM est soit :

- Soudé directement sur la carte mère.
- Un composant logicielle embarqué dans le processeur. On définit ce type de TPM comme étant une unité virtuelle.

Selon la documentation de Microsoft (2021n), nous pouvons comparer ce module à une extension de stockage permettant de sauvegarder des informations de connexion. Il dispose également d'une puissance de calcul relativement faible mais qui permet de randomiser des nombres, de procéder à un déchiffrement ou encore de créer des clés cryptographiques.

Ce module permet de lutter contre les attaques de bas niveau informatique pour empêcher l'injection d'un code malicieux pouvant corrompre la sécurité d'un utilisateur.

Figure 17 - Sécurité Windows Menu Informations module TPM (Source : Auteur)



Windows/Paramètres/Sécurité Windows/Sécurité des appareils/Détails du processeur de sécurité

1.1.5.3. Secure Boot

Dans le but de lutter contre l'utilisation de rootkit et plus particulièrement des bootkit, Windows implémente, dans son centre de sécurité, une option nommée « Secure boot ».

L'objectif de cette fonctionnalité est de s'assurer qu'uniquement le matériel approuvé et intégré par le fournisseur de l'équipement (OEM) est utilisé lors de la manœuvre de démarrage de l'appareil (Microsoft, 2019c).

D'après la documentation, lorsque l'appareil est enclenché, et que l'option « Secure boot » est activée, une vérification sur la base des signatures de tous les logiciels de démarrage est effectuée. Cela concerne également les pilotes des périphériques connectés à la carte mère. Dans le cas où, les signatures sont acceptées, selon la base de données des signatures stockées dans la RAM, l'appareil va continuer le processus de démarrage (Microsoft, 2019c).

Tout ce processus lutte contre l'utilisation des bootkits qui peuvent donner un accès administrateur à un potentiel pirate au moment du démarrage.

1.2. Solutions On-Premise

Le On-Premise ou « Sur site » en français est l'architecture sur laquelle les entreprises se sont développées depuis le début de l'informatique moderne. Ici, nous parlons d'infrastructure réseau comprenant un serveur sur laquelle toutes les ressources sont distribuées vers des machines clientes.

Ce type d'architecture est définit de la manière suivante :

> En français, « On-Premises » signifie littéralement « dans les locaux » ou « sur site ». Cette définition d'On-Premises fait référence à l'utilisation du serveur et de l'environnement informatique de l'entreprise. Dans ce modèle d'utilisation, le client, ou licencié, achète ou loue un logiciel basé sur serveur qui sera installé sur son propre serveur ou sur un serveur loué. Comme le licencié exploite le logiciel dans son propre centre de calcul sur son matériel ou sur du matériel loué, on parle également de logiciel « in-house » (IONOS, 2020).

La stratégie actuelle de Microsoft semble se diriger vers une globalisation et une extension de ses produits cloud. Cependant, il reste encore un grande partie des entreprises qui possèdent une infrastructure sur site. En effet, une étude réalisée par le groupe Spiceworks Ziff Davis (2021) démontre qu'il y aura toujours une majorité des entreprises qui compte faire l'acquisition de serveurs à l'horizon 2022.

Dans ce travail, nous nous intéressons aux solutions de sécurité proposées par Microsoft dans un cadre d'architecture « On-Premise ». Par conséquent, nous développons ci-dessous, une liste des outils pour gérer la sécurité des points de terminaisons d'une entreprise. Ces outils permettent d'administrer les paramètres de la sécurité que nous avons développés dans la rubrique précédente.

Il est important de savoir qu'étant donné que l'infrastructure est basée sur un environnement sur site et, donc, locale, il est nécessaire d'utiliser un VPN pour se connecter à distance sur le domaine de l'entreprise dans le cas d'une utilisation nomade.

1.2.1. Active Directory et Group Policy Objects

1.2.1.1. Active Directory

Afin de gérer les différents comptes des employés d'une organisation, Microsoft propose sa solution Active Directory Domain Services (AD DS). Le but de celle-ci est de proposer aux entreprises un moyen d'organiser la gestion de leurs identités à travers leur réseau de manière centralisée.

Les données au sein de la solution AD DS sont stockées en tant qu'objet de manière hiérarchique.

Il est possible de stocker plusieurs types d'objet, tels que des utilisateurs ou encore des machines.

La solution Active Directory existe depuis plus de 20 ans. Effectivement, AD DS a vu ses premiers jours sur les premières versions de Windows 2000 Server. Depuis, elle est encore disponible sur les versions récentes de la suite « Server » de Windows. Bien que les technologies du Cloud soient en plein essor, AD DS est toujours maintenu par Microsoft et l'entreprise continue d'en prendre soin.

La structure d'un Active Directory est décomposée comme suivant :

- Le domaine : Nous caractérisons un domaine comme étant un ensemble d'objets dans un réseau. Le domaine est géré par le Domain Name System (DNS). C'est grâce à celui-ci, que nous pouvons retrouver les données à travers le réseau.

- L'arbre : Dans un AD, nous pouvons retrouver un ou plusieurs domaines. Un arbre peut être constitué de plusieurs domaines. Les arbres sont souvent une représentation de la hiérarchie des départements d'une organisation. Un domaine pour les ressources humaines et un autre pour le département des finances peuvent être des exemples.

- La forêt : La forêt est un groupe constitué de plusieurs arbres. Ils partagent un seul et même schéma d'organisation. La forêt utilise un système de catalogue global qui permet de retrouver les domaines en son sein.

- L'unité organisationnelle (OU) : AD utilise les OU pour découper le domaine de manière logique pour l'administration. Elles organisent les utilisations, les groupes et les appareils d'un domaine.

D'un point de vue sécurité, un Active Directory est important dans la gestion des identités, car c'est lui qui permet aux utilisateurs du domaine de se connecter sur leur compte. Il agit comme un moyen d'authentification pour les utilisateurs.

Pour personnaliser la sécurité des clients dans un Active Directory, il est nécessaire d'utiliser des Group Policy Object (GPO) qui agissent comme des règles pour les utilisateurs et les machines d'un domaine.

1.2.1.2. Group Policy Objects

Les GPO sont des règles applicables à un domaine entier ou, plus spécifiquement, à une unité organisationnelle dans le cadre d'un Active Directory.

Ceux-ci permettent d'autoriser, d'interdire ou encore de personnaliser l'expérience d'un utilisateur lorsqu'il est connecté sur le domaine de l'entreprise.

Il existe plusieurs milliers de GPO disponibles pour les entreprises afin de personnaliser les clients Windows de leur domaine.

Dans le cadre de la sécurité informatique, nous retrouvons plusieurs GPO qui permettent de rendre un ordinateur plus sécurisé. En effet, il est tout à fait possible de restreindre l'utilisation de certaines parties logiciels du système d'exploitation pour empêcher un utilisateur d'avoir accès à des fonctionnalités pouvant mener à des problèmes de sécurité. A l'inverse, il existe des GPO qui permettent d'activer certaines composantes des clients Windows afin de garantir la sécurité du point de terminaison.

Les GPO sont divisés en 2 catégories :

- Computer Configuration (CC) : Ensemble des règles disponibles pour cibler un ordinateur du domaine.
- User Configuration (UC) : Ensemble des règles disponibles pour cibler un utilisateur du domaine.

C'est ainsi que la sécurité dans un environnement On-Premise peut être gérer. Il est nécessaire de disposer d'un AD et de GPO pour cibler et soumettre une stratégie de sécurité aux postes des utilisateurs d'une organisation.

1.2.2. System Center Configuration Manager

Dans la gamme des produits de Microsoft pour la protection des clients Windows, nous retrouvons « Microsoft Endpoint Manager » (MEM) qui, dans sa suite, contient le produit « System Center Configuration Manager » (SCCM) ou simplement « Configuration Manager » depuis la version 1910 selon Microsoft (2021k).

Selon Ben Rubenstein (2020), nous définissons SCCM comme un produit qui permet la gestion, le déploiement et la sécurité des appareils et des applications à travers le réseau de l'entreprise. SCCM est communément utilisé pour gérer la sécurité et la protection des points de terminaisons On-Premise au sein d'une grande organisation. Il permet également de gérer la gestion des mises à jour ou encore de la distribution des logiciels.

Le but de Configuration Manager est de proposer à un administrateur la possibilité d'unifier tout le processus de gestion des appareils et des comptes utilisateurs au sein d'un même logiciel. L'outil doit également être connecté à un AD pour bénéficier de ses ressources.

En effet, SCCM contient un service se nommant « Endpoint Protection » permettant de gérer la sécurité des appareils de l'entreprise. Il aide notamment à instaurer entre autres les éléments suivants selon la documentation de Microsoft (2021h) :

- Configuration d'une protection contre les malware.
- Paramétrage de « Windows Defender Firewall ».
- Installation et déploiement des mises à jour.

Cette suite logiciel s'inscrit donc parfaitement dans la gestion de la sécurité des points de terminaison d'une organisation.

1.2.2.1. Description du service

La console de Configuration Manager est divisée en 5 catégories basée sur leur utilisation :

- Assets and Compliance
- Software Library
- Monitoring
- Administration
- Community

Les deux rubriques les plus intéressantes en termes de sécurité sont celles des « Assets and Compliance » et « Monitoring ». Ce sont celles-ci que nous décrivons ci-dessous.

1.2.2.1.1. Assets and Compliance

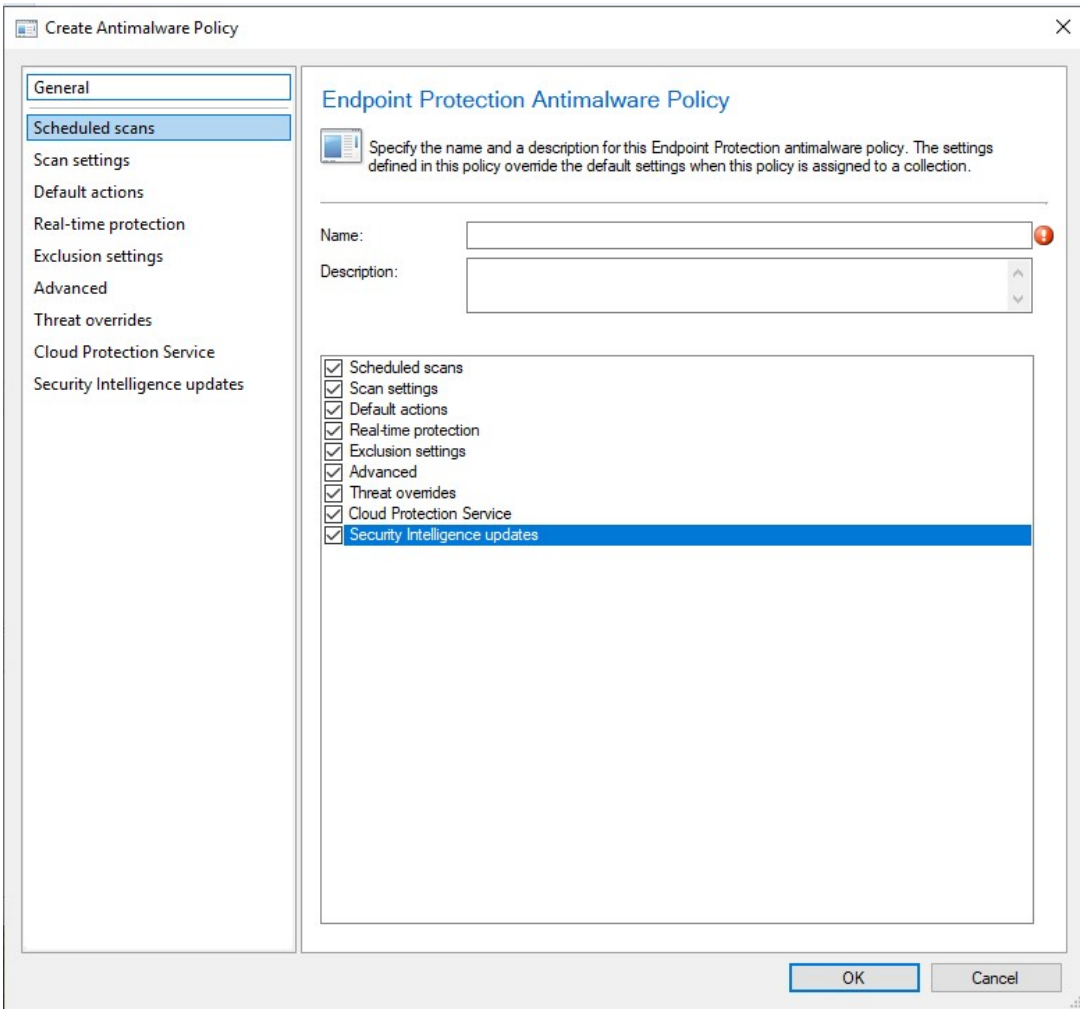
La première rubrique permet d'appliquer des règles à des utilisateurs ou des machines. Tout comme l'utilisation de GPO, il existe des paramètres de configuration. Ceux-ci sont ensuite déployés sur les machines ou chez les utilisateurs ciblés.

Toujours dans « Assets and Compliance » on retrouve une rubrique « Endpoint Protection ». Celle-ci contient plusieurs sous-rubrique permettant de gérer la sécurité des clients Windows. Nous détaillons les sous-rubriques utilisables dans un contexte On-Premise ci-dessous :

Antimalware Policies

C'est ici que l'ensemble des règles concernant la protection contre les malwares sont définies.

Figure 18 - SCCM Antimalware Policies
(Source : Auteur)



Une des règles qui peut être définie est le lancement de scan de l'appareil client programmable. Celle-ci permet de définir entre autres :

- L'activation du scan sur les ordinateurs clients
- Le type de scan (complet ou rapide)
- La date et l'heure du scan

Une autre règle consiste à la personnalisation du scan. Il est possible de choisir de scanner les mails, les fichiers présents dans le réseau ou encore d'analyser les disques amovibles (ex : USB).

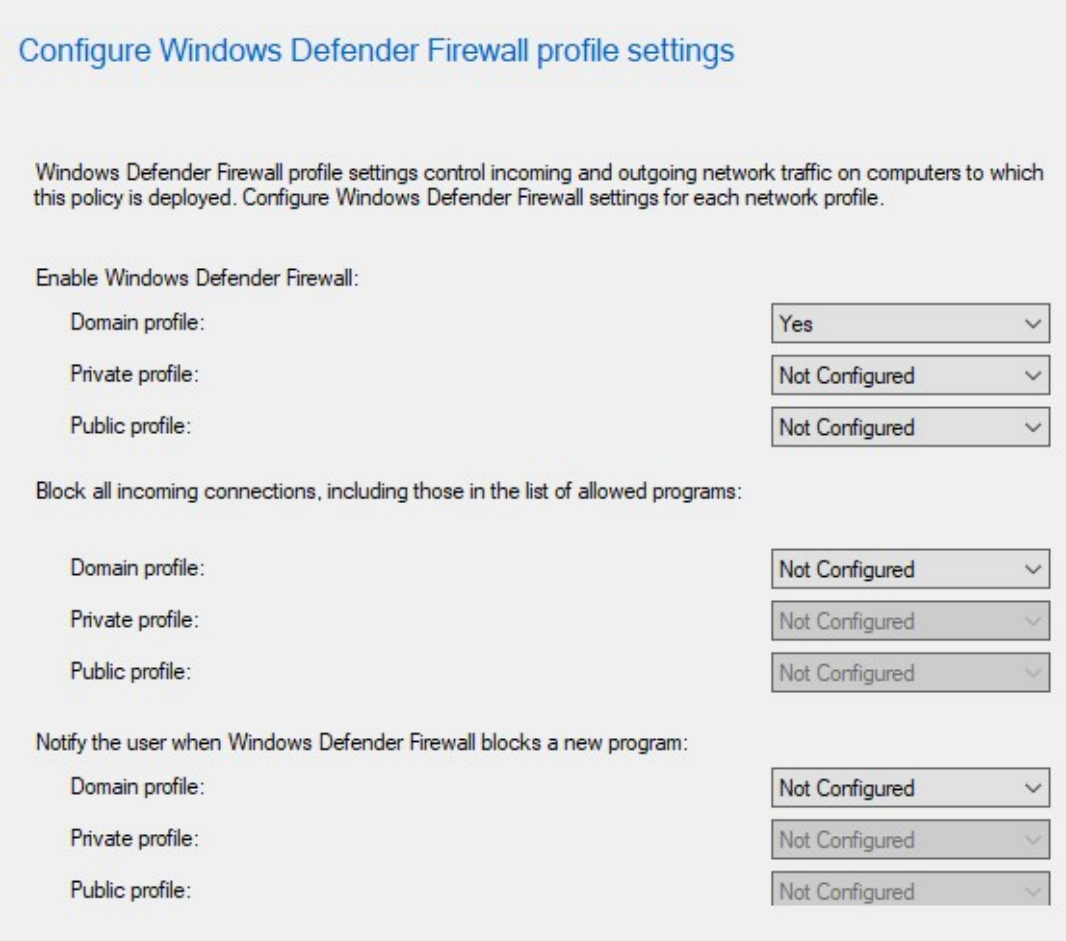
Il est également possible de choisir d'activer l'antivirus Microsoft Defender sur la machine en lui donnant certains paramètres, comme le scan des fichiers entrants ou sortants de l'appareil client.

Tout comme pour la gestion des GPO, il est possible de restreindre l'accès à certaines zones de Windows. En effet, il est totalement envisageable de bloquer l'accès de « Windows Security » afin que l'utilisateur ne puisse pas modifier les paramètres déjà mis en place.

Windows Defender Firewall Policies

Dans cette sous-rubrique, nous pouvons choisir de configurer les règles du pare-feu à déployer à nos clients Windows.

Figure 19 - SCCM Windows Defender Firewall Policies
(Source : Auteur)

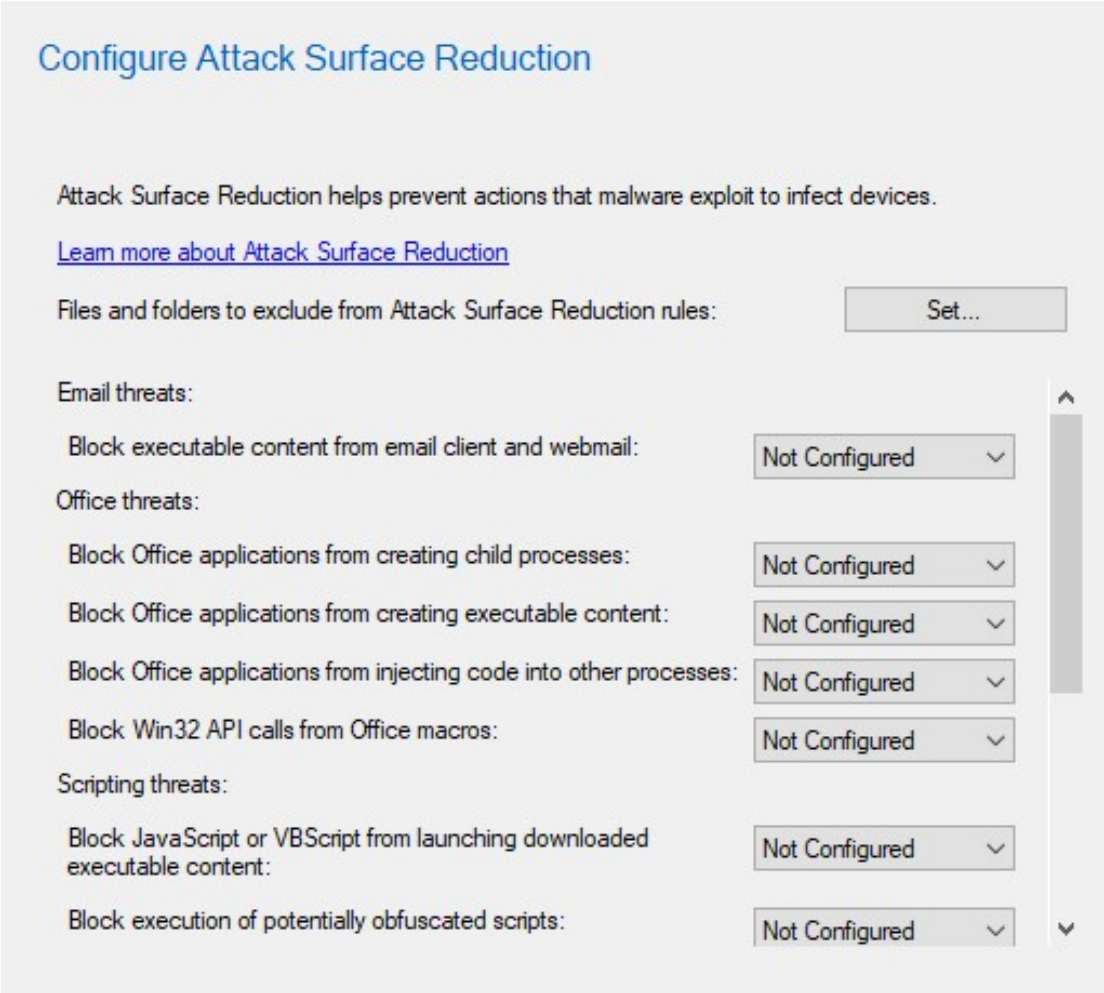


Comme nous pouvons le voir dans l'image ci-dessus, il est possible d'activer sur le domaine, publiquement ou de manière privée, le Firewall, de bloquer des connexions entrantes ou encore de notifier à l'utilisateur lorsqu'un programme est bloqué.

Windows Defender Exploit Guard

Cette sous-rubrique de la protection « endpoint « est utilisée pour gérer les tentatives d'exploitations du système par des pirates informatiques.

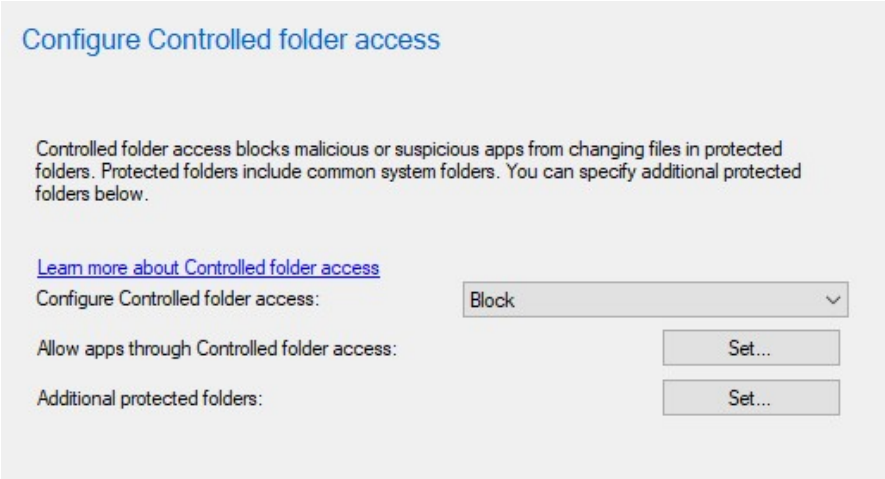
Figure 20 - SCCM Réduction de la surface d'attaque
(Source : Auteur)



Un des paramètres disponibles permet de réduire la surface d'attaque des malware. Dans ce dernier, il est possible de donner des règles dans le but de bloquer certaines applications ou l'exécution de script potentiellement malveillant.

Un autre paramètre est celui de la protection des dossiers lors d'une attaque par rançongiciel par exemple. Ci-dessous, nous définissons si la règle est activée et quelles sont les applications pouvant modifier le contenu d'un dossier.

Figure 21 - SCCM Accès contrôlé aux dossiers
(Source : Auteur)



Il est également envisageable de protéger certains appareils du domaine en donnant un fichier de configuration XML pour la protection contre l'exploitation des données.

Finalement, le dernier paramètre rend possible de bloquer certains sites potentiellement malveillant qui peuvent contenir des traces d'hameçonnage par exemple.

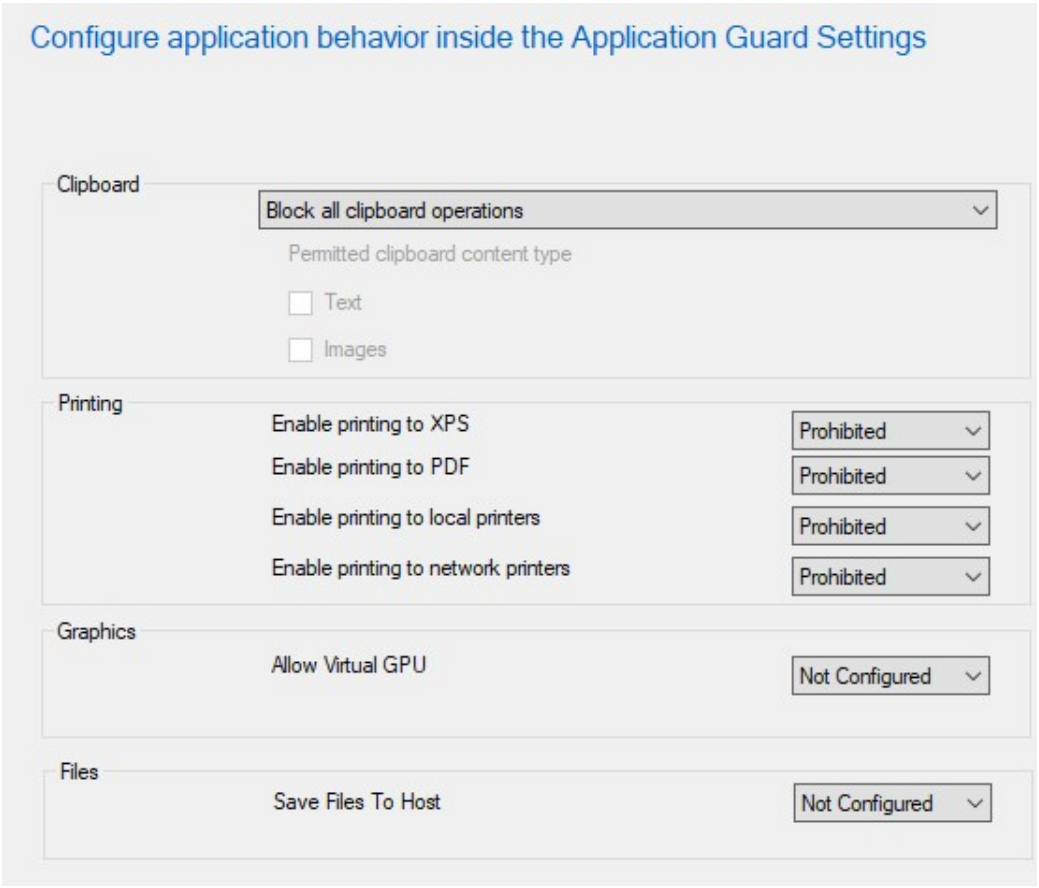
Figure 22 - SCCM Protection du réseau
(Source : Auteur)

Windows Defender Application Guard

C'est dans cette section que l'administrateur peut gérer les paramètres concernant la sécurité des applications et du navigateur internet de Microsoft. Ceux-ci peuvent contenir parfois des malwares. Pour pallier cette possibilité, Microsoft permet de containeriser les applications et les sites internet grâce à la technologie Hyper-V et de pouvoir les tester de manière isolée.

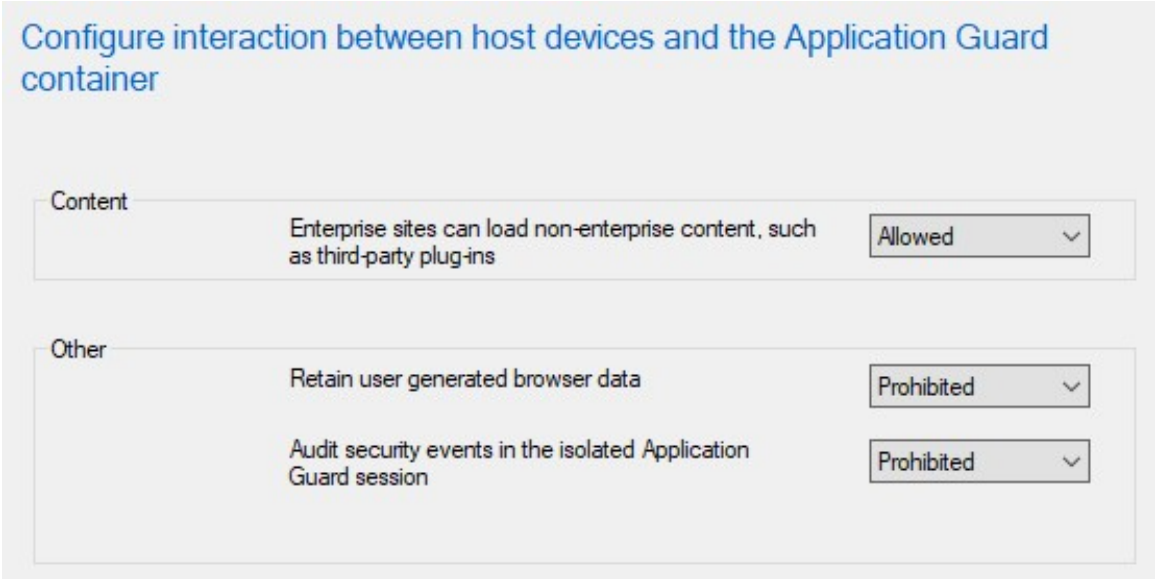
Ici, nous retrouvons tout d'abord les paramètres relatifs au comportement des applications dans les paramètres du service « Application Guard ». Par conséquent, il est possible de déterminer si l'utilisateur a le droit de copier des éléments ou encore d'imprimer lorsqu'il se trouve dans une session « Application Guard ».

Figure 23 - SCCM Paramètres Application Guard
(Source : Auteur)



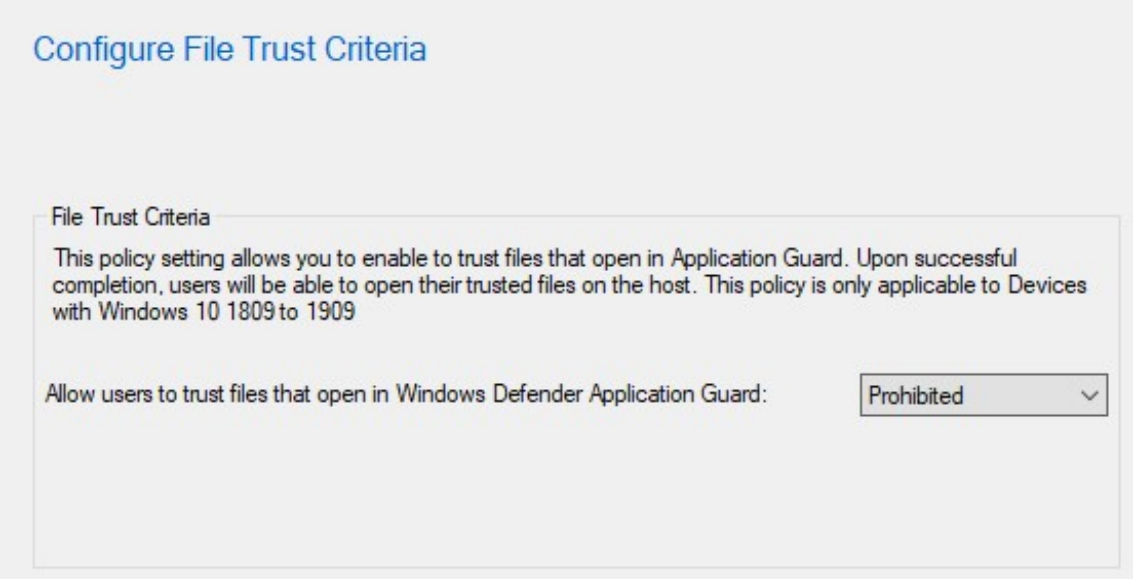
Également, il est possible de configurer l'interaction entre l'appareil hôte de l'utilisateur et le container. Ici, nous retrouvons les paramètres permettant d'autoriser des plug-in externes à l'organisation ou encore de sauvegarder les données de l'utilisateur du navigateur (ex : cookies, favoris, etc.) dans le container.

Figure 24 - SCCM Interaction entre l'hôte et le container Application Guard
(Source : Auteur)



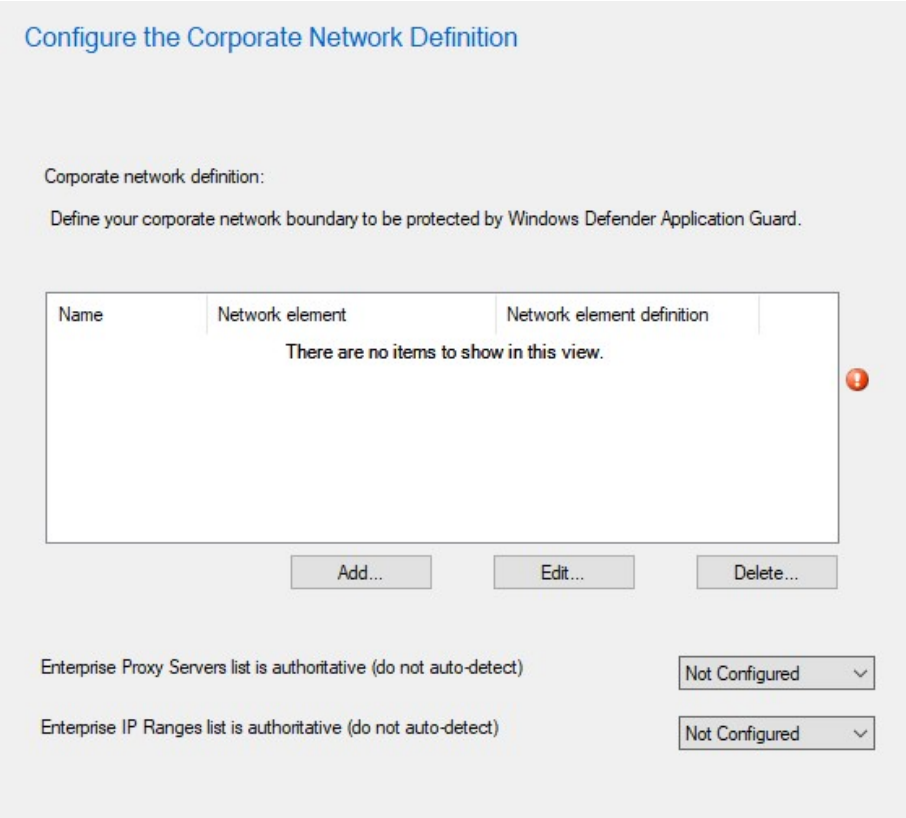
Un autre paramètre intéressant est celui de permettre ou non d'enregistrer des fichiers provenant du container « Application Guard » ou d'appliquer un contrôle de l'antivirus sur ceux-ci.

Figure 25 - SCCM Confiance des fichiers dans Application Guard
(Source : Auteur)



Nous pouvons aussi déterminer quels sont les utilisateurs ou les appareils du site de l'entreprise qui peuvent avoir accès à ces paramètres.

Figure 26 - SCCM Définition de la portée de la règle
(Source : Auteur)

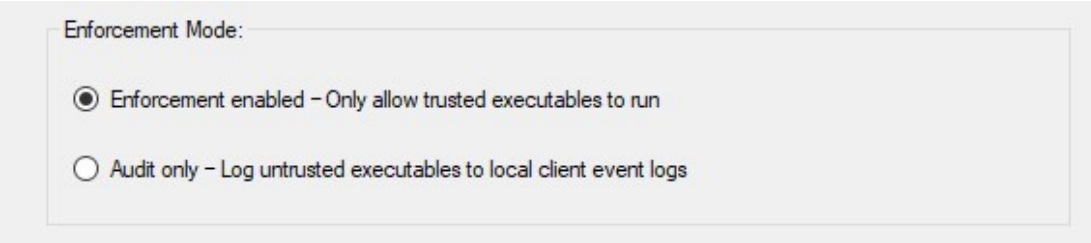


Windows Defender Application Control

Selon sa documentation, Microsoft (2021i) définit ce service en expliquant qu'il permet de protéger les clients contre des malwares et des logiciels potentiellement dangereux. Il prévient l'exécution de code malicieux en acceptant seulement les codes approuvés. En d'autres termes, seulement les applications autorisées par l'administrateur peuvent être utilisées sur les clients afin d'empêcher des infections.

Il est tout d'abord possible de choisir le mode d'imposition en définissant si nous acceptons uniquement les programmes que nous listons ou si une inscription dans les logs suffit.

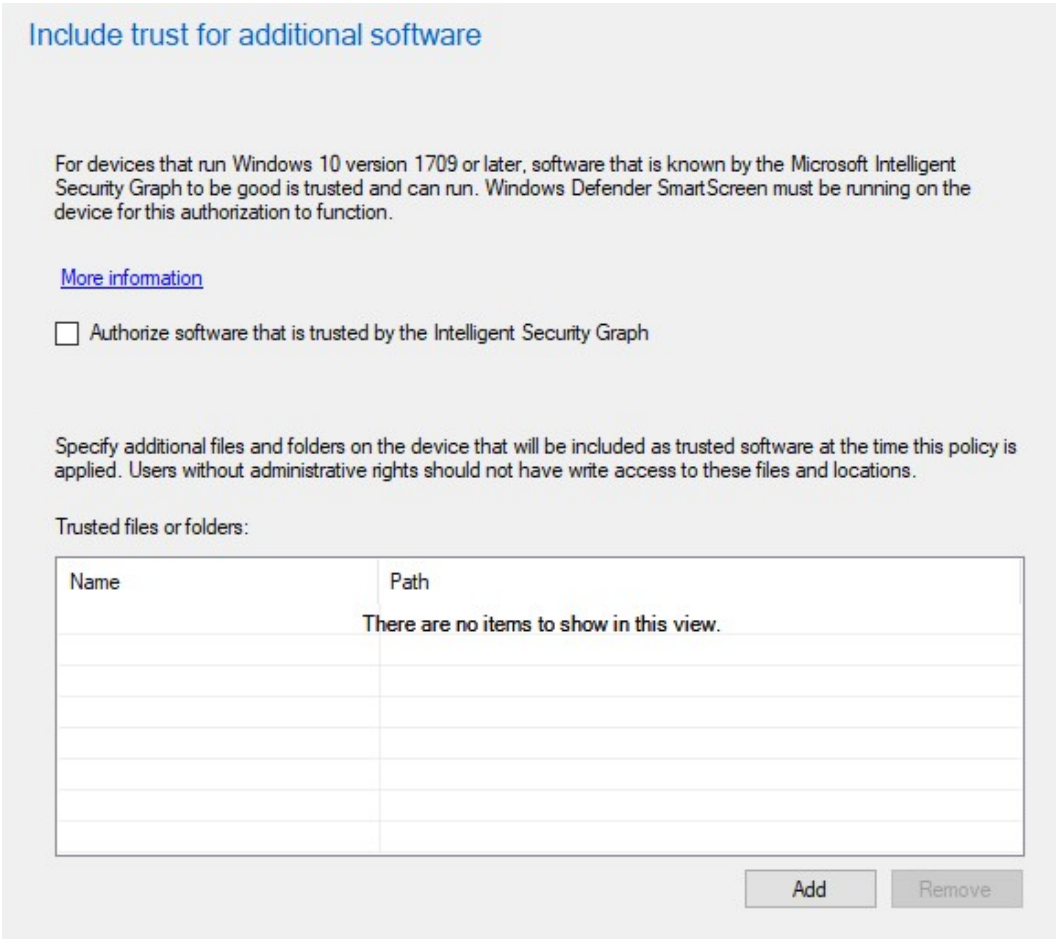
Figure 27 - SCCM Mode d'imposition
(Source : Auteur)



Le dernier paramètre permet de donner une liste des programmes dont l'administrateur a confiance pour les soumettre aux utilisateurs des clients.

Également, l'utilisateur peut choisir de faire confiance à Intelligent Security Graph qui se charge de faire l'analyse des logiciels par machine learning. Cette option permet d'installer les applications considérées saines par l'API Intelligent Security Graph.

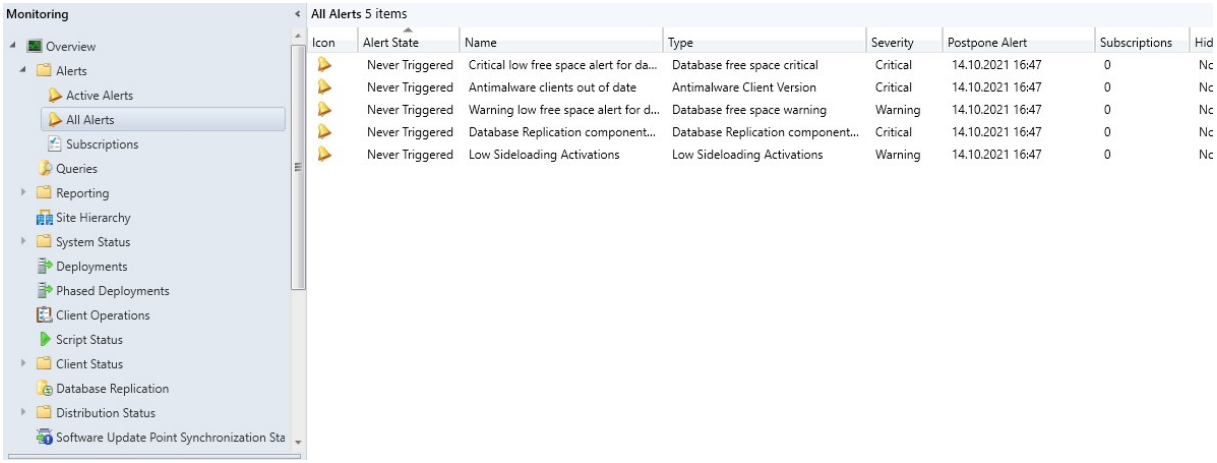
Figure 28 - SCCM Liste des fichiers et dossiers de confiance
(Source : Auteur)



1.2.2.1.2. Monitoring

La deuxième implique la gestion et le contrôle de l'infrastructure. C'est dans cet espace de travail, que l'administrateur peut voir l'ensemble des alertes de sécurité des appareils connectés sur le site.

Figure 29 - SCCM Alerte de sécurité
(Source : Auteur)



1.3. Solutions Cloud

Depuis début 2010, la technologie de l'informatique en nuage, ou, plus populairement appelée, en « Cloud » permet de s'affranchir de tout le matériel qu'implique une infrastructure dite « On-Premise ».

La pandémie Covid-19 a un impact sans précédent sur la popularité du Cloud. Une étude menée par Luxner (2021) démontre que 90% des entreprises sondées songe à avancer leur migration vers le Cloud en raison des conséquences du virus, dont notamment le télétravail.

Selon la revue scientifique Futura Sciences (s.d.), le cloud computing permet de proposer une infrastructure offrant de la puissance de calcul et de l'espace de stockage par le biais de plusieurs serveurs distants. Les utilisateurs accèdent à ces serveurs via Internet.

Le Cloud se divise en trois catégories selon l'utilisation qui en est faite :

- Public : Cette catégorie est celle à laquelle la plupart des gens font mention lorsqu'elle parle du Cloud. Les cloud publics sont des infrastructures informatiques appartenant au fournisseur de service. Le client va pouvoir bénéficier de la puissance de calcul et du stockage du fournisseur. Le terme « public » a son importance car il implique que les clients se partagent l'accès à cette infrastructure.

- Privé : Contrairement au cloud public, sa version privée se distingue par son exclusivité pour un client. Selon Redhat (s.d.) : « Les clouds privés sont généralement définis comme des environnements cloud spécifiques à un utilisateur final ou à un groupe ». Ils peuvent être situés soit dans les locaux du fournisseur, soit directement être un environnement On-Premise chez le client. Cela implique la responsabilité de ce dernier quant à l'infrastructure louée ou achetée. Un cloud privé permet plus de personnalisation du service proposé car il est exclusif à un client.

- Hybride : D'après la recherche de Jackson et Goessling (2018, p. 33) dans *Architecting Cloud Computing Solutions*, un cloud hybride est une solution qui fusionne un modèle de cloud publique avec un autre modèle de cloud ou On-Premise. De cette manière, le client possède une plus grande marge de manœuvre. Par exemple, une stratégie intéressante est de garder en son sein les données les plus confidentielles et de bénéficier de la puissance des centres de données des fournisseurs pour des services d'applications, tels que Microsoft Office 365 (Word, Powerpoint, Excel, etc.).

Il existe trois principaux types de services proposés par la technologie du cloud :

- Infrastructure as a Service (IaaS) : Ce type de service offre des composants d'infrastructure aux entreprises. La définition suivante est donnée par Bastien L. (2017c) : « Un fournisseur tiers héberge le hardware, le software, les serveurs, les connexions réseau, la bande passante, l'adressage, le stockage et les autres composants de l'infrastructure à la place des utilisateurs. ».

- Platform as a Service (PaaS) : Ce service permet de bénéficier d'outils hardware et logiciels en tant que service par le biais d'internet. Cela offre la possibilité à l'utilisateur de développer des applications tournant sur l'infrastructure chez le fournisseur (Bastien L., 2017a).

- Software as a Service (SaaS) : Le SaaS se base sur une distribution des applications. Ces dernières sont complètement administrées par le fournisseur pour proposer une solution finale à l'utilisateur via Internet (Bastien L., 2017d). Par exemple, la suite Office 365 est un SaaS.

Avant de passer aux services du Cloud permettant de sécuriser les clients Windows, il est nécessaire de faire un aparté sur la solution « Azure Active Directory ». En effet, cette dernière est intrinsèquement liée aux autres services que nous présentons dans ce travail.

Azure Active Directory

Tout comme sa version On-Premise, le service « Azure Active Directory » (AAD ou Azure AD) de Microsoft permet de gérer la protection de l'identité des utilisateurs d'une organisation, mais cette fois en utilisant internet et la technologie Cloud.

Pour comprendre un peu plus en profondeur comment le service Azure fonctionne, il est nécessaire d'assimiler la notion de « tenant ». Selon Saxton (2015), développeur chez Microsoft, un tenant peut être considéré comme étant un bac à sable dans lequel des ressources sont entreposées. Pour reprendre son exemple, nous pouvons supposer que le nom de notre tenant est « cokhevs » et dont le nom de domaine est « cokhevs.onmicrosoft.com ». Tous les utilisateurs des services Azure crées sous ce tenant possède un login avec une structure semblable à « kevin.coppey@cokhevs.onmicrosoft.com ».

Toroman (2018, p. 21) explique dans son livre que le service AAD est tout au sommet de la chaîne de management de Azure, il est directement lié au tenant. De plus, un compte utilisateur peut disposer de plusieurs tenants mais chacun de ceux-ci sont isolés des autres.

Selon la documentation, les utilisateurs créés sur la plateforme peuvent accéder à des ressources externes telles que des produits de la suite Microsoft 365 et à des milliers d'applications de type SaaS. Par conséquent, c'est à l'administrateur de rajouter les utilisateurs de son entreprise sur la plateforme et de leur permettre d'avoir accès aux ressources qu'il souhaite autoriser (Microsoft, 2021c).

AAD s'intègre parfaitement dans un scénario nomade ou BYOD étant donné sa disponibilité sur le Cloud et, par conséquent, son accessibilité à partir de n'importe quel endroit du monde. Il suffit que l'utilisateur se connecte avec son compte sur le tenant de l'organisation et il dispose de tous les services dont il a l'accès.

1.3.1. Microsoft Endpoint Manager Admin Center

Dans les produits de la suite « Microsoft Endpoint Manager » (MEM), nous retrouvons le service « Microsoft Intune ». Celui-ci permet une gestion des machines à travers le Cloud.

Ce service permet de gérer à distance tous les appareils des employés d'une entreprise. Que les employés se trouvent en Suisse ou à l'étranger, étant donné que le service utilise Internet, l'administrateur peut mettre en place toutes les stratégies qu'il souhaite.

Intune est défini de la manière suivante :

> Microsoft Intune est un service cloud qui se concentre sur la gestion des appareils mobiles (MDM) et la gestion des applications mobiles (GAM). Vous contrôlez la façon dont les appareils de votre organisation sont utilisés, y compris les téléphones mobiles, les tablettes et les ordinateurs portables. Vous pouvez également définir des stratégies spécifiques pour contrôler les applications. Par exemple, vous pouvez empêcher l'envoi de courriels à des personnes extérieures à votre organisation. Intune permet également aux utilisateurs de votre organisation de se servir de leurs appareils personnels à l'école ou au travail. Sur les appareils personnels, Intune garantit que les données de votre organisation restent protégées et peut isoler les informations professionnelles des données personnelles (Microsoft, 2021f).

Intune fonctionne en collaboration avec Azure AD afin d'avoir toutes les informations nécessaires des comptes utilisateurs, cela comprend également leur appareil de connexion.

Le service « Microsoft Endpoint Manager admin center « (MEMAC) permet à l'administrateur de s'occuper de l'enrôlement des machines des utilisateurs. Les machines enrôlées sur MEMAC sont ensuite complètement gérables par l'organisation via Intune. Tout comme avec des GPO, il est possible d'appliquer des règles de configuration, mais cette fois en utilisant la puissance du Cloud.

De plus, MEMAC dispose d'un tableau de bord afin de prendre connaissance du statut des appareils enrôlées sur le service. Lorsqu'un problème survient, l'administrateur est directement notifié sur le tableau de bord et peut prendre les mesures qu'il envisage comme nécessaire pour empêcher une sécurité compromise.

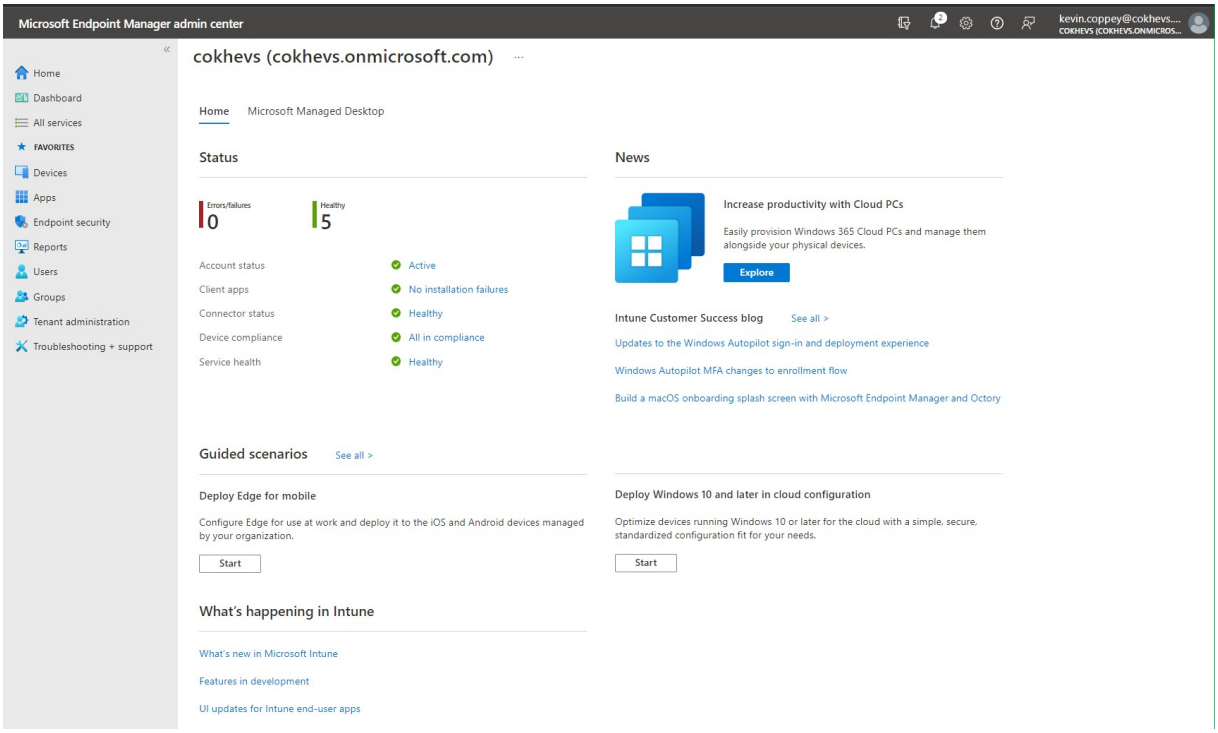
Du côté client, l'utilisateur doit être connecté à son compte Azure AD pour bénéficier des dernières mises à jour de l'organisation. Ce qui rend l'expérience en adéquation avec un scénario nomade. De plus, Intune est conçu pour offrir une expérience sécurisée aux employés dans un contexte BYOD. En effet, l'utilisateur peut se déconnecter du domaine Azure en quelques clics et profiter de son appareil comme il l'entend.

1.3.1.1. Description du service

Lorsque nous arrivons sur le portail « Microsoft Endpoint Manager admin center », la première page est l'accueil. Sur celle-ci, nous retrouvons le statut général des appareils et des comptes des utilisateurs du service. Cela permet à l'administrateur de directement savoir si un problème a été constaté sur un appareil.

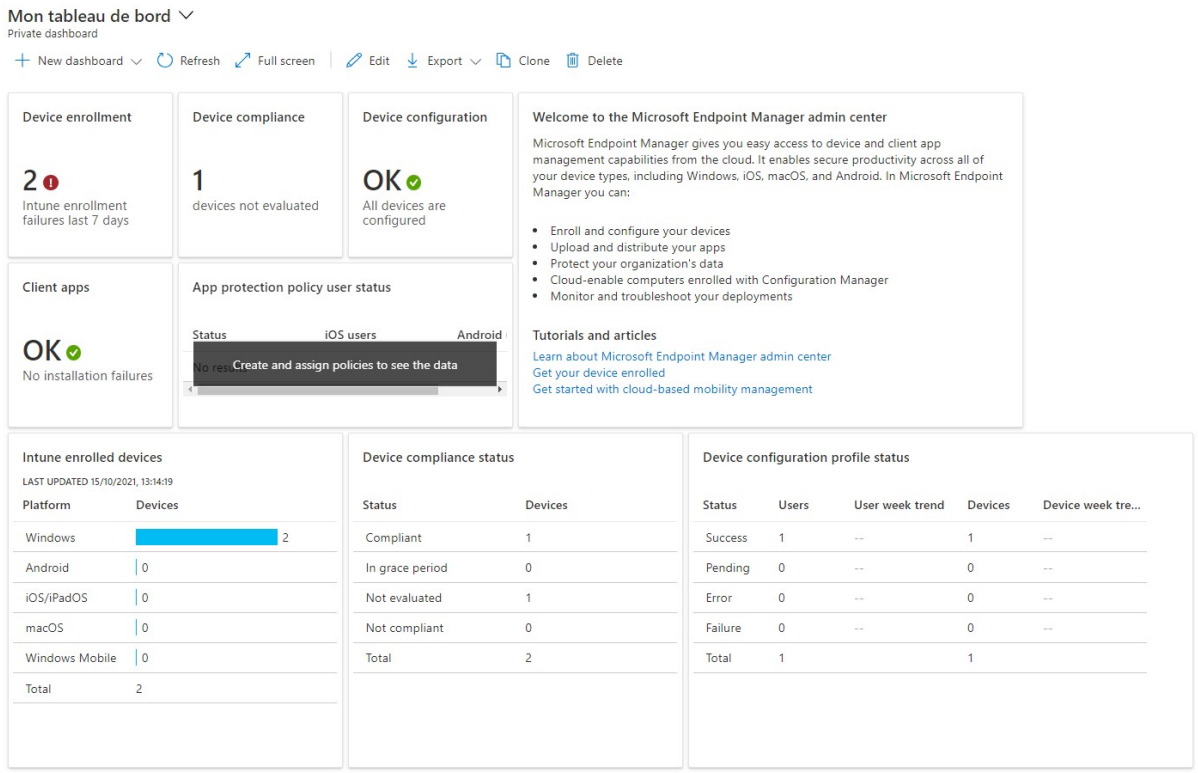
Également, Microsoft propose sur cette page, via la rubrique « News », les nouvelles du service et de la documentation pour en apprendre plus sur des mises à jour ou des fonctionnalités intéressantes.

Figure 30 - MEM Accueil
(Source : Auteur)



La prochaine page est celle du tableau de bord. Sur ce dernier, nous retrouvons les informations déjà présentées dans la page précédente, mais avec plus d'informations. L'avantage du tableau de bord est qu'il est entièrement personnalisable. L'administrateur peut choisir d'autres vignettes à intégrer qu'il juge utiles dans la sécurité des appareils des employés.

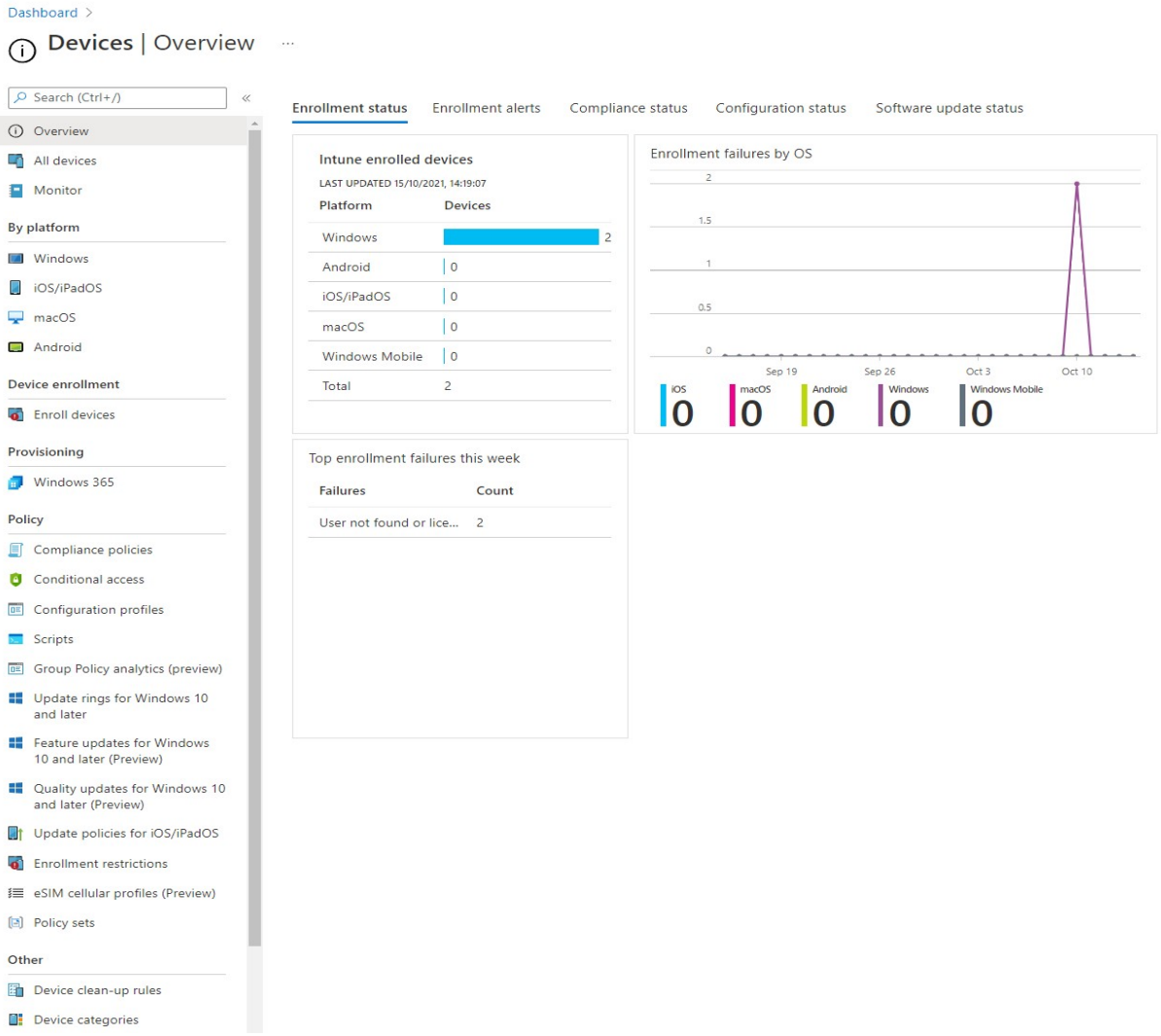
Figure 31 - MEM Tableau de bord
(Source : Auteur)



La page « All services » permet d'atteindre rapidement les autres pages en naviguant selon la catégorie du service recherché ou encore la barre de recherche pour filtrer les services.

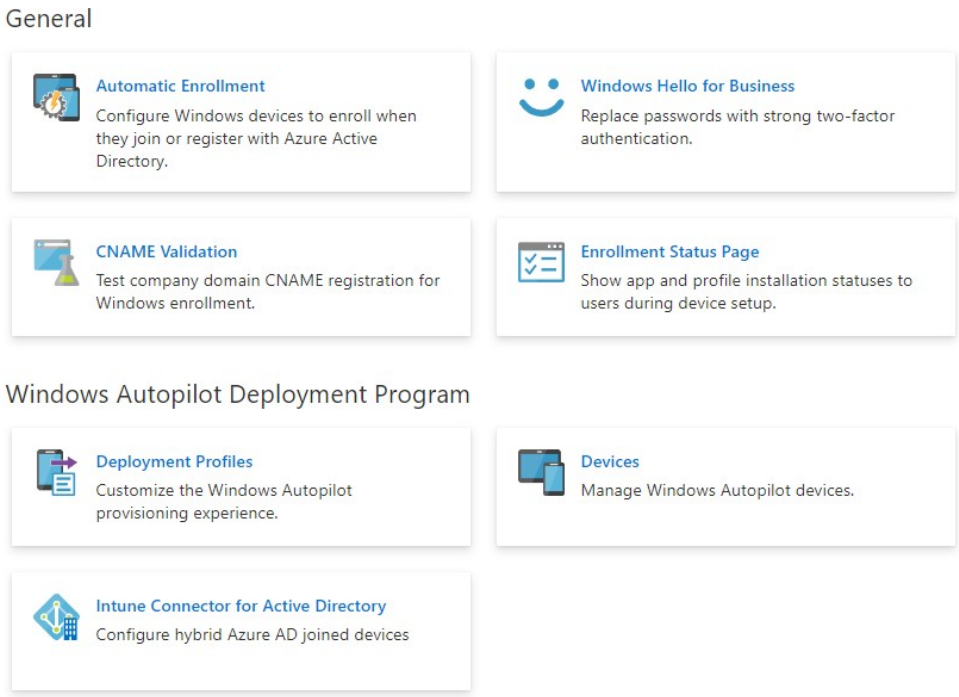
Une page importante pour l'administrateur est celle des « Devices ». C'est ici qu'il peut avoir une vue globale de tous les appareils des utilisateurs enrôlés sur le service. Il est possible de filtrer les recherches ou encore d'exporter des informations. De plus, l'administrateur peut gérer sur cette page l'ensemble des règles applicables ou déjà appliquées sur les appareils des employés.

Figure 32 - MEM Menu Appareils
(Source : Auteur)



Également sur cette page, nous pouvons organiser l'enrôlement des appareils. Différentes options existent.

Figure 33 – MEM Options d'enrôlement des machines
(Source : Auteur)



Sous la rubrique « Apps », l'administrateur peut déployer, sur les appareils enrôlés, des applications comme celle de la suite Office (Word, Excel, etc.).

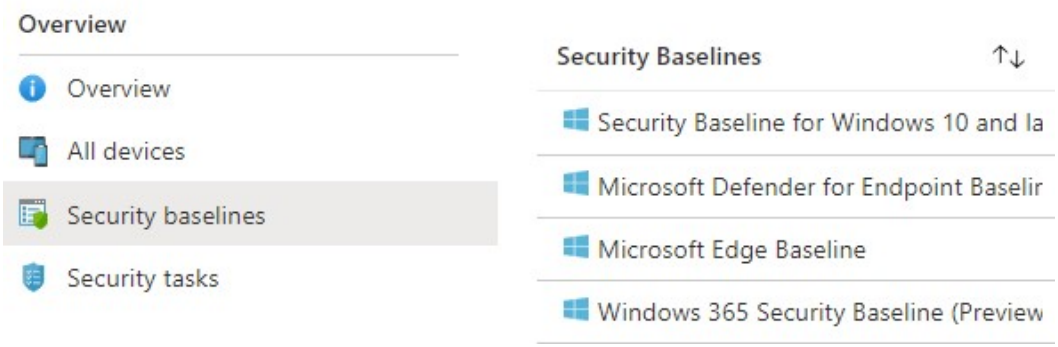
A des fins d'analyse, il est totalement envisageable d'utiliser MEMAC pour sortir des rapports d'utilisation et de sécurité grâce à la page « Reports ».

Comme expliqué plus haut, MEMAC fonctionne de pair avec Azure AD. Ainsi, pour certaines opérations telles que la création d'un utilisateur ou encore la gestion des licences d'un groupe d'employés, il n'est pas nécessaire de quitter MEMAC. Ces paramètres s'administrent dans les pages « Users » et « Groups ».

La rubrique la plus intéressante dans le cadre de ce travail est celle de la sécurité des points de terminaison. C'est sur celle-ci que nous pouvons paramétrer et monitorer des règles spécifiques à la sécurité des appareils Windows.

Nous retrouvons tout d'abord les règles recommandées par Microsoft. Celles-ci sont très intéressantes afin de bénéficier rapidement d'une première infrastructure sécurisée. Cependant, il est possible de créer nos propres règles en fonction de la stratégie de sécurité d'une entreprise.

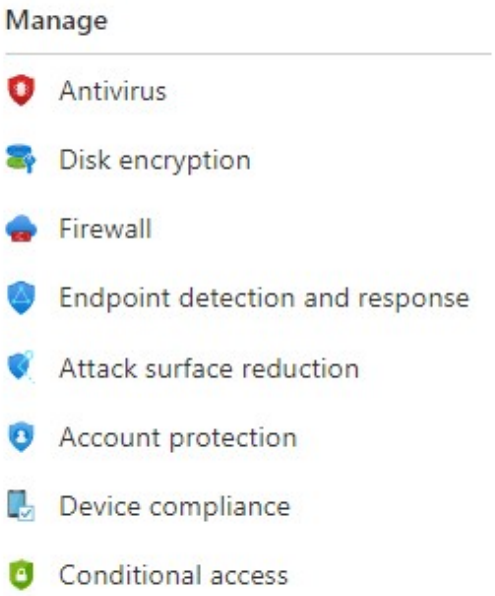
Figure 34 - MEM Règles de sécurité de Microsoft
(Source : Auteur)



Pour créer ses propres règles, il est nécessaire de passer soit par la page « Devices » sous la rubrique Policy, soit par la rubrique « Manage » de la page consacrée à la sécurité des clients. Cette dernière est divisée en huit sous-rubriques en fonction de leur champs d'action :

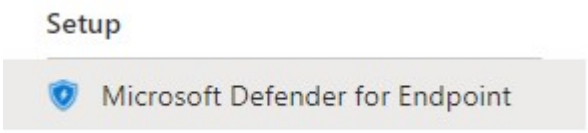
- Antivirus : Dans « Antivirus », il est possible de gérer les paramètres destinés à lutter contre les malwares.
- Disk encryption : Avec Intune, il est possible d'appliquer une stratégie de chiffrement des disques en utilisant BitLocker.
- Firewall : Les paramètres du pare-feu et ses règles sont définis dans cette partie du portail.
- Endpoint detection and response : La détection et les actions entreprises dans le cadre d'une infection sont gérées ici.
- Attack surface reduction : Tous les paramètres concernant l'isolation des processus et la protection contre l'exploitation des failles sont réunis sous « Attack surface reduction ».
- Account protection : Les services tels que « Credential Guard » et « Windows Hello for Business » permettant de garantir la sécurité du compte de l'utilisateur sont trouvables dans cette partie.
- Device compliance : Si l'administrateur souhaite appliquer une stratégie selon le système d'un appareil, il peut passer par cette rubrique.
- Conditional access : Pour empêcher un utilisateur de se connecter dans une certaine région du monde ou encore pour appliquer une stratégie en fonction du département de l'utilisateur, nous devons appliquer des paramètres d'accès conditionnel retrouvés ici.

Figure 35 - MEM Menu Protection des clients (Source : Auteur)



MEMAC peut également fonctionner avec le portail Microsoft 365 Defender qui permet d'utiliser le service « Microsoft Defender for Endpoint ».

Figure 36 - MEM Option Microsoft Defender for Endpoint
(Source : Auteur)



1.3.2. Microsoft Defender for Endpoint

Afin de bénéficier d'un service de monitoring beaucoup plus élaboré que celui proposé par MEMAC, il est possible d'utiliser le portail Microsoft365 Defender. Celui-ci comprend l'outil « Microsoft Defender For Endpoint » (MDE) qui apporte beaucoup plus d'informations et propose des mesures d'amélioration au niveau de la sécurité des machines clientes.

D'après la recherche de Morris (2021), la solution MDE peut être considérée comme étant une protection destinée aux entreprises permettant de garantir la sécurité des appareils des utilisateurs tels que les tablettes, les téléphones ou encore les ordinateurs portables. Cette solution de sécurité est basée sur le cloud et permet de prévenir, de détecter, d'enquêter et de répondre aux attaques informatiques menaçants les points de terminaison. Son avantage est sa simplicité d'utilisation et d'installation, car MDE ne demande aucune installation d'infrastructure particulière et se met automatiquement à jour.

Le service permet également de simuler des attaques afin de tester son infrastructure et les outils mis en place pour mitiger les agressions.

Selon la documentation officielle de Microsoft (2021p), « Microsoft Defender for Endpoint » axe sa stratégie selon sept principes :

La gestion des menaces et des vulnérabilités

Ce premier principe implique une approche basée sur le risque afin d'agir avant que celui-ci n'intervienne. L'utilisation de tableau de bord ou encore la recommandation en matière de sécurité font parties de ce pilier de MDE.

La réduction de la surface d'attaque

C'est en protégeant l'utilisateur sur les terrains où il est le plus vulnérable aux menaces comme sur Internet par exemple que s'articule ce principe.

La protection de nouvelle génération

Microsoft est très actif sur le développement des nouvelles fonctionnalités à proposer à ses utilisateurs. Cela passe par la maintenance de son service antivirus ou encore par la mise à jour de ses produits. Ces actions renforcent le périmètre de sécurité des appareils et du réseau.

La détection et réponse des points de terminaison

MDE implique une détection des menaces quasiment en temps-réel afin de laisser les administrateurs proposer une réponse. En effet, des alertes peuvent être mises en place dans le but de réagir le plus rapidement possible contre une menace potentielle.

Examen et correction automatisés

Il est également envisageable de programmer des actions automatiques qui répondent à une menace sans que l'administrateur n'ait besoin d'intervenir. MDE propose des mesures d'investigation et de correction automatiques en fonction du type d'alerte déclenché.

Niveau de sécurité Microsoft pour les appareils

MDE apporte une notion de score en fonction du degré de sécurisation qu'un appareil a reçu. Plus il est haut, plus la sécurité est élevée. S'il est bas, le service propose des actions à mettre en place pour augmenter son niveau.

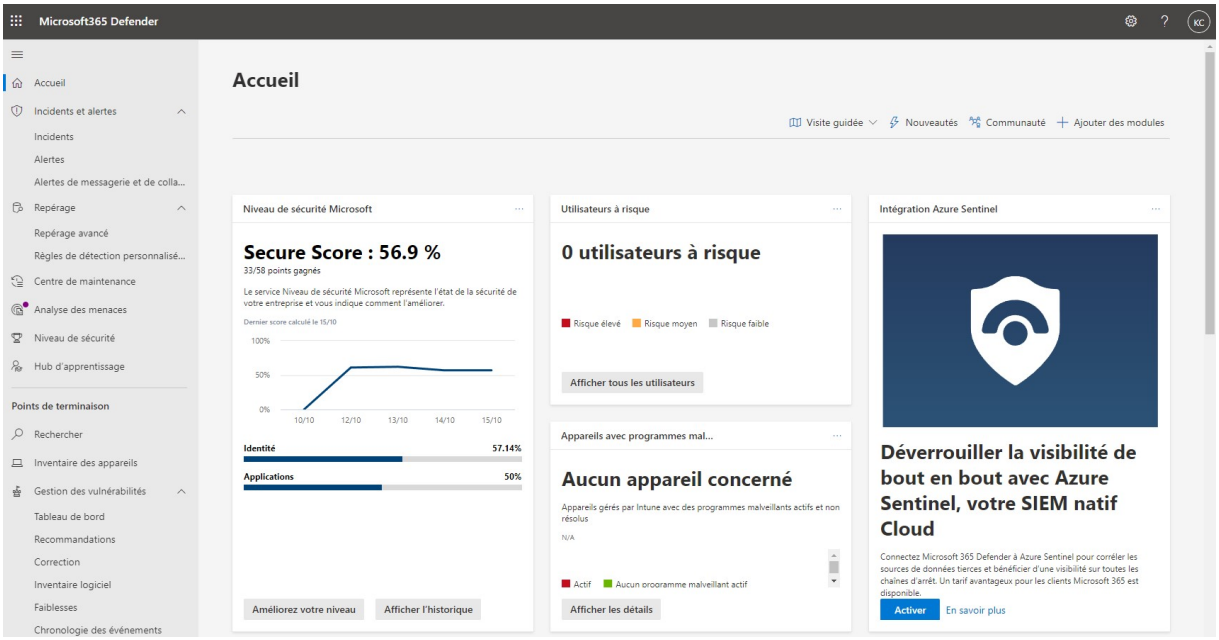
Spécialiste des menaces Microsoft

En tant que client MDE, il est possible de recevoir une assistance par des experts en cybersécurité de chez Microsoft afin de cibler précisément les menaces importantes pour les clients ou simplement pour une demande d'audit.

1.3.2.1. Description du service

Lors de l'ouverture du portail, nous arrivons sur la page d'accueil qui contient les informations générales concernant la sécurité des clients de notre organisation. Il est tout à fait possible de paramétrer l'affichage des vignettes en ajoutant d'autres.

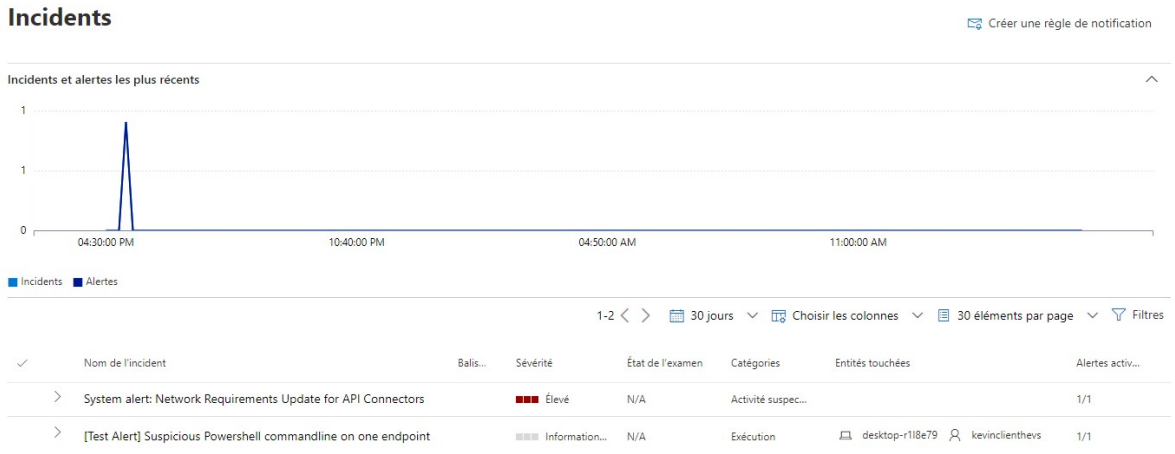
Figure 37 - MDE Accueil
(Source : Auteur)



Dans le menu contextuel de gauche, nous pouvons accéder à plusieurs pages permettant d'avoir une idée de la sécurité mise en place et des actions à entreprendre pour l'améliorer. Nous allons passer en revue les pages les plus intéressantes.

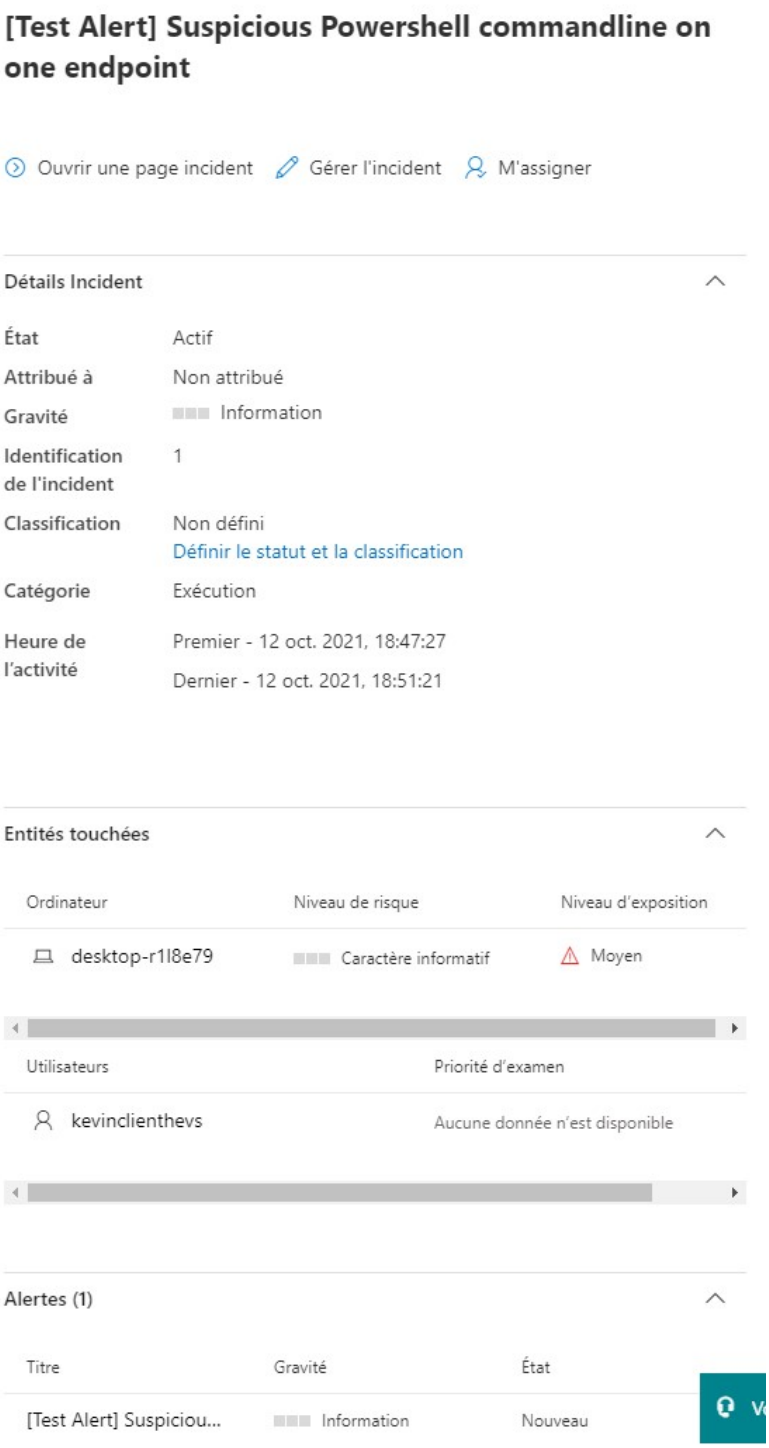
La première que nous retenons est la page « Incidents et alertes », dans celles-ci, l'administrateur de l'organisation peut consulter l'ensemble des incidents et des alertes de sécurité qui se sont produits sur l'ensemble des entités touchées.

Figure 38 - MDE Incidents et alertes
(Source : Auteur)



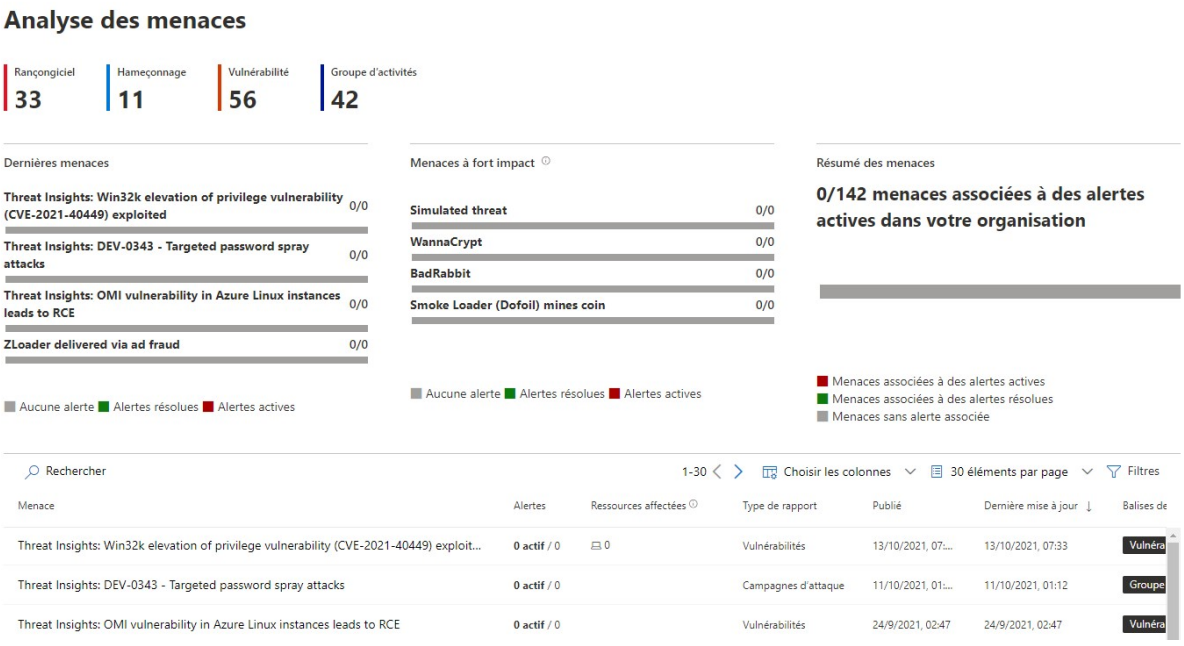
En cliquant sur l'alerte déclenchée, il est possible d'avoir plus d'information la concernant. Également, une liste des mesures conseillées est proposée pour que l'administrateur sache comment réagir pour comprendre ce qu'il s'est exactement passé.

Figure 39 - MDE Exemple d'opération suspecte
(Source : Auteur)



La page « Analyse des menaces » est également intéressante. Elle permet de prendre connaissance de l'ensemble des vulnérabilités et des attaques qui sont enregistrées par Microsoft. Ces menaces ne sont pas celles-qui sont présentes sur notre infrastructure, elles sont celles qui sévissent actuellement dans le monde. Cependant, il est possible de savoir si une de ces menaces affectent nos ressources.

Figure 40 - MDE Analyse des menaces
(Source : Auteur)

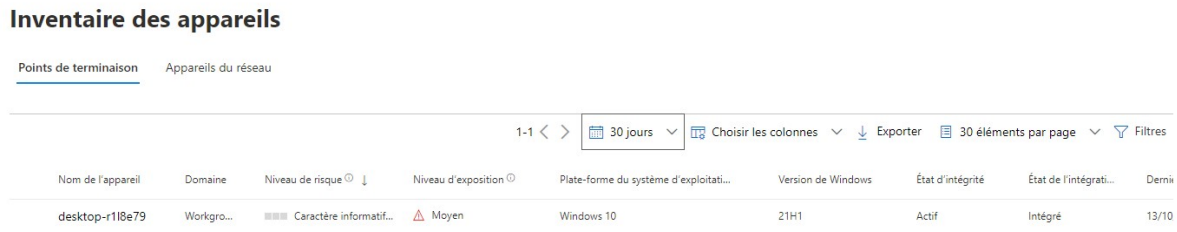


Une autre page intéressante est « Niveau de sécurité Microsoft ». Sur celle-ci, nous pouvons prendre connaissance du score de sécurité que MDE nous attribue. Il est également possible de consulter l'historique des actions qui nous ont fait perdre ou gagner des points. De plus, l'onglet « Actions d'amélioration » nous propose toute une série de stratégies à mettre en place pour améliorer la sécurité de nos clients, et, de ce fait, améliorer notre score.

La rubrique « Point de terminaison » regroupe plusieurs fonctionnalités :

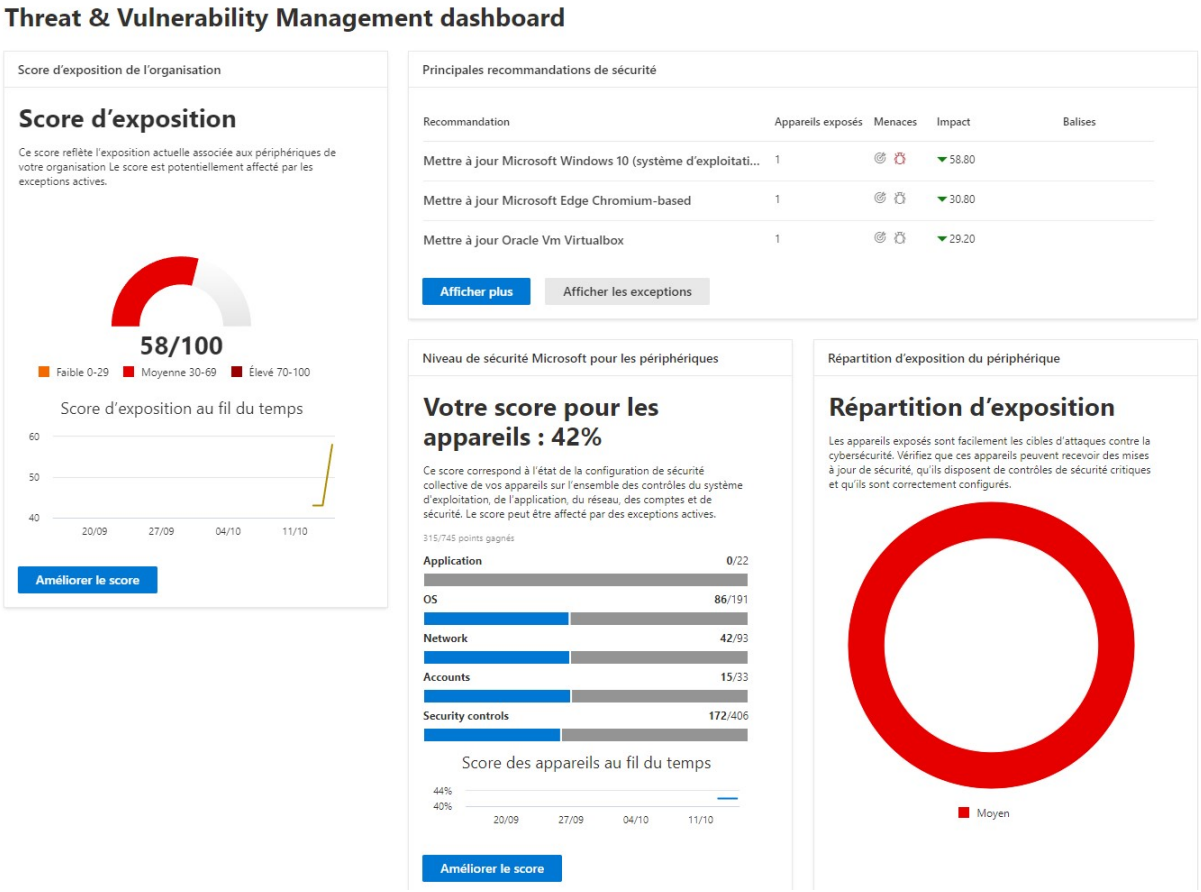
- La recherche des points de terminaison enrôlés dans notre organisation pour bénéficier d'information de sécurité supplémentaire.
- Un inventaire de tous nos appareils et, surtout de leur niveau d'exposition aux menaces détectées.

Figure 41 - MDE Inventaire des appareils
(Source : Auteur)



- La gestion des vulnérabilités de nos appareils regroupe l'ensemble des informations et des recommandations relatives à la santé générale de notre stratégie de sécurité mise en place. Un historique est également disponible afin de constater les mesures précédemment entreprises.

Figure 42 - MDE Gestion des vulnérabilités et des menaces
(Source : Auteur)

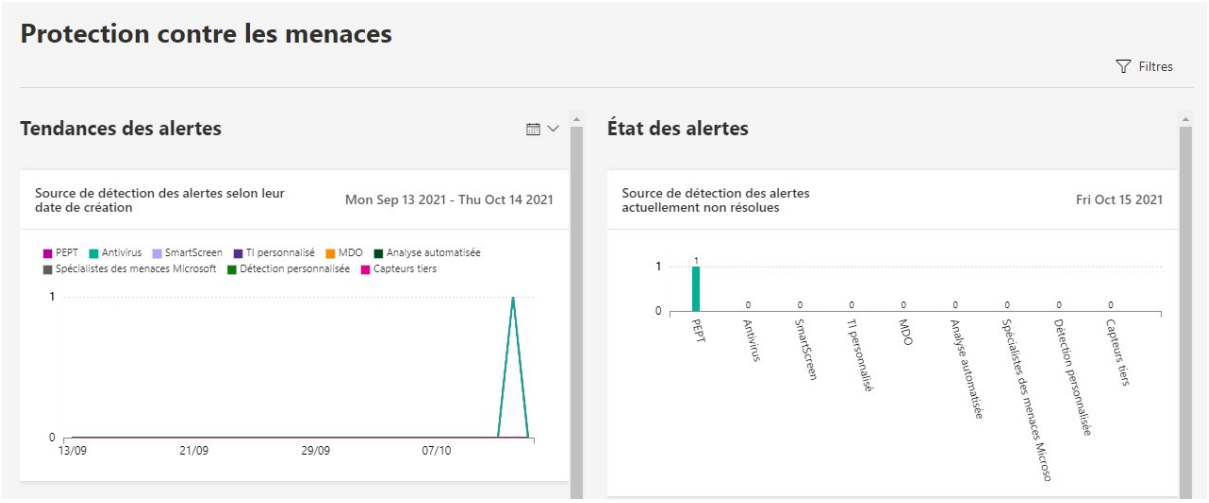


- La rubrique « Evaluations et didacticiels » est particulièrement intéressante pour une première prise en main. En effet, MDE peut mettre en place un laboratoire de test dans le but de comprendre comment le système répond à une attaque. Plusieurs types d'attaque sont disponibles à l'utilisation.

Figure 43 - MDE Evaluation et didacticiels
(Source : Auteur)

La rubrique « Rapports » permet de générer des résultats d'analyse de notre infrastructure.

Figure 44 - MDE Rapport des menaces
(Source : Auteur)



1.3.3. Microsoft Defender for Office 365

Toujours dans le portail Microsoft365 Defender, nous retrouvons le service « Microsoft Defender for Office 365 » qui participe également à garantir la sécurité des clients en agissant sur les courriers électroniques.

Selon le rapport d'une entreprise de cybersécurité, de la période de juillet à octobre 2020, les hackers ont utilisé en majorité (25,36%) le trojan pour infecter les machines via courrier électronique (ESET, 2020, p. 26). Cela peut mener à des graves conséquences sur la machine d'un utilisateur, comme la suppression de ses données ou encore causer des problèmes de performance.

Ainsi, il est possible, avec ce service, d'apposer des règles de sécurité sur les courriels entrants. De plus, un système de monitoring est disponible pour l'administrateur afin d'analyser les dernières menaces et potentiellement prendre des initiatives.

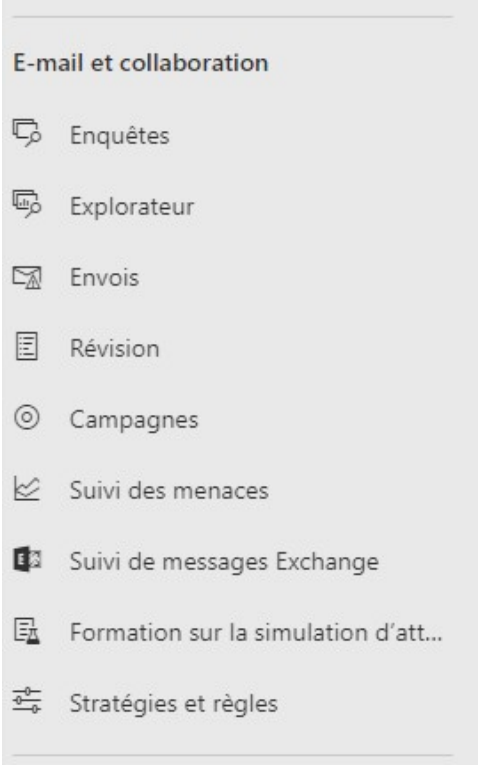
Regardons maintenant d'un peu plus près ce que le service « Microsoft Defender for Office 365 » peut nous offrir.

1.3.3.1. Description du service

Comme expliqué plus haut, la gestion se fait également sur le portail Microsoft365 Defender mais cette fois plus particulièrement sous la rubrique « E-mail et collaboration ».

Sous celles-ci nous retrouvons les pages suivantes :

Figure 45 - MDO365 Menu E-mails et collaboration
(Source : Auteur)



Enquêtes

Lorsque des alarmes sont déclenchées vis-à-vis des mails potentiellement malveillants, elles se retrouvent dans cette section. Il est possible ensuite de prendre les mesures nécessaires pour sécuriser le poste de l'utilisateur.

Explorateur

Selon Microsoft (2021), l'explorateur aide les équipes des opérations de sécurité à examiner les menaces et à y répondre efficacement. Il est possible d'y appliquer des filtres pour faire ressortir uniquement certains types de courriel. De plus, un rapport, permettant d'examiner les courriels malveillants ou encore d'afficher les URL d'hameçonnage, est généré.

Envois

Les utilisateurs ont la possibilité de signaler des messages qu'ils jugent comme étant indésirables. Ceux-ci sont affichés dans cette section. Il est également possible d'envoyer ces courriels à Microsoft pour une analyse plus approfondie.

Révision

Sur cette page il est possible d'accéder :

- Au centre de notification : Celui-ci permet de répertorier toutes les campagnes malveillantes via courriel du moment.
- A la quarantaine : Il est possible de mettre des courriers électroniques en quarantaine si le contenu paraît dangereux.
- Aux Utilisateurs restreints : Lorsqu'un utilisateur envoie trop de courriels, il peut se voir bloquer la fonctionnalité d'en envoyer plus. Dans ce cas, il apparaît dans cette section. Il est possible pour l'administrateur de le débloquer.

Campagnes

Lorsqu'une organisation est victime d'une attaque par courrier électronique de grande ampleur, nous appelons ça une campagne. Par conséquent, cette page permet de les répertorier et de les analyser pour potentiellement en connaître la cause et la source de l'attaque.

Suivi des menaces

Cette page fonctionne de pair avec la page « Explorateur ». Elle permet de suivre les menaces ou les campagnes qui ont été détectées.

Formation sur la simulation d'attaque

Comme pour MDE, « Microsoft Defender for Office 365 » dispose de son laboratoire de test. Celui-ci permet d'envoyer des courriels malicieux de test pour voir le comportement des règles de sécurité mises en place.

Stratégie et règles

C'est la partie la plus intéressante en ce qui concerne la protection des clients. Dans cette page, nous pouvons configurer des règles d'application qui se déclenchent lorsqu'un courriel est reçu par un utilisateur. Il est possible de créer quatre types de règles :

- Stratégie de menace : Permet de créer des règles et des stratégies de lutte contre les menaces de type phishing ou contre les malwares présents dans les pièces jointes.
- Stratégie d'alerte : Cette option permet de créer une stratégie d'alerte qui lance, par exemple, une notification lorsque l'utilisateur fait une action qui concorde avec la stratégie mise en place.

- Gérer les alertes avancées : Redirige l'administrateur vers la plateforme « Cloud App Security » qui permet de paramétrer plus en détail les applications.

- Alertes d'activité : Permet d'alerter un membre du domaine lorsque l'utilisateur lance une action spécifique comme archiver un fichier ou s'il copie un fichier d'un courriel.

1.4. Solutions hybrides

Après s'être intéressé aux infrastructures On-Premise et dans le cloud, il est temps de regarder ce que nous appelons communément le cloud hybride.

Nous définissons le cloud hybride ou mixte comme étant la combinaison entre une infrastructure basée sur site avec une infrastructure utilisant la technologie du Cloud. Cette rencontre entre ces deux mondes permet de bénéficier des avantages de chacun pour construire une nouvelle infrastructure qui répond aux besoins d'une organisation.

Il existe plusieurs raisons qui fait qu'une entreprise souhaite bénéficier d'un environnement mixte. Selon Toroman (2018, p. 239), ces raisons sont entre autres les suivantes :

- Lorsqu'un investissement de grande envergure a été récemment fait pour une infrastructure sur site, il est difficile d'abandonner ce qui a été mise en place pour bénéficier de la puissance du Cloud.

- Il existe certains pays qui n'autorisent pas les entreprises à externaliser à l'étranger les informations personnelles de ses utilisateurs.

Par conséquent, l'implémentation d'une architecture mixte permet de respecter ces raisons ci-dessus et de bénéficier des fonctionnalités de l'informatique en nuage.

Nous nous intéressons dans cette partie uniquement aux solutions de protection des clients qu'un environnement hybride peut apporter. Le but recherché est toujours la protection des points de terminaisons d'une entreprise pour garantir un niveau de sécurité maximal aux utilisateurs.

1.4.1. Cogestion

Microsoft offre la possibilité de combiner l'utilisation d'une architecture On-Premise avec l'utilisation du Cloud pour protéger les clients d'une entreprise. Cela se fait en utilisant un serveur avec le logiciel SCCM et le service Endpoint Manager.

Voici une manière de définir la « Cogestion » ou « Co-Management » :

La cogestion vous permet de gérer simultanément des appareils Windows 10 à l'aide de Configuration Manager et Microsoft Intune. Elle vous permet d'attacher via le cloud votre investissement existant dans Configuration Manager en ajoutant de nouvelles fonctionnalités. À l'aide de la cogestion, vous avez la possibilité d'utiliser la solution de technologie qui convient le mieux à votre organisation (Microsoft, 2021e).

Il existe deux moyens de mettre en place une stratégie de cogestion :

- Configuration Manager déjà appliqué sur des clients : Ce cas de figure se présente lorsque les appareils clients sont déjà configurés et enrôlés sur la console de Configuration Manager. A ce moment-là, il est nécessaire de les inscrire à Intune et de configurer Azure AD hybride permettant de créer une communication entre l'Active Directory On-Premise et celui du Cloud.

- Clients pas encore enrôlés sur Configuration Manager : Cette stratégie s'applique lorsque le Configuration Manager n'est pas encore installé. Les clients sont quant à eux déjà présents et enrôlés sur Intune.

Microsoft explique qu'il y a plusieurs avantages à mettre en place ce type d'architecture.

Tout d'abord, avec une approche de cogestion, il est envisageable de mettre en place un accès conditionnel avec conformité de l'appareil. Ce service permet de gérer les appareils et les comptes d'utilisateur en leur appliquant des règles d'utilisation. Un exemple de règle permet d'obliger la connexion multi-facteur lorsqu'un utilisateur se connecte dans un autre pays.

De plus, la cogestion active la possibilité de bénéficier du contrôle à distance des appareils des employés. Il est complètement envisageable de mettre en place des règles d'utilisation à un utilisateur nomade ne se trouvant pas sur le site de l'entreprise.

En outre, il est légitime de se demander si un risque de conflit est possible. Avec la cogestion, il est nécessaire de basculer une charge de travail sur Intune ou la garder sur Configuration Manager. Cela signifie qu'une partie des fonctionnalités est appliquée sur la console On-Premise et qu'une autre est gérée via le Cloud. Ainsi, il n'y pas de risque de conflit entre les deux services.

1.4.1.1. Description du service

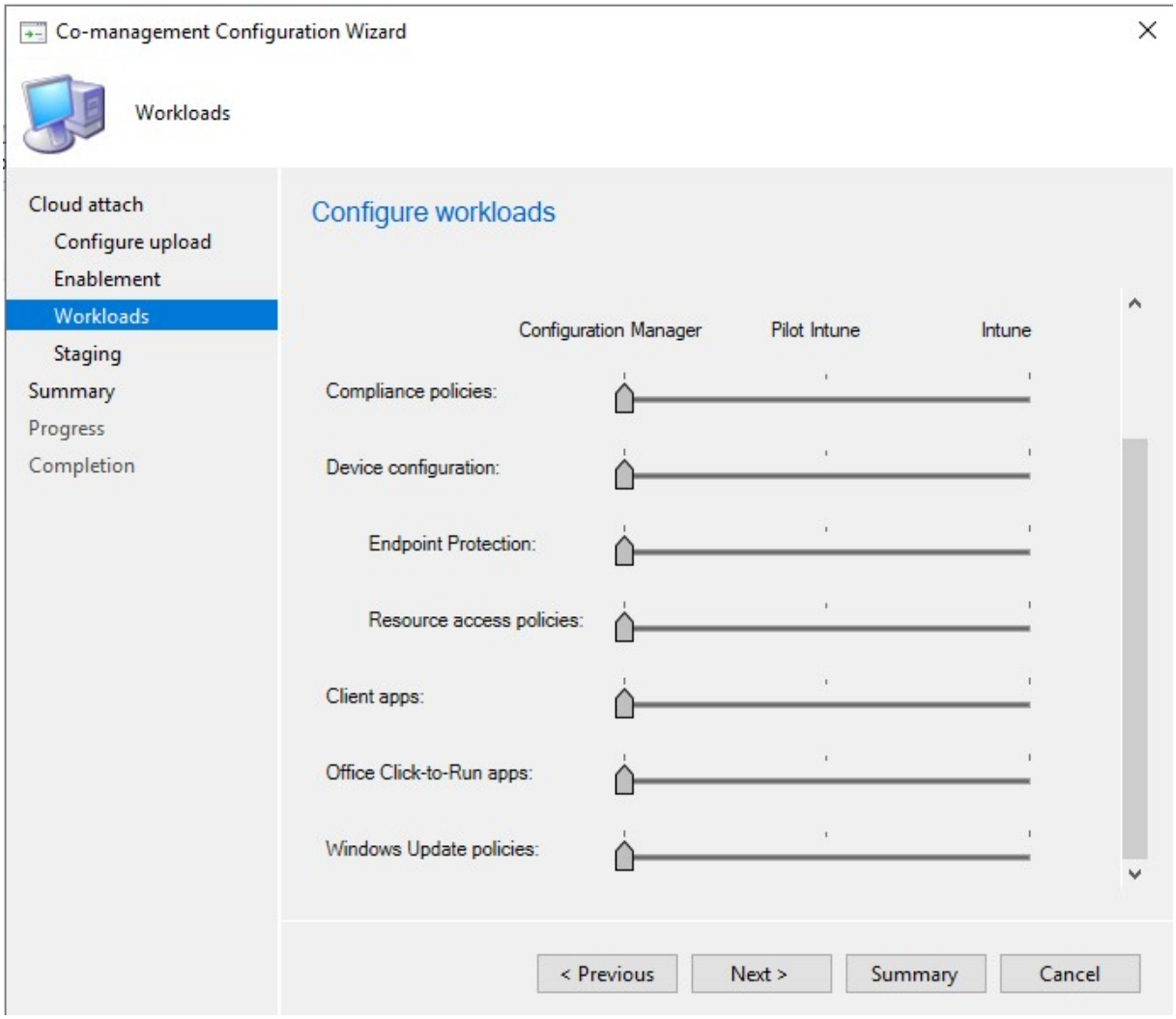
La gestion des règles se passe de la même manière qu'expliquée dans la partie On-Premise de SCCM.

La différence se trouve dans la configuration de la répartition de la charge de travail associée à Intune ou à la console du Configuration Manager.

Nous pouvons donc choisir ici, par quel service, nous voulons effectuer la gestion de la sécurité de nos clients. Il est possible de choisir entre 3 options :

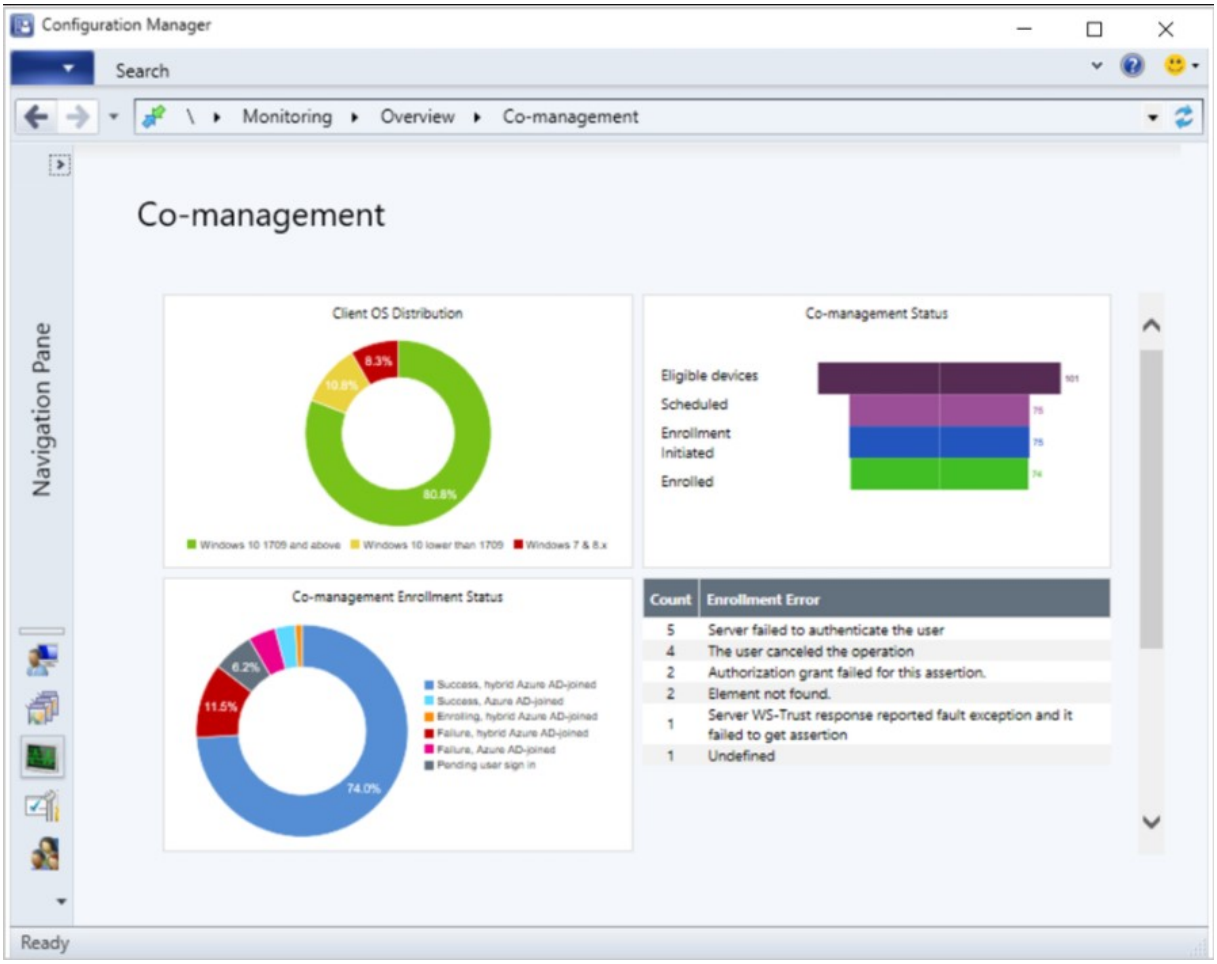
- Configuration Manager : Permet de gérer l'option sur la console de SCCM.
- Pilot Intune : Permet de donner, dans la prochaine page « Staging », la répartition des fonctions spécifiques disponibles dans la protection des clients.
- Intune : Laisse la gestion de l'option dans le Cloud uniquement.

Figure 46 - Cogestion Répartition de la charge de travail
(Source : Auteur)



Dans l'onglet « Monitoring », sous « Co-management », nous avons un tableau de bord qui permet de prendre connaissance de notre architecture cogérée avec le Cloud.

Figure 47 - Cogestion Tableau de bord Monitoring
(Source : Microsoft, 2021r)



Nous décrivons ces métriques ci-dessous :

Distribution des systèmes d'exploitation clients

Ce graphique nous montre le pourcentage pour chaque système d'exploitation présent dans l'infrastructure.

Etat de la cogestion

Il est possible d'avoir une vision globale de l'état de nos machines dans l'environnement cogéré :

- Appareils éligibles : Représente le nombre d'appareils qui sont éligibles à une cogestion.
- Planifié : Représente le nombre d'appareils dont l'inscription dans la cogestion est planifiée.

- Inscription lancée : Permet de voir le nombre de clients sur le point d'être intégré à la cogestion.

- Inscrit : Représente le nombre de point de terminaison enrôlé dans l'architecture de cogestion.

Etat d'inscription à la cogestion

Dans un état de cogestion, un appareil peut rejoindre l'environnement soit via l'Active Directory d'Azure soit via la version hybride d'Azure Active Directory. Cette dernière permet la collaboration entre l'AD On-Premise et celui dans le Cloud.

Sur le graphique ci-dessus, nous avons la possibilité de prendre connaissance des appareils qui ont rejoint la cogestion avec succès, qui sont encore en attente ou qui ont échoués.

Transition des charges de travail

Ce graphique apporte à l'administrateur un graphique à barres démontrant le nombre de clients dont la charge de travail est assignée sur le Cloud.

2. Analyse et choix

Nous passons maintenant à la partie analyse de ce travail afin de déterminer quelle solution entre une infrastructure On-Premise, Cloud ou Mixte est meilleure selon notre hypothèse.

Nous analysons les produits de Microsoft qui sont détaillés dans les rubriques précédentes de ce document.

Pour plus de clarté, nous décidons d'agréger les produits du Cloud en utilisant la dénomination de la licence qui permet d'y accéder : « Entreprise Mobility + Security E5 ».

Par conséquent, nous analysons les solutions suivantes :

- Active Directory avec GPO
- Configuration Management (SCCM)
- Enterprise Mobility + Security E5

Notre hypothèse se base sur la possibilité de travailler en dehors et à l'intérieur du réseau de l'entreprise. Ainsi, nous souhaitons déterminer la meilleure solution dans un potentiel contexte nomade d'utilisation pour une entreprise.

Nous imaginons le scénario d'une start-up qui pratique une stratégie BYOD. En effet, pour limiter les coûts de l'entreprise, qui peuvent être relativement élevés au début, elle demande à ses employés d'utiliser leur propre appareil pour travailler.

Pour analyser notre hypothèse, nous retenons les critères suivants :

- Limites : Nous mettons en place ce critère pour comparer les limites de chacune des solutions.
- Fonctionnalités : Chaque infrastructure dispose de ses fonctionnalités. Ce critère permet de déterminer si la solution analysée dispose des fonctionnalités intéressantes.
- Evolutivité : Une infrastructure est vouée à évoluer avec son temps. Ainsi, nous prenons en compte ce critère pour imaginer une opération de mise à niveau en fonction de l'évolution technologique.
- Maintenance : Nous nous intéressons, avec ce critère, à la nécessité de maintenir une infrastructure spécifique pour un administrateur.
- Déploiement : Nous nous intéressons ici à la facilité de configuration de la solution analysée et de son déploiement sur les postes clients.

- Mobilité : Dans un contexte nomade, il est important de savoir quelle solution possède le plus de potentiel lorsqu'il s'agit d'un accès à l'infrastructure depuis l'extérieur.

Nous ne prenons pas en compte un critère de prix dans cette analyse en raison de la forte disparité en fonction de l'infrastructure et la localisation géographique de l'entreprise.

De plus, les solutions natives à la sécurité de Windows ne sont pas pris en compte dans la matrice de comparaison car elles constituent les paramètres configurables dans les solutions On-Premise, Cloud et Hybride.

2.1. Active Directory avec GPO

2.1.1. Limites

Selon la documentation de Microsoft (2015), il est possible de créer un maximum d'environ 2,15 milliards d'objet par forêt. De plus, un nombre maximal d'identification de sécurité (SID) pour les utilisateurs d'un milliard est possible. En ce qui concerne les GPO, il est envisageable d'appliquer environ 999 règles par utilisateur.

Nous pouvons donc partir du principe que le combo AD associé au GPO permet une grande marge de manœuvre avant d'atteindre sa limite.

2.1.2. Fonctionnalités

En dehors de l'utilisation de l'Active Directory et de ses GPO, il n'existe pas d'outils natifs permettant un « monitoring » intuitif de l'infrastructure comparé aux autres solutions.

Il est cependant possible de se rendre dans l'observateur d'événement de Windows pour avoir un aperçu des changements et du statut de l'AD.

2.1.3. Evolutivité

L'ajout d'un nouvel utilisateur, d'un nouveau domaine ou encore même d'une nouvelle forêt se fait relativement rapidement et facilement.

A noter que dans le cas d'un souhait de se tourner vers une solution Cloud à l'avenir, Microsoft propose un service de migration avec Active Directory Connect. Cette solution permet d'étendre l'AD On-Premise vers le cloud.

De plus, le service Active Directory n'est pas prévu d'être stoppé par Microsoft pour le moment.

2.1.4. Maintenance

En ce qui concerne la maintenance, elle doit être effectuée par des employés de l'entreprise. Cette maintenance a un coût et, si elle n'est pas bien organisée, cela peut se résulter par un dysfonctionnement de l'infrastructure.

De plus, la sauvegarde des données est de la responsabilité de l'entreprise.

2.1.5. Déploiement

L'installation et la configuration d'un Active Directory se fait très facilement en installant le rôle approprié via le gestionnaire de serveur nativement présent sur le système d'exploitation.

Il suffit ensuite de paramétrer les GPO et de les déployer sur la bonne unité organisationnelle.

2.1.6. Mobilité

L'infrastructure est uniquement disponible sur le réseau de l'entreprise, ce qui implique l'utilisation d'un serveur VPN pour y accorder un accès à l'extérieur. Sans cela, il n'est pas possible de bénéficier de l'application de la stratégie de sécurité de l'entreprise.

2.2. Configuration Manager (SCCM)

2.2.1. Limites

Selon la documentation de Microsoft (2021j), dans une topologie de hiérarchie basée sur l'utilisation d'un site principal autonome, il est possible d'enrôler 175'000 appareils Windows sur SCCM. Cependant, de ces 175'000 il n'est possible que de gérer la sécurité de 50'000 d'entre eux. Il est possible d'augmenter ce nombre jusqu'à 100'000 d'appareils gérables mais il est nécessaire de changer la topologie de hiérarchie mise en place pour inclure un site d'administration centrale. Ce cas est généralement réservé pour les grandes organisations.

2.2.2. Fonctionnalités

Configuration Manager permet de bénéficier d'une interface de monitoring pour disposer de métriques intéressantes. Cependant, les métriques ne sont pas aussi développées que sur EMS E5.

De plus, il n'est pas possible d'utiliser la fonction d'accès conditionnel permettant de restreindre l'accès d'un utilisateur selon une liste de critère. L'accès conditionnel est uniquement présent sur le Cloud ou via Co-Management.

2.2.3. Evolutivité

SCCM permet d'évoluer et de profiter des fonctionnalités du Cloud en profitant d'une gestion des points de terminaison hybrides. Avec le Co-management, il est possible d'avoir une partie de la gestion faite par SCCM et une autre dans le cloud via Intune.

Nous pouvons également rajouter que le Configuration Manager est encore continuellement mis à jour et n'est pas prêt d'être stoppé par Microsoft.

2.2.4. Maintenance

Étant donné que SCCM est un outil On-Premise, la gestion de la maintenance des serveurs doivent être effectués par le personnel de l'entreprise dans tous les cas.

2.2.5. Déploiement

L'installation de SCCM implique plusieurs licences et un temps non-négligeable lors de l'installation du logiciel. L'entreprise qui fait le choix de SCCM doit être au courant que sa configuration demande beaucoup de rigueur et de temps.

En ce qui concerne le déploiement, l'enrôlement d'un appareil sur SCCM est contraignant. Il est nécessaire d'attendre parfois plusieurs heures avant que la synchronisation se fasse. Le déploiement de règles sur les appareils peut prendre également le même temps.

2.2.6. Mobilité

SCCM peut être utilisé pour gérer la sécurité des clients en dehors du réseau de l'entreprise mais il est nécessaire de disposer d'un serveur VPN.

Lorsque le Co-management est mise en place, il est possible de basculer la charge de travail sur le Cloud et de configurer les stratégies sans passer par un VPN.

2.3. Microsoft Entreprise Mobility + Security

2.3.1. Limites

Par défaut, il est possible de disposer d'un maximum de 500'000 ressources (ex : utilisateurs, groupes, etc.) par tenant. Cependant, ce nombre peut être augmenté en contactant directement Microsoft.

2.3.2. Fonctionnalités

Le Cloud dispose de nombreuses fonctionnalités disponibles à l'utilisation, comme l'accès conditionnel. Ce dernier n'est pas disponible sur un environnement On-Premise.

De plus, EMS E5 permet d'utiliser Microsoft Defender for Endpoint qui s'avère être un outil utile dans la détection des malwares et dans les solutions proposées pour les traiter.

2.3.3. Evolutivité

Le cloud est entièrement prévu pour apporter un maximum de flexibilité à l'utilisateur. Microsoft propose toujours la version la plus à jour de son service.

L'ajout d'un produit se fait relativement rapidement. Il suffit de disposer d'une licence et de l'ajouter pour bénéficier des services qui y sont associés.

2.3.4. Maintenance

Aucune maintenance n'est nécessaire. Tout le processus est géré directement par Microsoft étant donné que nous nous trouvons dans une structure publique.

2.3.5. Déploiement

Afin de déployer les solutions présentées, il est uniquement nécessaire de contracter un abonnement « Entreprise Mobility + Security » et de configurer un tenant via Microsoft Azure Active Directory.

L'enrôlement d'un appareil est très facile à configurer et en quelques minutes l'appareil est prêt pour la gestion.

Il est cependant nécessaire d'attendre jusqu'à une trentaine de minutes avant qu'une règle s'applique sur un poste client.

2.3.6. Mobilité

La solution est complètement pensée pour une gestion des clients à travers le monde. Il est simplement nécessaire que l'utilisateur se connecte sur le domaine de l'entreprise et qu'il dispose d'une connexion internet.

2.4. Matrice décisionnelle

Pour procéder à notre choix, nous mettons en place une matrice de comparaison. Chaque solution se voit attribuer une note en fonction de l'appréciation générale de chaque critère développé dans la partie précédente.

Les notes données avec leur explication sont les suivantes :

- La note de 4 : Suffisant
- La note de 5 : Bon
- La note de 6 : Excellent

La moyenne arithmétique des notes est ensuite effectuée afin de déterminer quelle architecture nous choisissons.

Tableau 1 - Matrice décisionnelle
(Source : Auteur)

	Limites	Fonctionnalités	Evolutivité	Maintenance	Déploiement	Mobilité	Note
Active Directory + GPO	4	4	5	4	5	5	4,5
SCCM	4	5	5	4	4	5	4,5
On-Premise							**4,5**
EMS E5	5	6	5	6	5	6	5,5
Cloud							**5,5**
Co-management	5	6	5	4	4	6	5
Mix							**5**

Selon la comparaison, ci-dessus, nous nous rendons compte que la meilleure solution validant notre hypothèse se trouve dans le Cloud via la solution EMS E5.

Dans un cadre On-Premise, l'entreprise est dépendante d'une infrastructure à mettre en place. Étant donné qu'elle ne possède pas beaucoup de ressources et de temps pour gérer un environnement sur-site, nous ne recommandons pas cette solution. De plus, il existe des fonctionnalités supplémentaires intéressantes dans le Cloud qui ne sont pas disponibles dans un cadre On-Premise.

Le monde hybride implique également l'existence d'une infrastructure On-Premise. L'architecture hybride permet néanmoins de bénéficier d'une meilleure mobilité grâce à l'absence d'un serveur VPN et des fonctionnalités uniquement présentes sur le Cloud, c'est pourquoi nous lui attribuons une meilleure note que l'architecture On-Premise. Malgré tout, nous ne pouvons pas conseiller ce type d'architecture à une entreprise qui commence son exploitation.

En conclusion, une entreprise, qui vient tout juste de se lancer, ne dispose pas d'une grande infrastructure. Nous pouvons ajouter également que ses ressources sont limitées. Ainsi, une stratégie BYOD couplée avec une infrastructure Cloud permet de passer outre ses inconvénients. La start-up fait bénéficier à ses employés d'une protection avancée et peut se consacrer au reste de ses affaires.

3. Application

Notre analyse nous a permis de déterminer que le Cloud est la meilleure solution permettant la gestion des points de terminaison dans un contexte nomade.

Ainsi, nous développons plusieurs cas d'utilisation constituant les meilleures pratiques à suivre pour sécuriser les postes clients sur le Cloud. Par manque de temps, nous développons uniquement cinq bonnes pratiques à mettre en place lors d'une utilisation du Cloud.

3.1.1. Windows Update for Business

Microsoft, par le biais de son service Intune, permet de gérer l'installation des mis à jour sur les clients d'une entreprise. En effet, il est possible de créer une stratégie de déploiement afin de garantir l'application de patchs correctifs pour Windows.

Les mis à jour sont cruciales dans le cadre de la sécurité afin d'éviter l'exploitation de failles des systèmes de Microsoft connues sous le nom de « Common Vulnerabilities and Exposures » (CVE). Une liste de celles-ci est disponible au grand publique et administrée par l'organisme MITRE, elle-même subventionnée par la « Cybersecurity and Infrastructure Security Agency » (CISA) qui fait partie du département de la Sécurité intérieure des Etats-Unis (RedHat, 2020) :

https://www.cve.org/

En utilisant le service « Windows Update for Business », il est possible de sélectionner le canal de distribution et d'avoir un large contrôle sur les mises à jour qui ajoutent des fonctionnalités ou celles qui améliorent la sécurité.

Étant donné que le service Intune est intrinsèquement lié avec les autres services de Microsoft, tel que « Azure Active Directory », il est envisageable de créer des stratégies pour chaque groupe d'utilisateurs. Par exemple, le groupe contenant les utilisateurs du département des finances d'une entreprise doit bénéficier de mis à jour plus souvent en raison du caractère confidentiel des données traitées.

De plus, dans un contexte BYOD, il est totalement possible de contrôler les mises à jour des appareils externes de l'entreprise. La configuration est complète et va même jusqu'à proposer des tranches horaires dans lesquelles les redémarrages doivent être faits.

Enfin, Microsoft propose également un service de gestion des mis à jour. Celui-ci permet de bénéficier d'une vision globale des versions actuelles de tous les appareils des employés.

3.1.1.1. Informations

Ce guide est basé sur celui réalisé par Mark Dunkerley et Matt Tumbarello dans leur livre *Mastering Windows Security and Hardening* (2020, p. 323-327), qui représente les bonnes pratiques de sécurité à appliquer, et sur la documentation de Microsoft à ce sujet (2021b).

3.1.1.2. Exigences

- Une licence permettant d'utiliser Intune avec configuration du tenant (voir Annexe I).
- Une machine virtuelle ou un ordinateur physique sous Windows 10 connecté à Internet.
- Un utilisateur préalablement crée sur le domaine « Azure Active Directory » avec sa machine enrôlée (voir Annexe II).

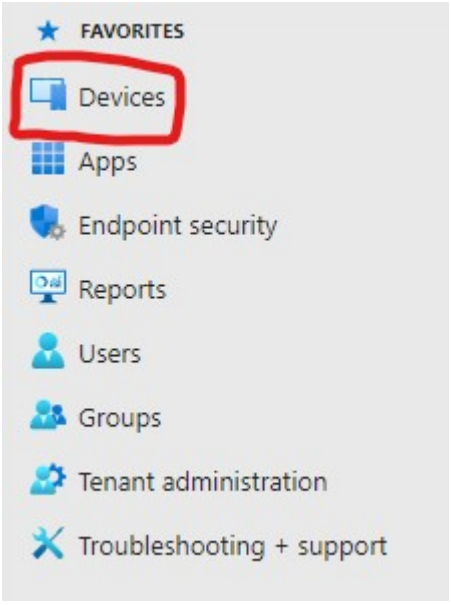
3.1.1.3. Configuration

1) Se connecter sur « Microsoft Endpoint Manager Admin Center » https://devicemanagement.microsoft.com

Figure 48 - MEM Connexion sur le portail pour la stratégie de mise à jour (Source : Auteur)

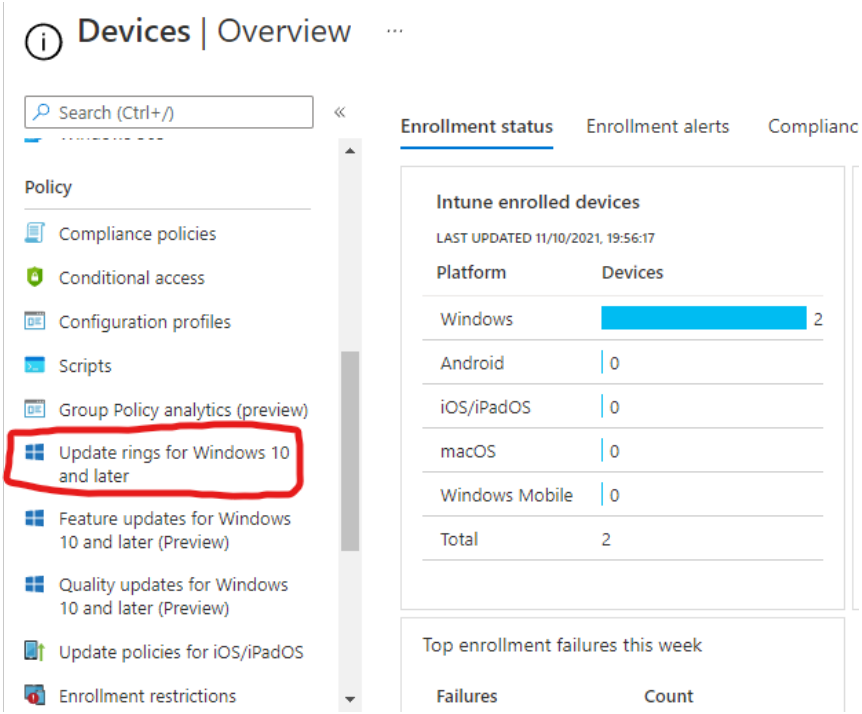
2) Dans le menu latérale droite, cliquer sur « Devices » :

Figure 49 - MEM Rubrique des appareils pour la stratégie de mise à jour
(Source : Auteur)



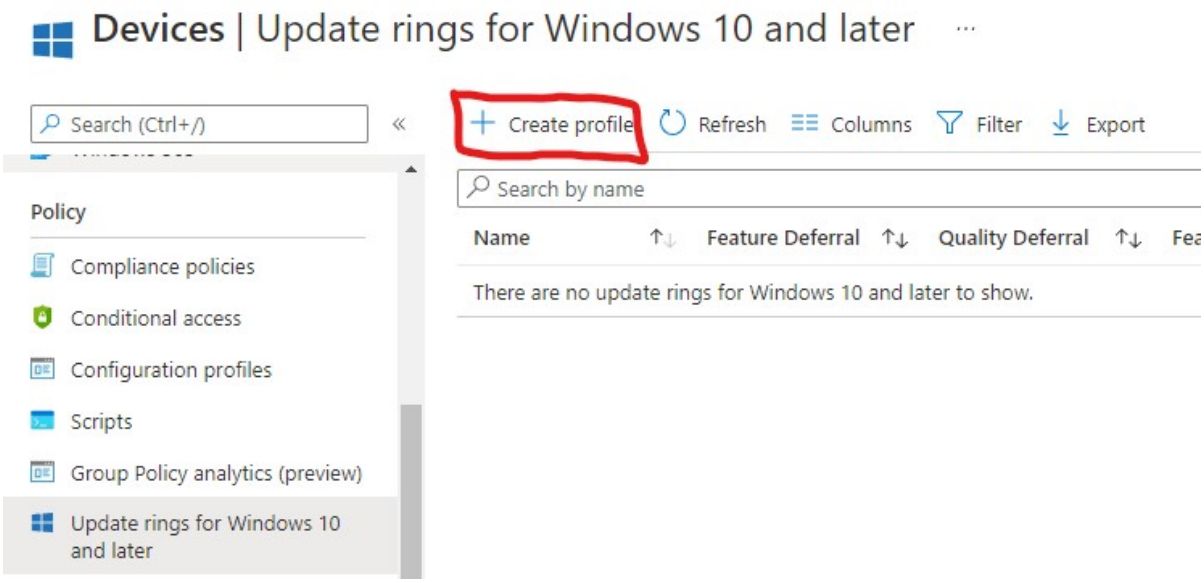
3) Sur la page des appareils, sous la rubrique « Policy », cliquer sur le bouton « Update rings for Windows 10 and later » :

Figure 50 - MEM Rubrique de mise à jour
(Source : Auteur)



4) Cliquer sur le bouton « Create Profile » pour créer une nouvelle stratégie de mise à jour :

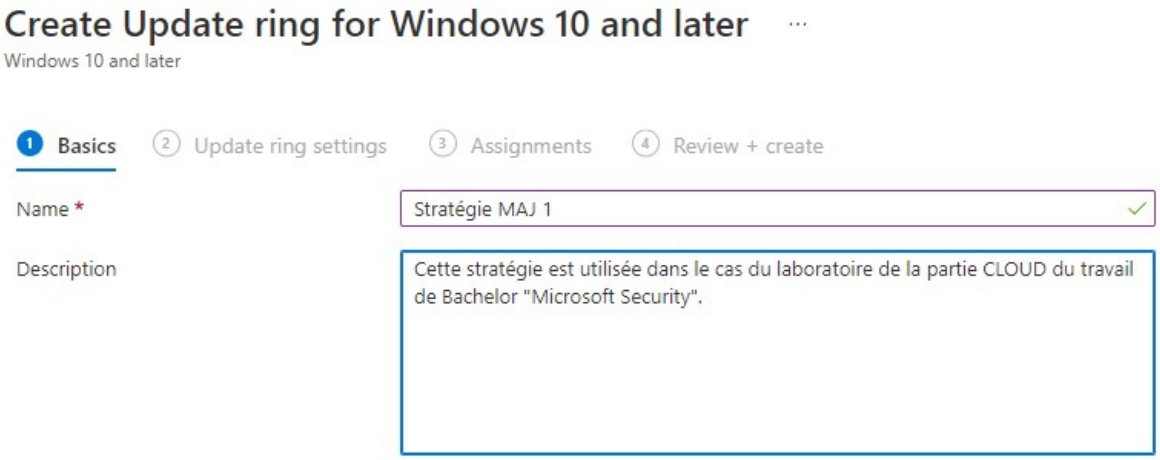
Figure 51 - MEM Création de profil de la stratégie de mise à jour
(Source : Auteur)



5) Remplir selon les informations suivantes et « Next » :

- Name : Nom de la stratégie de mise à jour.
- Description : Description de la stratégie de mise à jour.

Figure 52 - MEM Information de base de la stratégie de mise à jour
(Source : Auteur)



6) Remplir selon les informations suivantes et « Next » :

Update settings

- Servicing channel : Choix du canal de distribution des mises à jour de Microsoft.
    - Semi-Annual Channel : Canal de production de Microsoft. L'entreprise fourni en général deux grandes mises à jour par année.
    - Windows Insider : Canal de bêta-test. Microsoft permet à ses utilisateurs d'essayer des fonctionnalités en avance pour fournir des retours.
- Microsoft product updates : Permet d'autoriser ou de bloquer le scan chez l'utilisateur pour détecter de nouvelles mises à jour.
- Windows drivers : Permet d'autoriser ou de bloquer les mises à jour relatives aux pilotes des périphériques.
- Quality update deferral period (days) : Permet de différer les mises à jour de qualité en soumettant un nombre de jours jusqu'à 30 maximum.
- Feature update deferral period (days) : Permet de différer les mises à jour des fonctionnalités en soumettant un nombre de jours jusqu'à 365 maximum.
- Set feature update uninstall period (2-60 days) : Permet de donner une période après laquelle les mises à jour de fonctionnalités ne peuvent plus être désinstallées.

User experience settings

- Automatic update behavior : Permet de choisir comment les mises à jour sont installées automatiquement sur la machine cliente.
    - Notify download : Cette option n'installe pas la mise à jour automatiquement, elle notifie à l'utilisateur simplement la présence d'une nouvelle mise à jour.
    - Auto install at maintenance time : Cette option permet l'installation d'une mise à jour dans une période de la journée (Il est possible de configurer des heures d'installation).

  - Auto install and restart a scheduled time : Cette option permet l'installation d'une mise à jour et le redémarrage de la machine dans une période de la journée (Il est possible de configurer des heures d'installation et redémarrage).

  - Auto install and reboot without end-user control : Les mises à jour et le redémarrage s'actionnent automatiquement lorsque l'appareil n'est pas en cours d'utilisation et que la batterie n'est pas faible.

  - Reset to default : Permet de revenir à la dernière mise à jour.

- Restart checks : Permet de passer outre les conditions de base de Windows pour effectuer une mise à jour (ex : Niveau de batterie à 40% minimum, Mode présentation activé, etc.)

- Option to pause Windows updates : Permet à l'utilisateur de mettre en pause une mise à jour pour un certain nombre de jour si l'option est activée.

- Option to check for Windows updates : Permet à l'utilisateur de lancer le scan pour découvrir de nouvelles mises à jour à installer.

- Require user approval to dimiss restart notification : Si l'option est acceptée, l'utilisateur reçoit une notification pour l'avertir du redémarrage. Il peut ensuite choisir s'il veut redémarrer ou non. Sinon le redémarrage survient après 25 secondes.

- Remind user prior to required auto-restart with dismissible reminder : Permet de choisir la prochaine apparition de la notification pour redémarrer l'ordinateur. L'utilisateur peut la repousser.

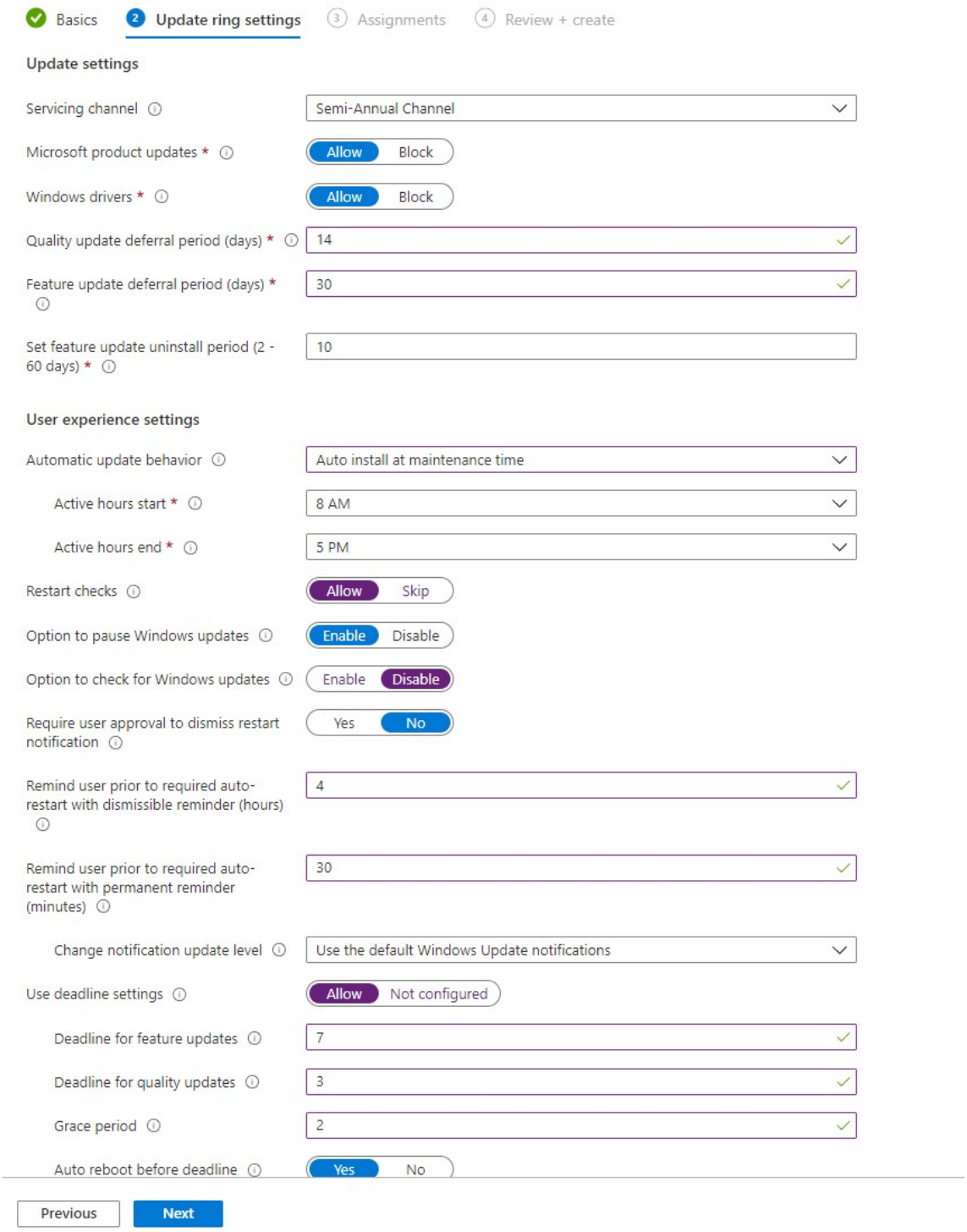
- Remind user prior to required auto-restart with permanent reminder : Permet de choisir la prochaine apparition de la notification pour redémarrer l'ordinateur. L'utilisateur ne peut pas la repousser.

- Change notification Update level : Permet de configurer le type de notification que l'utilisateur reçoit de la part de Windows Update. Il est également possible de désactiver les notifications en excluant ou non celles demandant un redémarrage.

  - Default Windows Update notifications : Utilisation du modèle d'affichage de la notification de base.

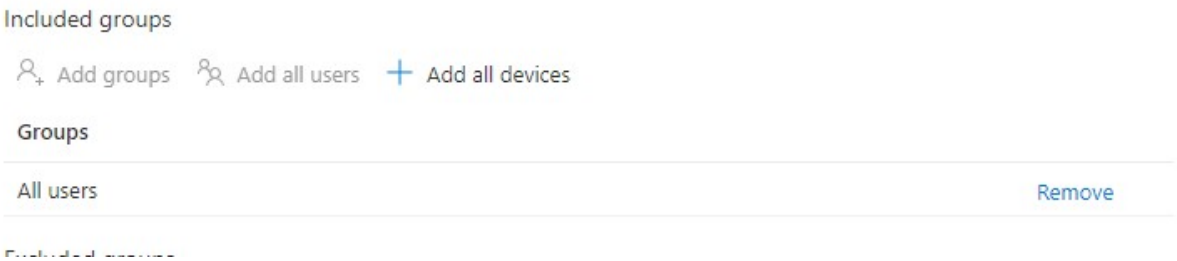
- Use deadline settings : Permet d'appliquer une date limite pour que l'utilisateur fasse la mise à jour. Si elle est dépassée, la mise à jour s'installe automatiquement.

Figure 53 - MEM Paramètres de la stratégie de mise à jour (Source : Auteur)



7) Dans l'écrans suivants, ajouter tous les utilisateurs en cliquant sur le bouton « Add all users » et faire suivant.

Figure 54 - MEM Portée de la règle de mise à jour
(Source : Auteur)



8) Revoir les paramètres appliqués pour la stratégie et cliquer sur le bouton « Create » tout en bas de la page :

Figure 55 - MEM Création de la stratégie de mise à jour
(Source : Auteur)

Create Update ring for Windows 10 and later ...
Windows 10 and later

Basics | Update ring settings | Assignments | 4 Review + create

Summary

Basics

Name	Stratégie MAJ 1
Description	Cette stratégie est utilisée dans le cas du laboratoire de la partie CLOUD du travail de Bachelor "Microsoft Security".

Update ring settings

Update settings	
Servicing channel	Semi-Annual Channel
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	14
Feature update deferral period (days)	30
Set feature update uninstall period (2 - 60 days)	10
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Disable
Require user approval to dismiss restart notification	No
Remind user prior to required auto-restart with dismissible reminder (hours)	4
Remind user prior to required auto-restart with permanent reminder (minutes)	30
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	7
Deadline for quality updates	3
Grace period	2
Auto reboot before deadline	Yes

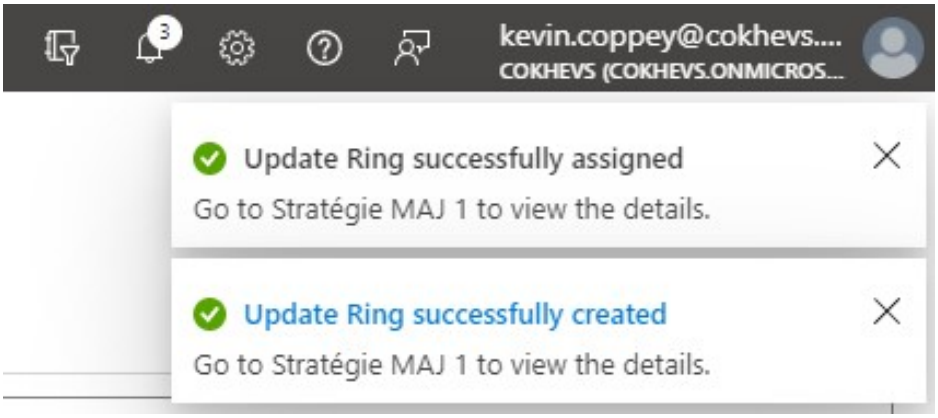
Assignments

Included groups	All users
Excluded groups	--

Previous | Create

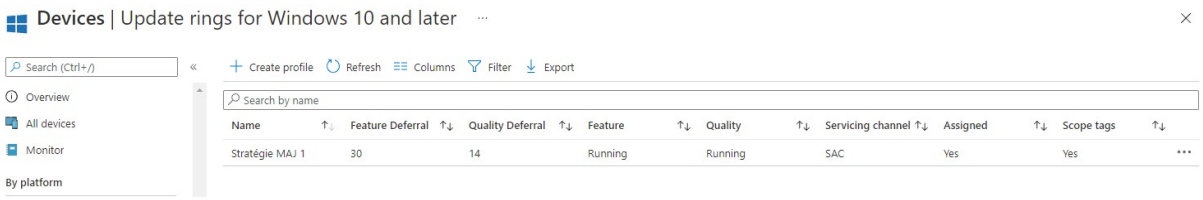
9) Une notification apparaît tout en haut à droite de l'écran pour signaler l'application de la stratégie :

Figure 56 - MEM Notification d'application de la stratégie de mise à jour
(Source : Auteur)



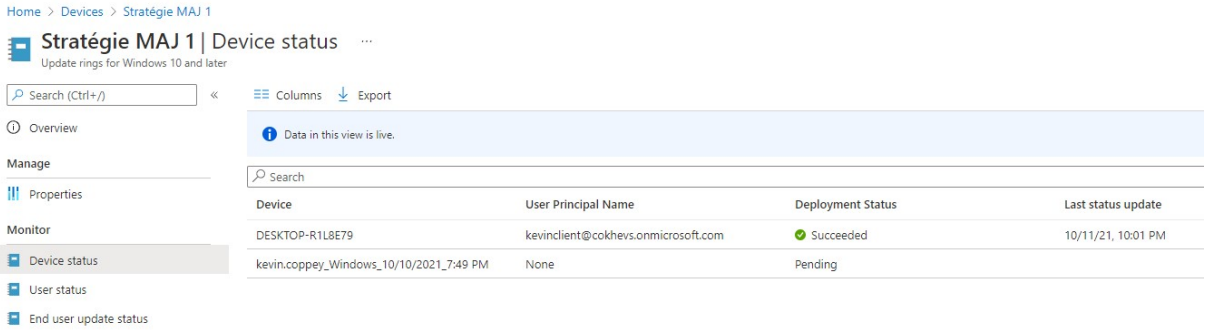
10) Contrôler sous « Update rings for Windows 10 and later » que la stratégie soit présente et qu'elle ait le statut « Running » sous « Quality » et « Feature » :

Figure 57 - Stratégie de mise à jour démarrée
(Source : Auteur)



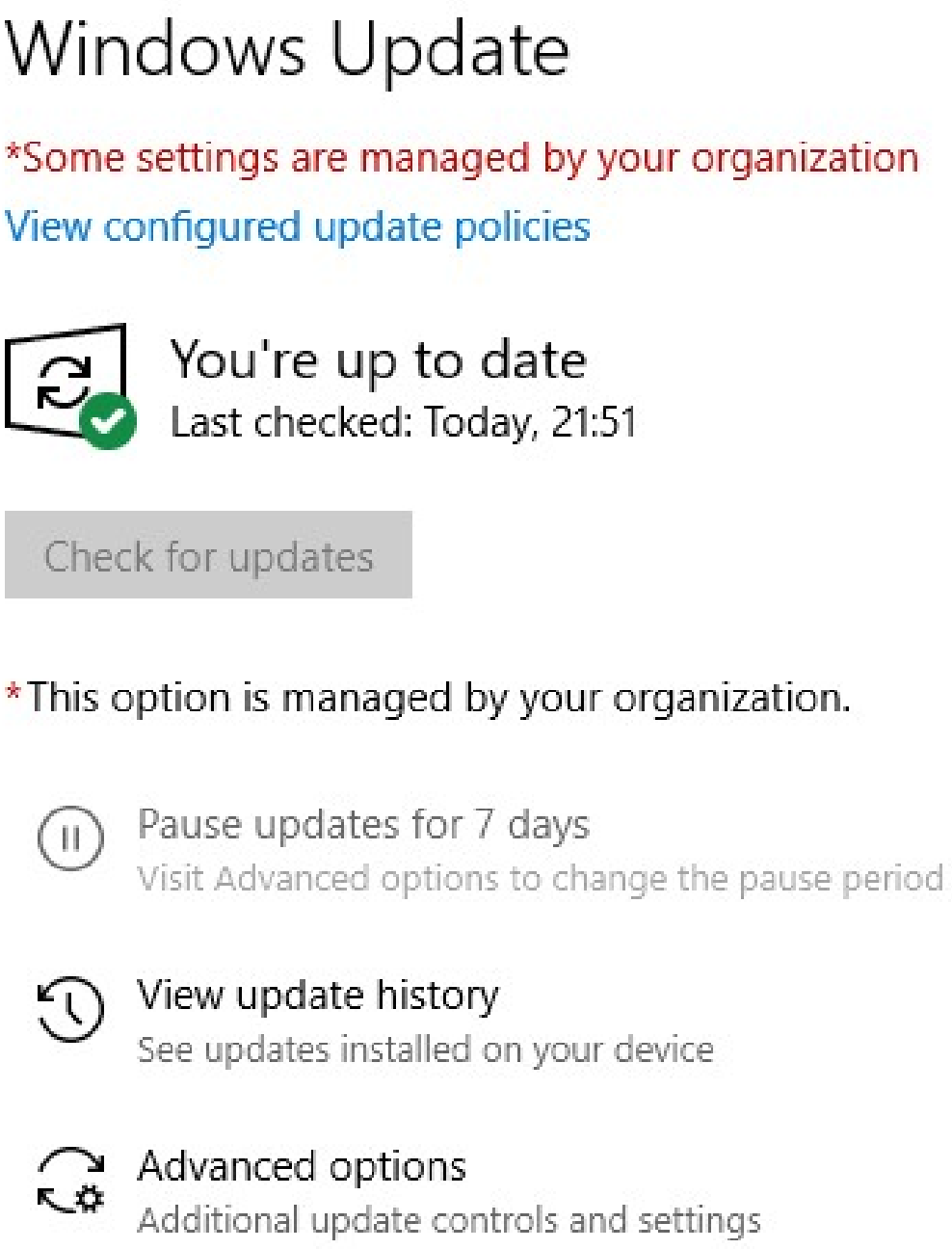
11) Contrôler que la stratégie a été appliquée sur le portail :

Figure 58 - MEM Contrôle de l'application de la stratégie de mise à jour
(Source : Auteur)



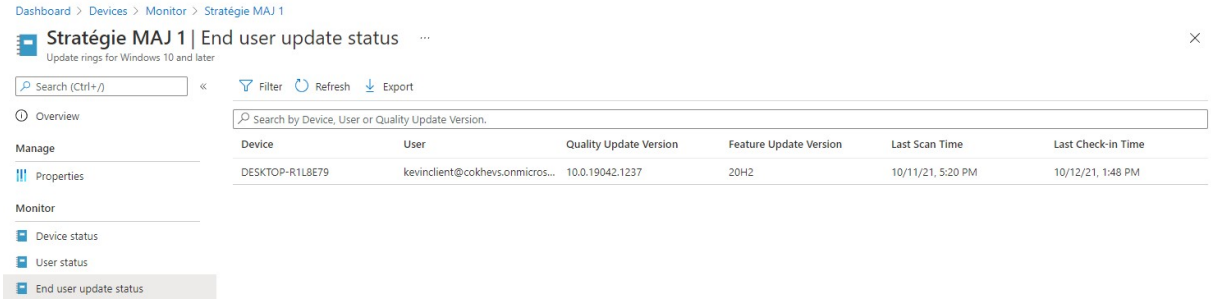
12) Précédemment, nous avons mis en place une option ne permettant pas à l'utilisateur de scanner lui-même si des nouvelles mises à jour sont disponibles. Se rendre sur la machine cliente et vérifier :

Figure 59 - Vérification sur le client de la stratégie de mise à jour
(Source : Auteur)



13) Il est également possible de consulter l'historique des mises à jour effectuées pour chaque version dans la rubrique Monitor > End user update status :

Figure 60 - MEM Historique des mises à jour des clients
(Source : Auteur)



A présent, l'ordinateur est bel est bien synchronisé avec la stratégie que nous avons mise en place dans ce guide pour garantir sa sécurité.

3.1.2. BitLocker Encryption

La sécurité des données est un élément crucial lorsque l'on parle de sécurité des points de terminaison. Il n'est pas très compliqué de prendre le contrôle de toutes les données contenues dans un disque dur ou un SSD d'une personne. Effectivement, en connectant le composant informatique avec un lecteur de disque dur, un hacker a tout le loisir de récupérer toutes les informations stockées appartenant à l'utilisateur si les données ne sont pas chiffrées.

Également, un rapport annuel sur les brèches de données explique que 2% du coût total des crimes relatifs à la cybersécurité concerne le vol de données, ce qui représente environ 120 milliards de dollars américain (Identity Theft Resource Center, 2020, p. 14).

Dans cette optique, il est logique de penser à protéger ces données, surtout dans le cas d'un contexte nomade.

Pour ce faire, Microsoft propose depuis plusieurs années une solution permettant de chiffrer les données présentes sur un ordinateur : « BitLocker ». Microsoft (2018) définit son produit de la manière suivante : « BitLocker est une fonctionnalité de protection des données qui s'intègre au système d'exploitation et résout les menaces de vol ou d'exposition de données provenant d'ordinateurs perdus, volés ou mis hors service de manière inappropriée. »

Depuis son déploiement, BitLocker est géré par l'outil « Microsoft BitLocker Administration and Monitoring » (MBAM). Cependant, Microsoft (2019a) a annoncé que MBAM ne recevra plus aucune mise à jour d'ici avril 2026. En effet, l'entreprise encourage désormais de passer sur ses solutions cloud pour s'occuper du déploiement et de la gestion de BitLocker.

Ce faisant, nous détaillons, dans cette partie du document, la mise en place d'une stratégie de chiffrement des données en utilisant les fonctionnalités du Cloud de Microsoft.

3.1.2.1. Informations

Ce guide est basé sur celui réalisé par Mark Dunkerley et Matt Tumbarello dans leur livre *Mastering Windows Security and Hardening* (2020, p. 331-334), qui représente les bonnes pratiques de sécurité à appliquer, et sur la documentation de Microsoft à ce sujet (2021e).

3.1.2.2. Exigences

- Une licence permettant d'utiliser Intune avec configuration du tenant (voir Annexe I).
- Une machine virtuelle ou un ordinateur physique sous Windows connecté à Internet.
- Un utilisateur préalablement crée sur le domaine « Azure Active Directory » avec sa machine enrôlée (voir Annexe II).

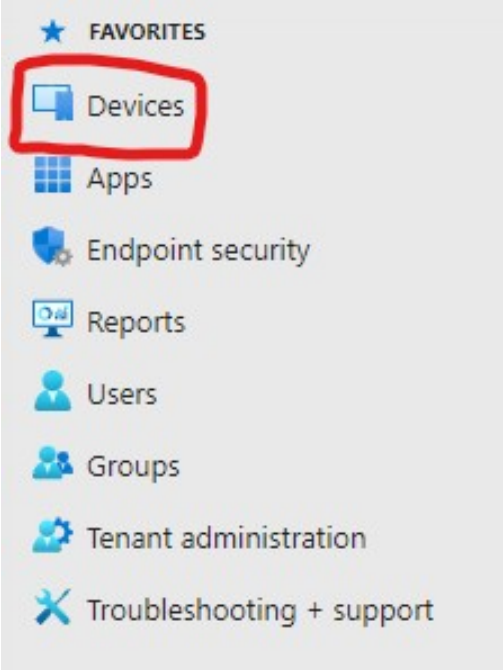
3.1.2.3. Configuration

1) Se connecter sur « Microsoft Endpoint Manager Admin Center » https://devicemanagement.microsoft.com

Figure 61 - MEM Accueil pour la stratégie BitLocker
(Source : Auteur)

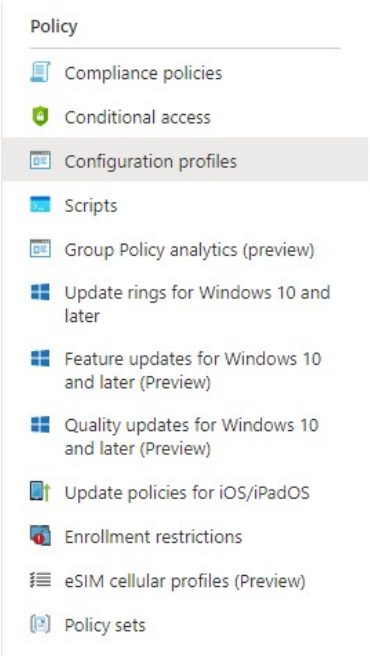
2) Dans le menu latérale droite, cliquer sur « Devices » :

Figure 62- MEM Menu pour la stratégie BitLocker
(Source : Auteur)



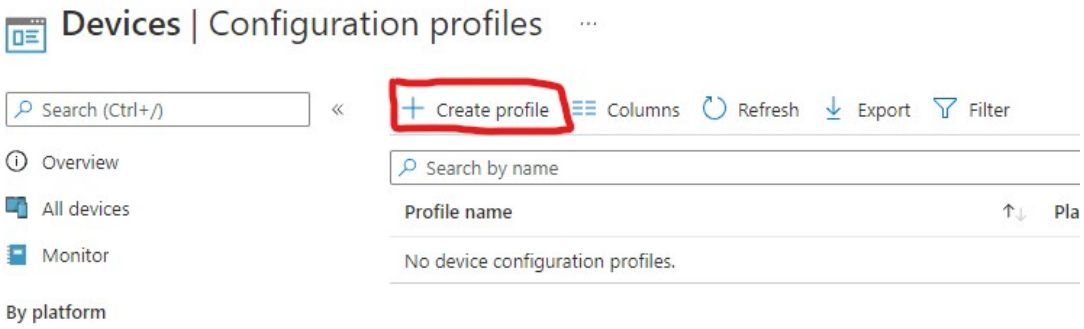
3) Sous la rubrique « Policy », cliquer sur « Configuration profiles » :

Figure 63- MEM Configuration des profiles pour la stratégie BitLocker
(Source : Auteur)



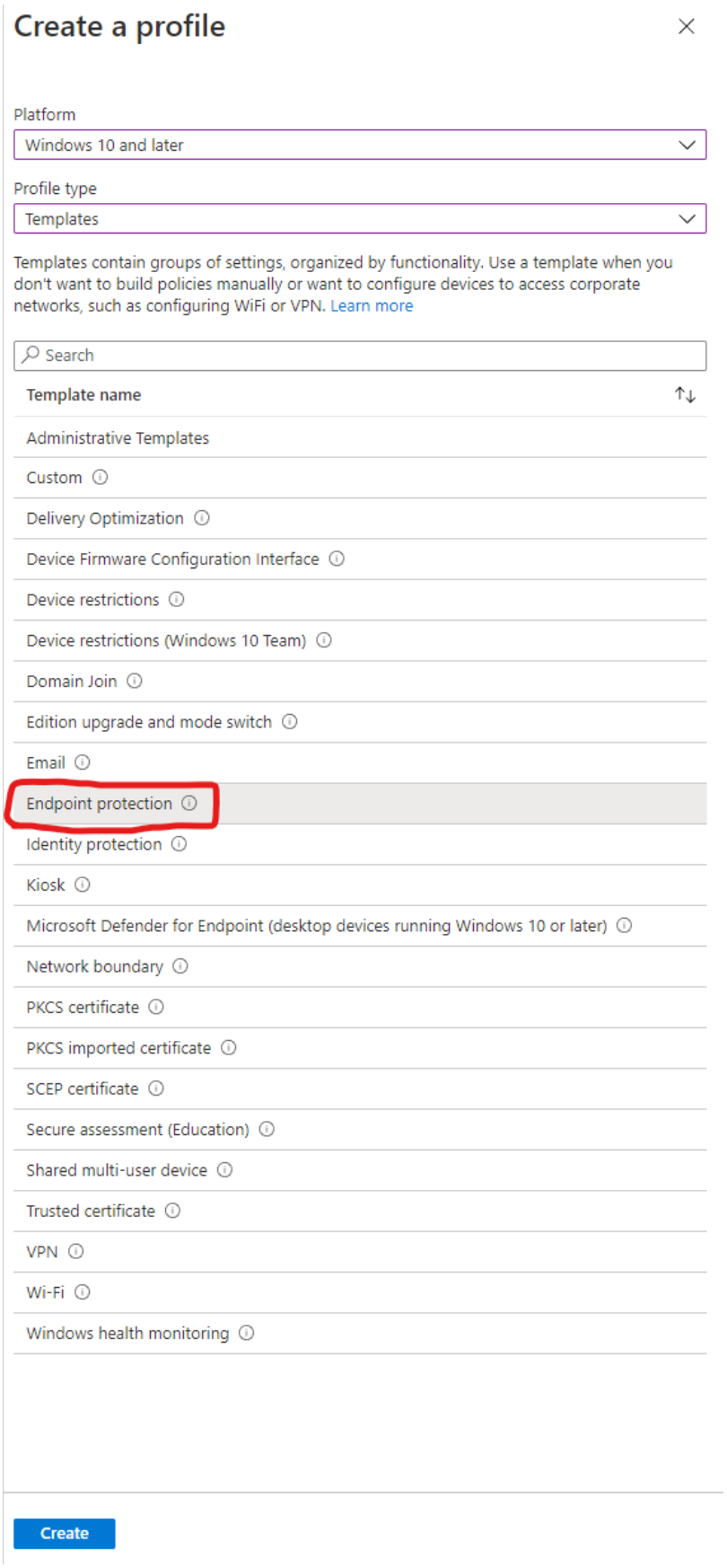
4) Cliquer ensuite sur « Create profile » dans la barre d'outils en haut de la page :

Figure 64 - MEM Ajout d'une nouvelle stratégie BitLocker
(Source : Auteur)



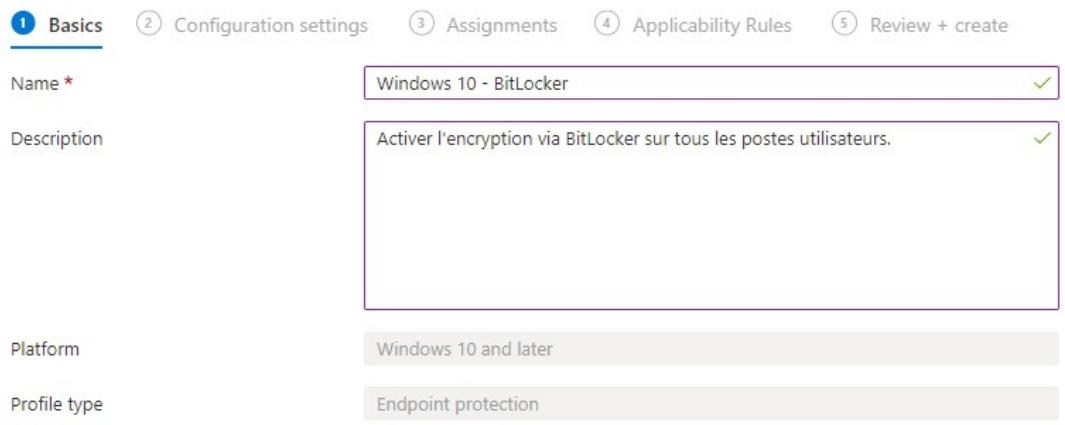
5) Dans le menu contextuel qui apparaît à droite de l'écran, remplir selon l'image suivante, choisir « Endpoint protection » et cliquer sur « Create » :

Figure 65 - MEM Rubrique protection des clients pour la stratégie BitLocker
(Source : Auteur)



6) Remplir selon les informations suivantes et cliquer sur « Next » tout en bas de la page :

Figure 66 - MEM Information de base pour la stratégie BitLocker
(Source : Auteur)

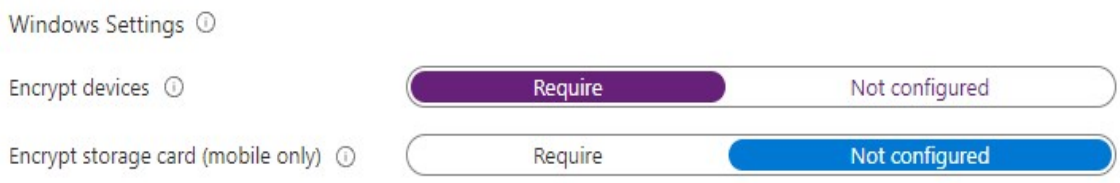


7) Sous la rubrique « Windows Encryption », remplir selon les informations suivantes :

Windows settings

- Encrypt devices : En choisissant d'activer cette option, BitLocker s'active.
- Encrypt storage card : Cette option permet de chiffrer les cartes de stockages qui sont des composantes de Windows mobile et Windows Phone 8.1 uniquement.

Figure 67 - MEM Paramètres Windows pour la stratégie BitLocker
(Source : Auteur)



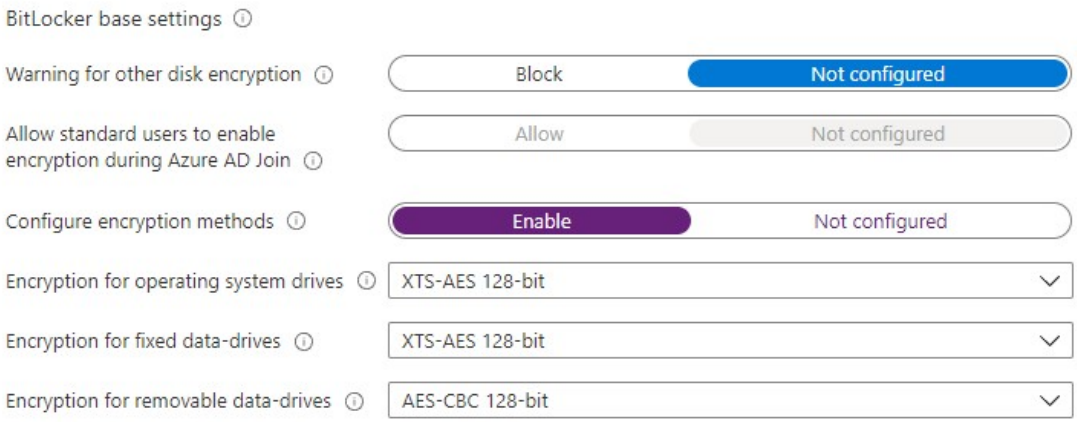
BitLocker base settings

- Warning for other disk encryption : Ce paramètre permet d'afficher une fenêtre expliquant à l'utilisateur les dangers d'utiliser une autre solution de chiffrement en même temps que BitLocker. S'il est bloqué, l'installation se fera silencieusement.

- Allow standard users to enable encryption during Azure AD Join : Cette option permet, aux utilisateurs n'ayant pas de droits administrateurs, de chiffrer leurs données. Cette option est uniquement disponible sur les appareils, sur lesquels le service « Azure Active Directory Joined »[1] (AADJ) est activé.

- Configure encryption methods : En activant cette option, l'administrateur peut choisir le type de chiffrement des données selon le type de disque utilisé. Par défaut, BitLocker utilise l'algorithme de chiffrement XTS-AES 128.

Figure 68 - MEM Paramètres BitLocker de base pour la stratégie BitLocker (Source : Auteur)



Étant donné que notre machine virtuelle ne contient pas de puce TPM, Microsoft (2021e) nous indique que nous ne pouvons pas lancer l'installation silencieuse. Dans un environnement professionnel, il est utile de la mettre en place pour rendre la configuration automatique.

BitLocker OS drive settings

- Additional authentication at startup : Activer cette option permet de configurer un autre moyen d'authentification lorsque BitLocker est activé. Il est possible d'utiliser la puce TPM ou le PIN de Windows Hello comme moyen d'authentification.

- BitLocker with non-compatible TPM chip : Dans l'optique ou l'appareil de l'utilisateur ne dispose pas d'une puce TPM ou d'une version suffisante de celle-ci, BitLocker est désactivé.

- Compatible TPM startup : Permet de déterminer si une puce TPM est obligatoire, autorisée ou interdite.

[1] AADJ est l'état de synchronisation entre AD On-Premise et de AD Azure dans un contexte d'utilisation hybride.

- Compatible TPM startup PIN : Permet de déterminer si l'authentification PIN via TPM est obligatoire, autorisée ou interdite.

- Compatible TPM startup key : Permet de déterminer si l'authentification par insertion d'un lecteur flash USB contenant une clé de démarrage via TPM est obligatoire, autorisée ou interdite.

- Minimum PIN Length : Cette option est utilisée pour configurer la longueur minimum du PIN.

- Minimum PIN characters : Cette option est utilisée pour configurer le nombre minimum de caractère présent dans le PIN.

- OS drive recovery : Ce paramètre permet de définir la stratégie de restauration lorsque la clé de démarrage n'est pas disponible.

- Certificate-based data recovery agent : Permet de bloquer l'apparition de l'agent de restauration des données avec des lecteurs chiffrés par BitLocker.

- User creation of recovery password : Permet de configurer l'autorisation, l'obligation ou l'interdiction de générer un mot de passe de recouvrement de 48 caractères si le mot de passe est perdu.

- User creation of recovery key : Permet de configurer l'autorisation, l'obligation ou l'interdiction de générer une clé cryptographique de recouvrement de 256-bits si le mot de passe est perdu.

- Recovery options in the BitLocker setup wizard : Ce paramètre permet de bloquer les options de recouvrement lorsque BitLocker est activé.

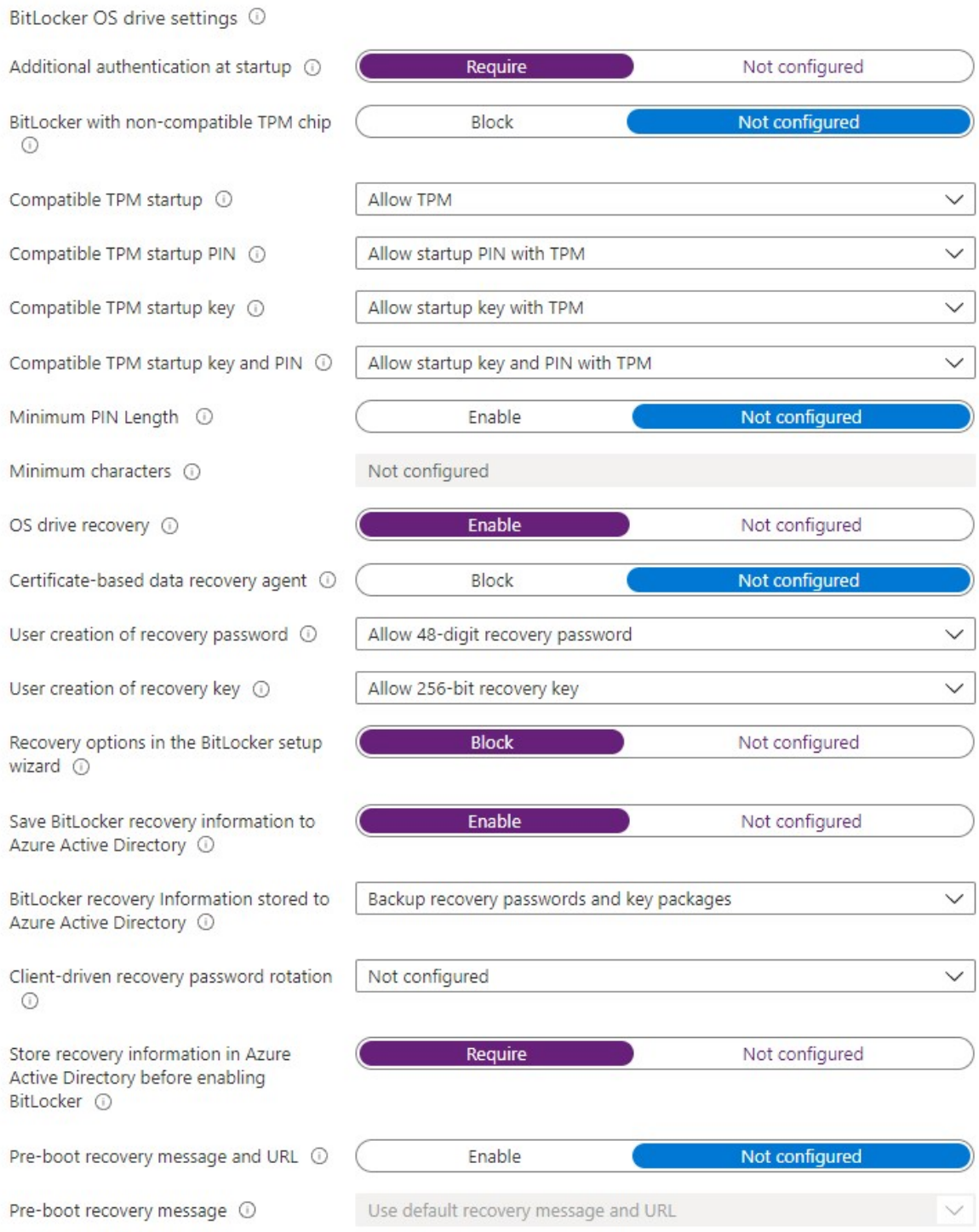
- Save BitLocker recovery information to Azure Active Directory : En activant cette fonctionnalité, la clé de recouvrement est sauvegardée dans les informations de l'appareil d'un utilisateur sur Azure Active Directory.

- Client-driven recovery password rotation : Si ce paramètre est activé, l'utilisateur est invité à choisir un nouveau mot de passe lorsqu'une restauration du système d'exploitation a lieu.

- Store recovery information in Azure Active Directory before enabling BitLocker : Cette option empêche un utilisateur d'activer BitLocker tant que les informations de restauration ne sont pas sauvegardées sur « Azure Active Directory ».

- Pre-boot recovery message and URL : Ce paramètre permet de personnaliser le message de restauration des données.

Figure 69 - MEM Paramètres de disque contenant le système d'exploitation pour la stratégie BitLocker (Source : Auteur)

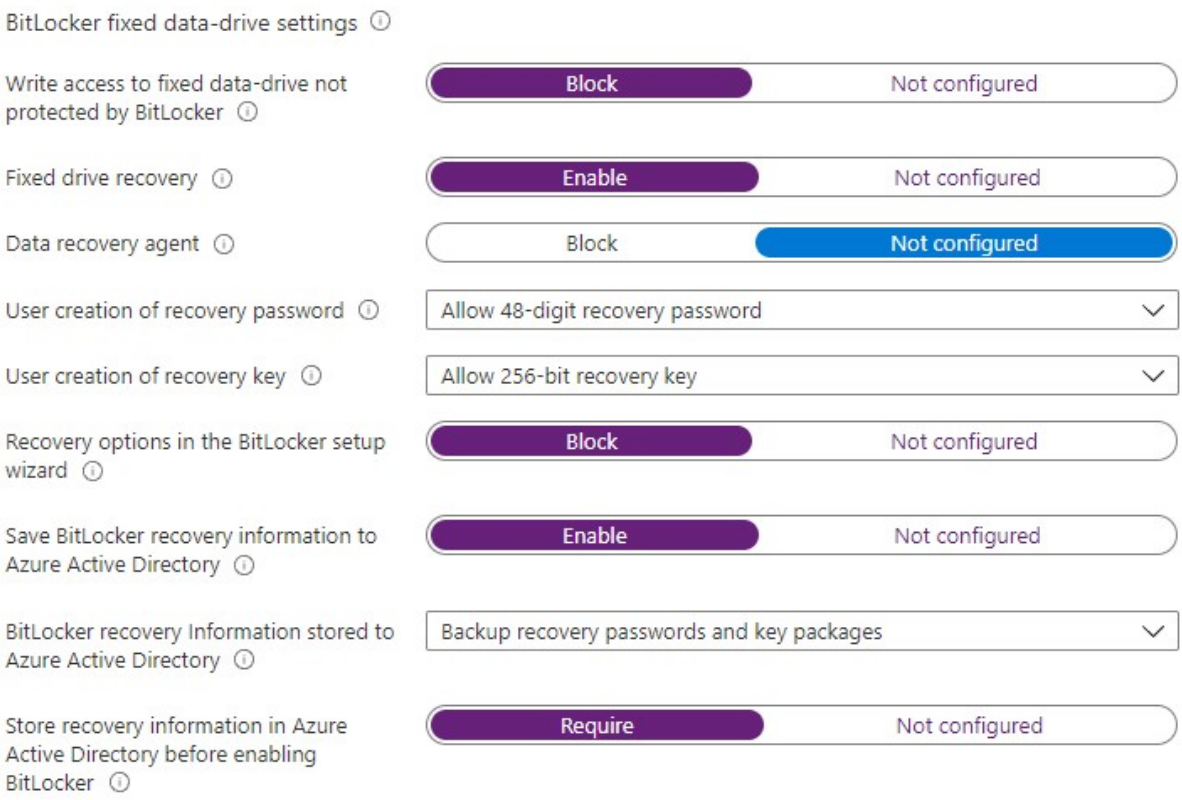


BitLocker fixed data-drive settings

- Write access to fixed data-drive not protected by BitLocker : Choisir "Block" permet de bloquer l'écriture sur un disque dur lorsque BitLocker n'est pas activé.

- Fixed drive recovery : Permet de contrôler la manière dont les disques durs sont restaurés en proposant des alternatives.
- Data recovery agent : Ce paramètre bloque l'apparition de l'agent de restauration avec des disques durs chiffrés.

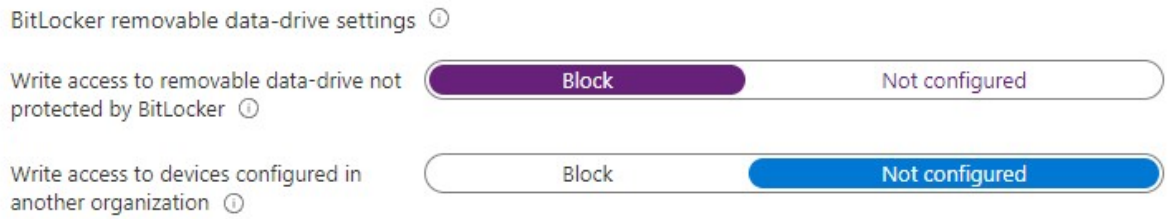
Figure 70 - MEM Paramètres de disque pour la stratégie BitLocker
(Source : Auteur)



BitLocker removable data-drive settings

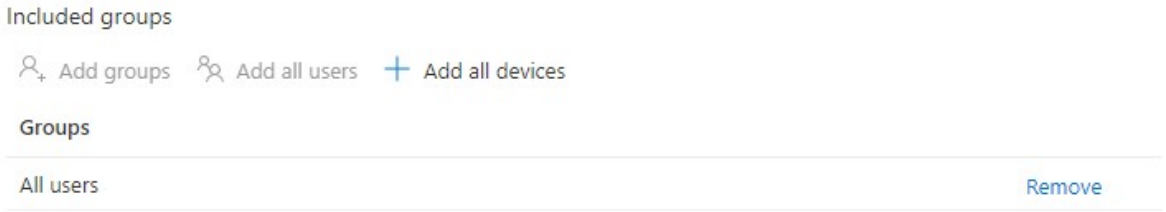
- Write access to removable data-drive not protected by BitLocker : Choisir "Block" permet de bloquer l'écriture sur un disque amovible lorsque BitLocker n'est pas activé.
- Write access to devices configured in another organization : Permet l'écriture des données sur un disque amovible venant d'une organisation externe.

Figure 71 - MEM Paramètres de disque externe pour la stratégie BitLocker
(Source : Auteur)



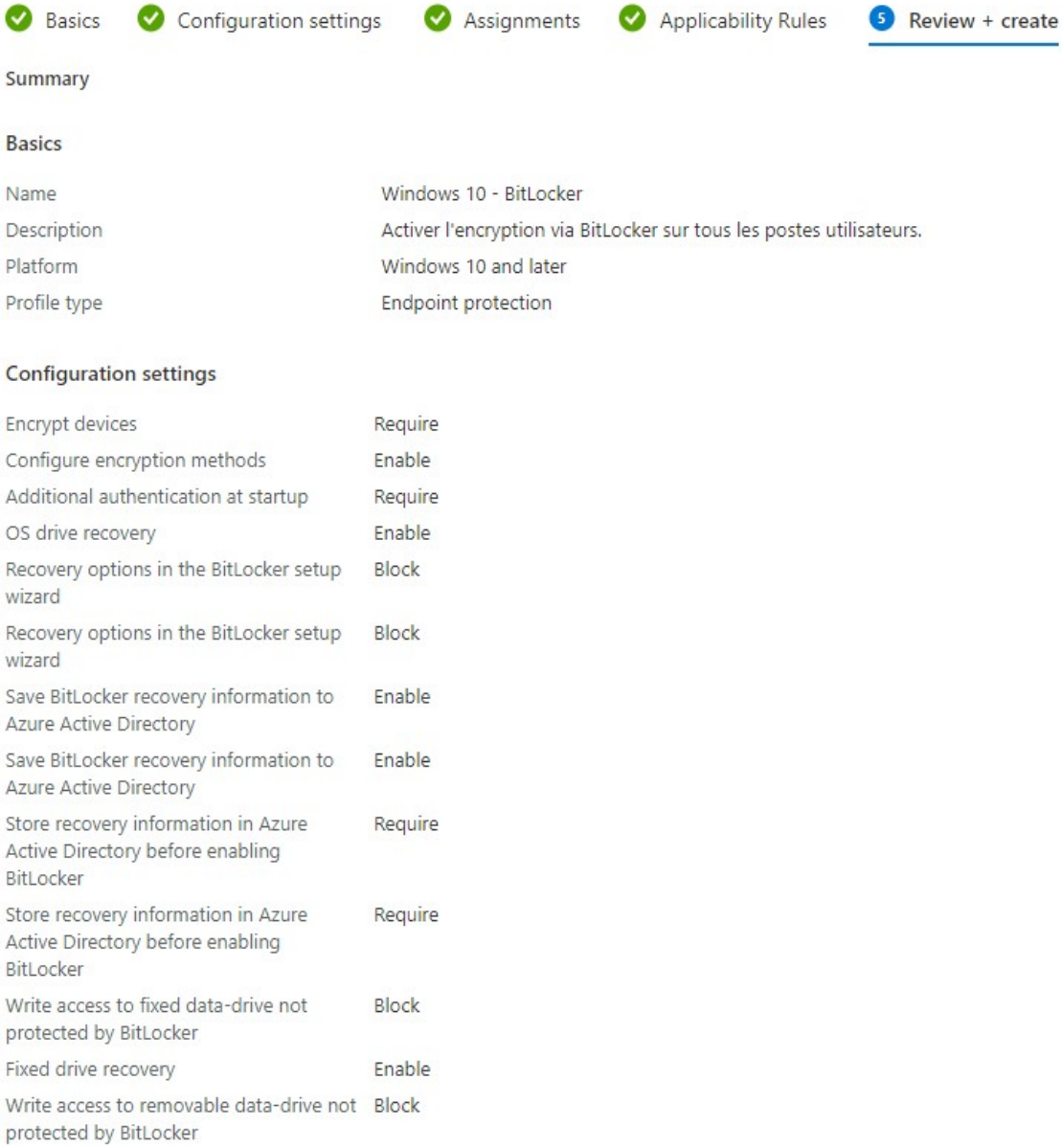
8) Sur la page suivante, cliquer sur « Add all users » :

Figure 72 - MEM Portée ajoutée pour la stratégie BitLocker
(Source : Auteur)



9) Vérifier la configuration et cliquer sur « Create » en bas de la page :

Figure 73 - Création de la stratégie BitLocker
(Source : Auteur)



10) Après quelques minutes, la stratégie se met en place et une notification apparaît chez l'utilisateur. Cliquer sur cette notification :

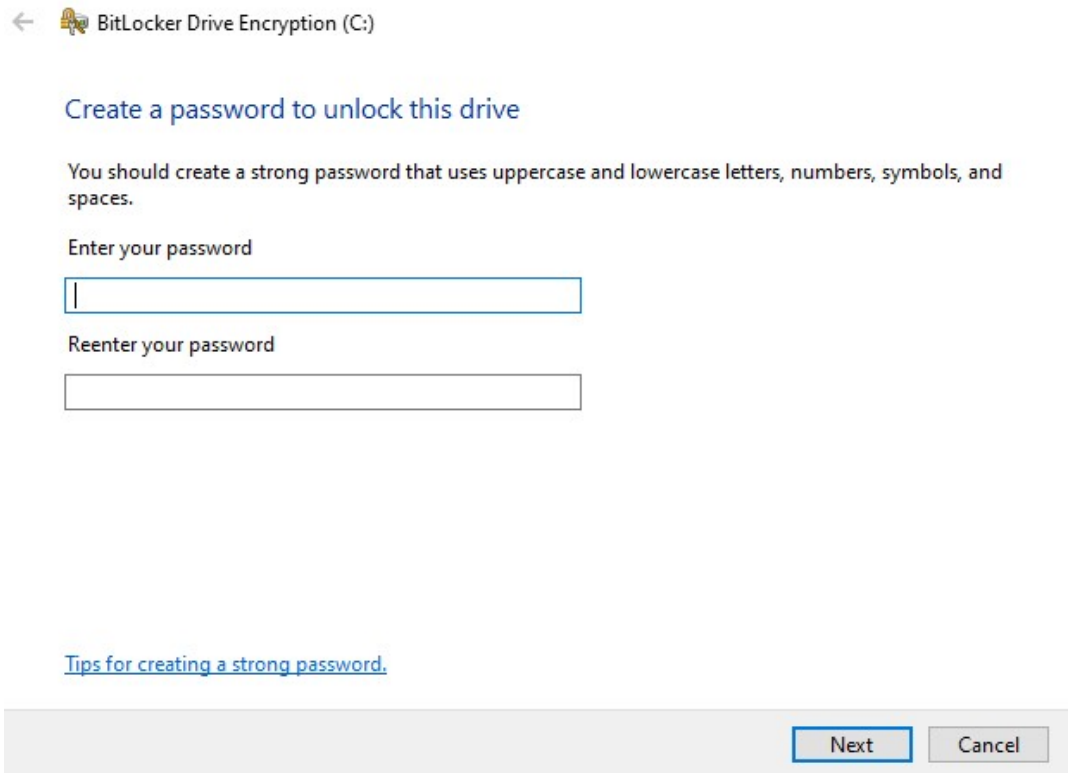
Figure 74 - Notification sur le client pour la stratégie BitLocker
(Source : Auteur)

11) Dans la fenêtre suivante, cocher la première case car nous ne disposons pas d'autres logiciels de chiffrement des données et cliquer sur « Yes ».

Figure 75 - Début du processus de chiffrement
(Source : Auteur)

12) Entrer un mot de passe à utiliser pour déchiffrer les données et cliquer sur « Next » :

Figure 76 - Choix du mot de passe pour la stratégie BitLocker
(Source : Auteur)



13) Dans la prochaine fenêtre, choisir de chiffrer uniquement la partie du disque utilisée et cliquer sur « Next ». Les nouvelles données écrites sont aussi chiffrées automatiquement.

Figure 77 - Choix de la méthode de chiffrement
(Source : Auteur)

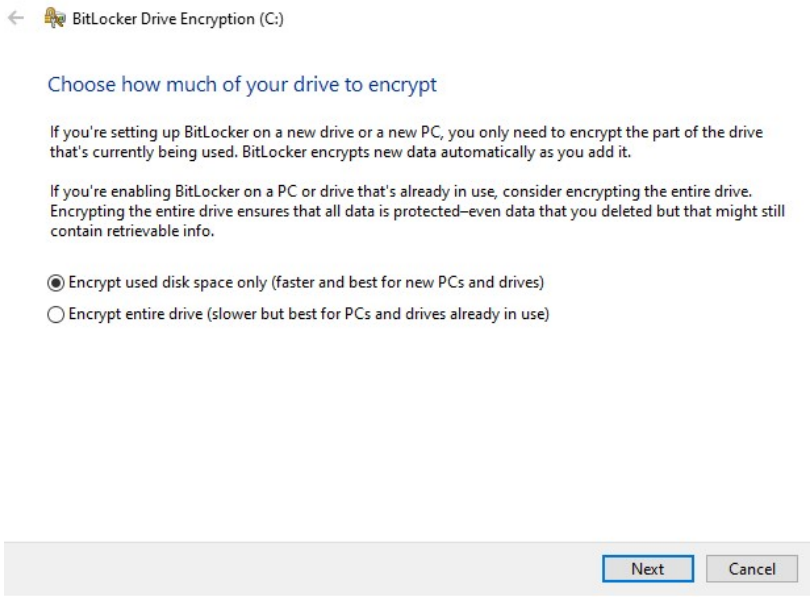
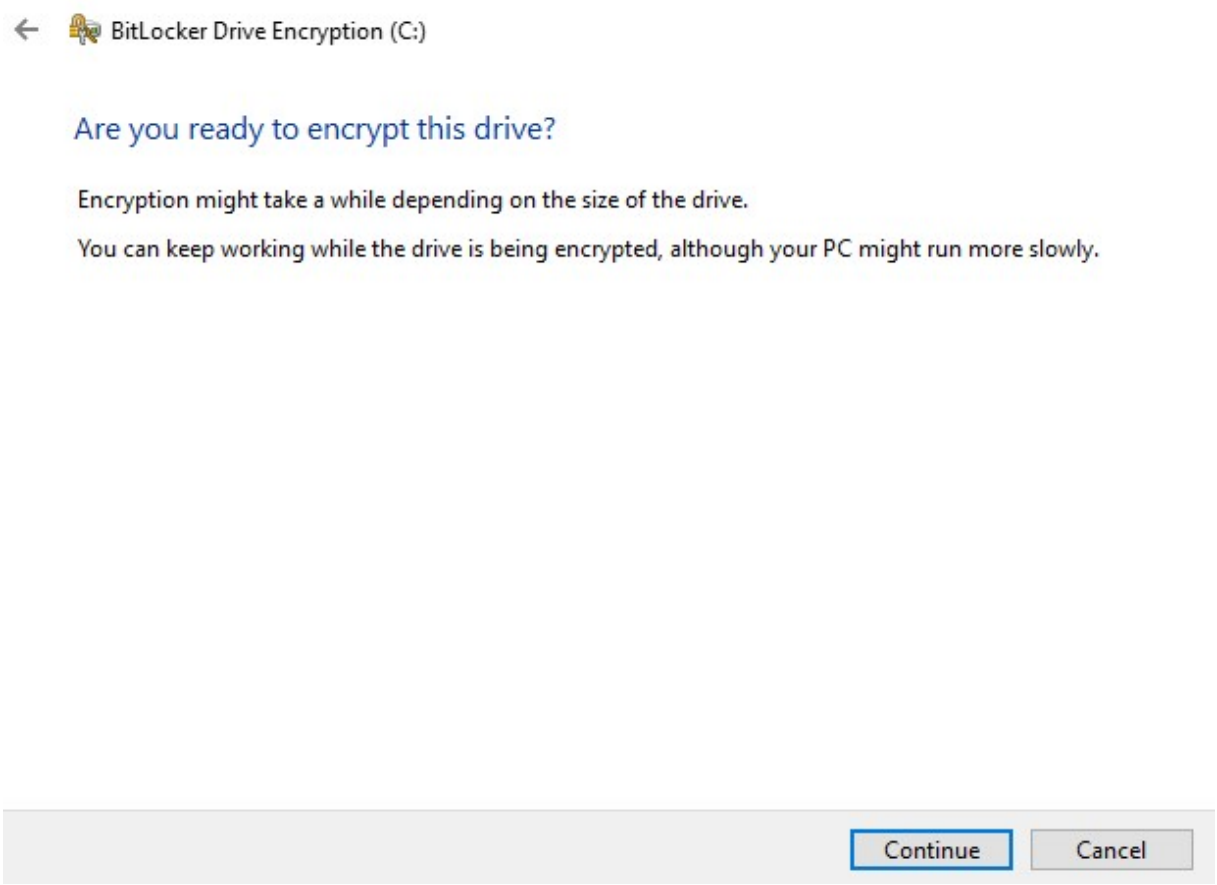


Figure 78 - Fin de la configuration de chiffrement
(Source : Auteur)

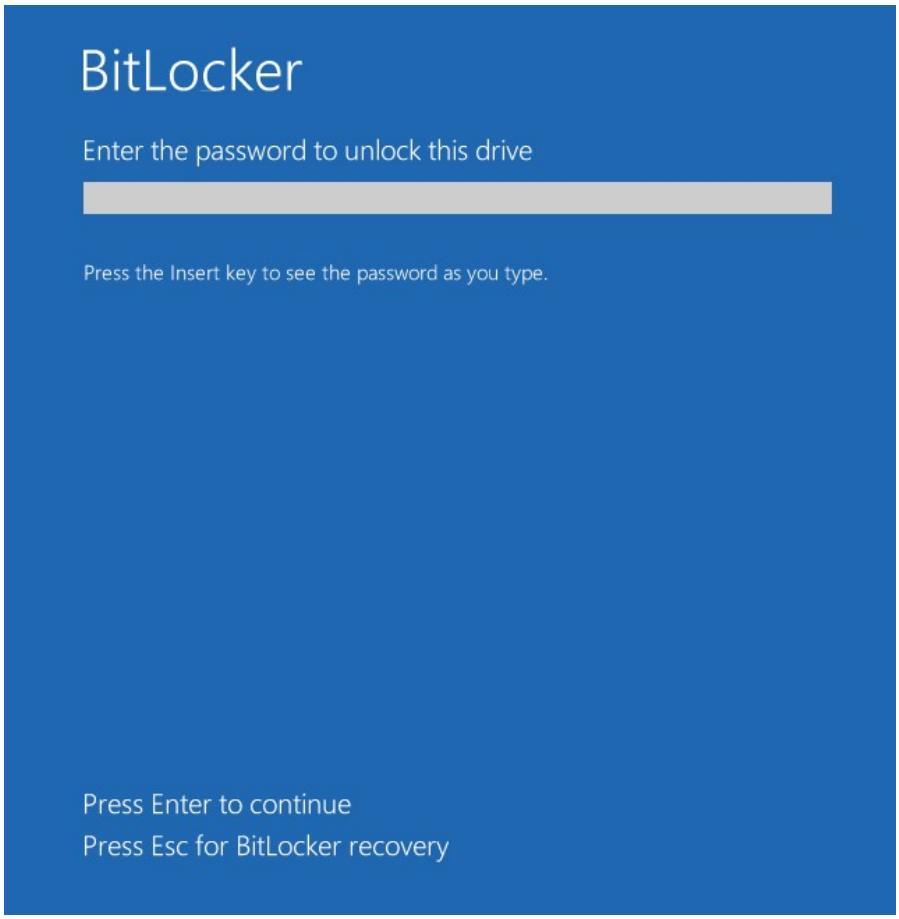


14) Attendre la fin du chiffrement des données (Le temps dépend de la taille des données à chiffrer) :

Figure 79 - Chiffrement en cours
(Source : Auteur)

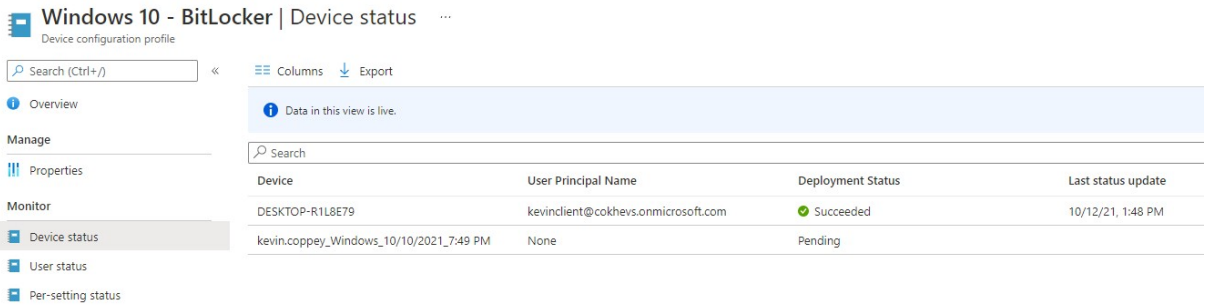
15) Lors du redémarrage, le mot de passe de BitLocker est demandé à l'utilisateur :

Figure 80 - Interface BitLocker sur le client
(Source : Auteur)



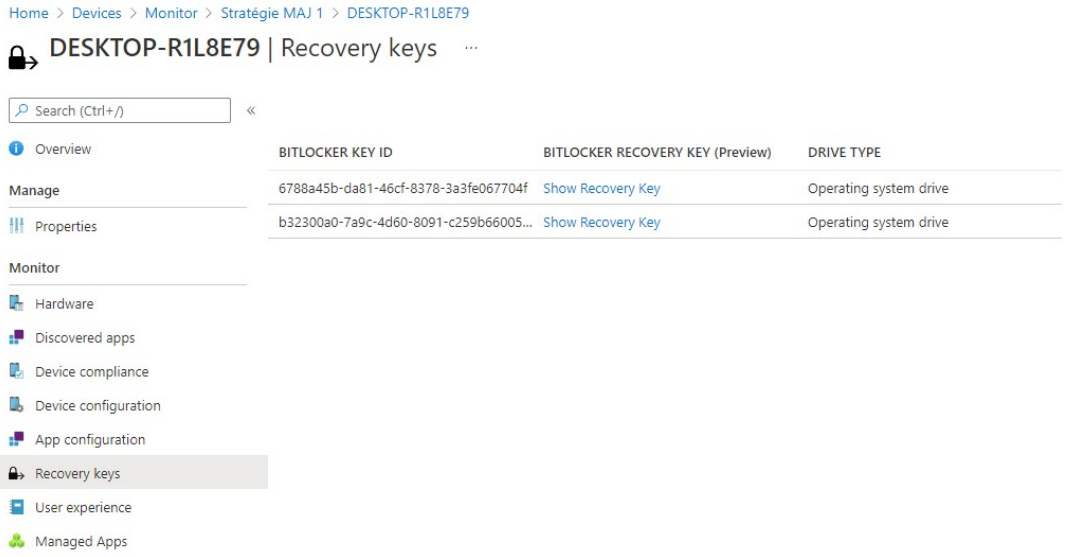
16) Contrôler que le statut de déploiement sur le portail :

Figure 81 - MEM Vérification du déploiement de la stratégie BitLocker
(Source : Auteur)



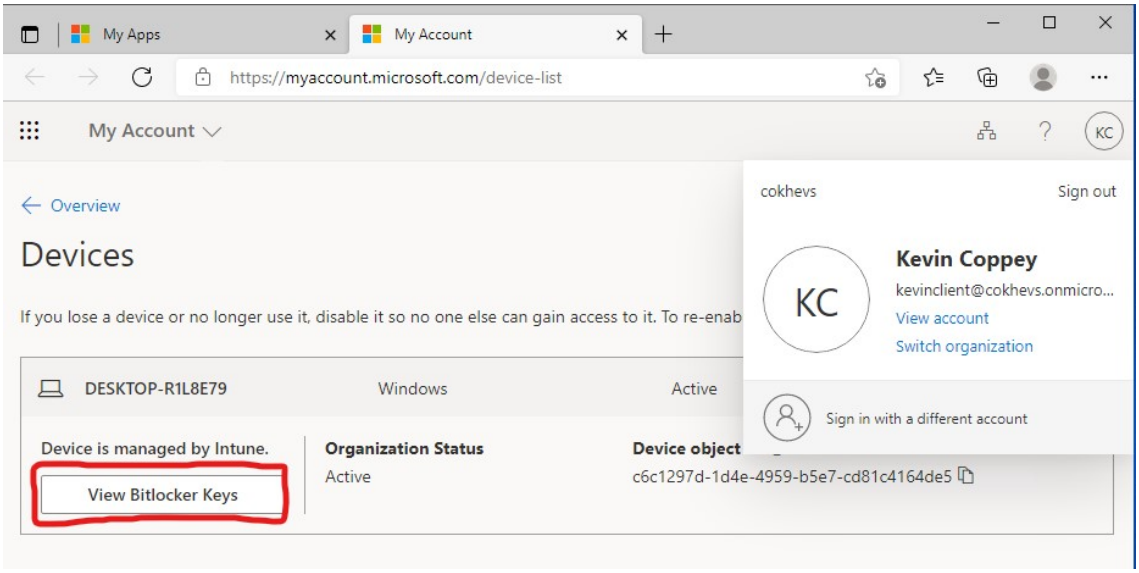
Selon la stratégie que nous avons mis en place, les clés de restauration sont disponibles sur le portail sous la rubrique « Monitor » :

Figure 82 - MEM Clé de recouvrement pour la stratégie BitLocker
(Source : Auteur)



L'utilisateur a également la possibilité de consulter sa clé de recouvrement enregistrée sur Azure en se rendant sur https://myaccount.microsoft.com/device-list :

Figure 83 - Contrôle de la clé de recouvrement par l'utilisateur du client
(Source : Auteur)



Dorénavant, l'utilisateur dispose d'un disque dur chiffré. S'il devait perdre un jour son ordinateur, ses données sont protégées contre une tentative de récupération malveillante. Cela améliore la sécurité des clients Windows.

3.1.3. Windows Defender Antivirus

Sur internet, les menaces sont légion. Il suffit de télécharger une seule fois un fichier malveillant pour corrompre tout un poste de travail. C'est dans l'optique de lutter contre ces menaces que les antivirus ont vu le jour.

Microsoft possède une solution de traitement active des menaces connue sous le nom de « Microsoft Defender ». Celle-ci est nativement disponible sur tous les ordinateurs sous les systèmes d'exploitation Windows 10 et 11. Cependant, il est possible de gérer son activation et son fonctionnement dans le Cloud grâce à l'outil « Windows Defender Antivirus ».

Une étude menée par l'organisme AV-Comparatives (2020, « Test Results » section) démontre que l'antivirus de Microsoft est efficace à 99,8% contre les attaques des malwares sur internet.

Dans une stratégie d'entreprise BYOD, il est nécessaire de garantir une protection en temps réel afin d'empêcher toutes les éventuelles menaces qu'un utilisateur puisse rencontrer en utilisant son poste de travail de manière personnelle.

Du fait de toutes ces raisons, regardons maintenant comment se passe la configuration de cet outil dans le cloud.

3.1.3.1. Informations

Ce guide est basé sur celui réalisé par Mark Dunkerley et Matt Tumbarello dans leur livre *Mastering Windows Security and Hardening* (2020, p. 334-335), qui représente les bonnes pratiques de sécurité à appliquer, et sur la documentation de Microsoft à ce sujet (2021t).

3.1.3.2. Exigences

- Une licence permettant d'utiliser Intune avec configuration du tenant (voir Annexe I).
- Une machine virtuelle ou un ordinateur physique sous Windows connecté à Internet.
- Un utilisateur préalablement crée sur le domaine « Azure Active Directory » avec sa machine enrôlée (voir Annexe II).

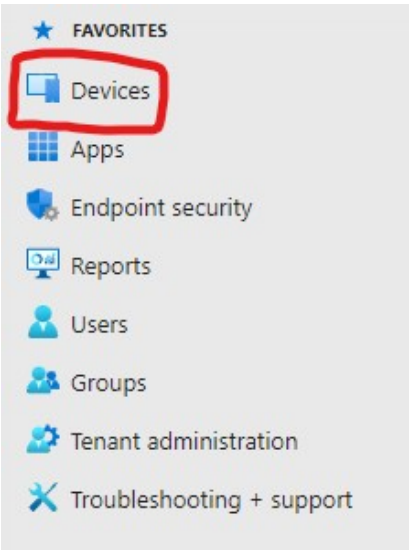
3.1.3.3. Configuration

1) Se connecter sur « Microsoft Endpoint Manager Admin Center »
   https://devicemanagement.microsoft.com

Figure 84 - MEM Accueil pour la stratégie antivirus
(Source : Auteur)

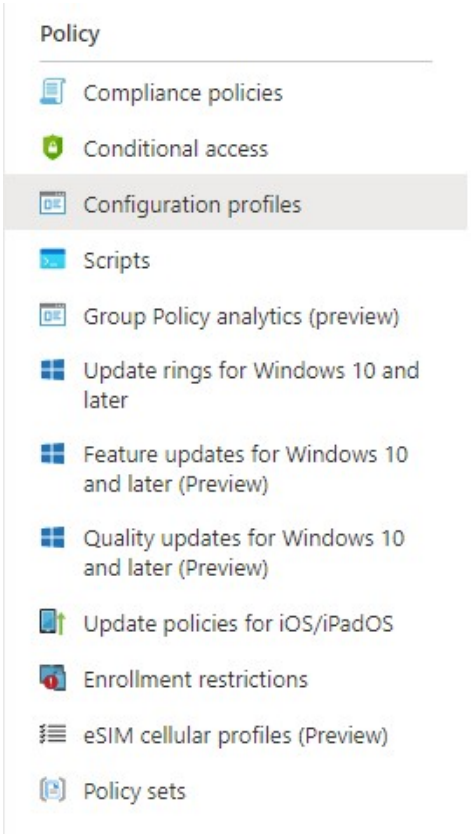
2) Dans le menu latérale droite, cliquer sur « Devices » :

Figure 85 - MEM Menu pour la stratégie antivirus
(Source : Auteur)



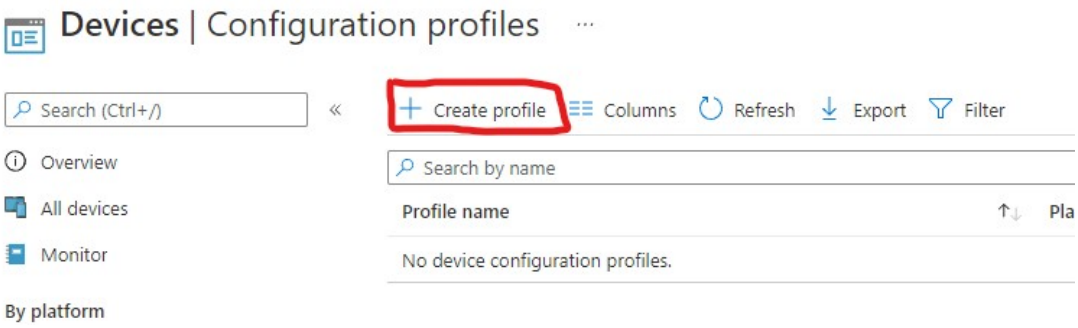
3) Sous la rubrique « Policy », cliquer sur « Configuration profiles » :

Figure 86 - MEM Profil de configuration pour la stratégie antivirus (Source : Auteur)



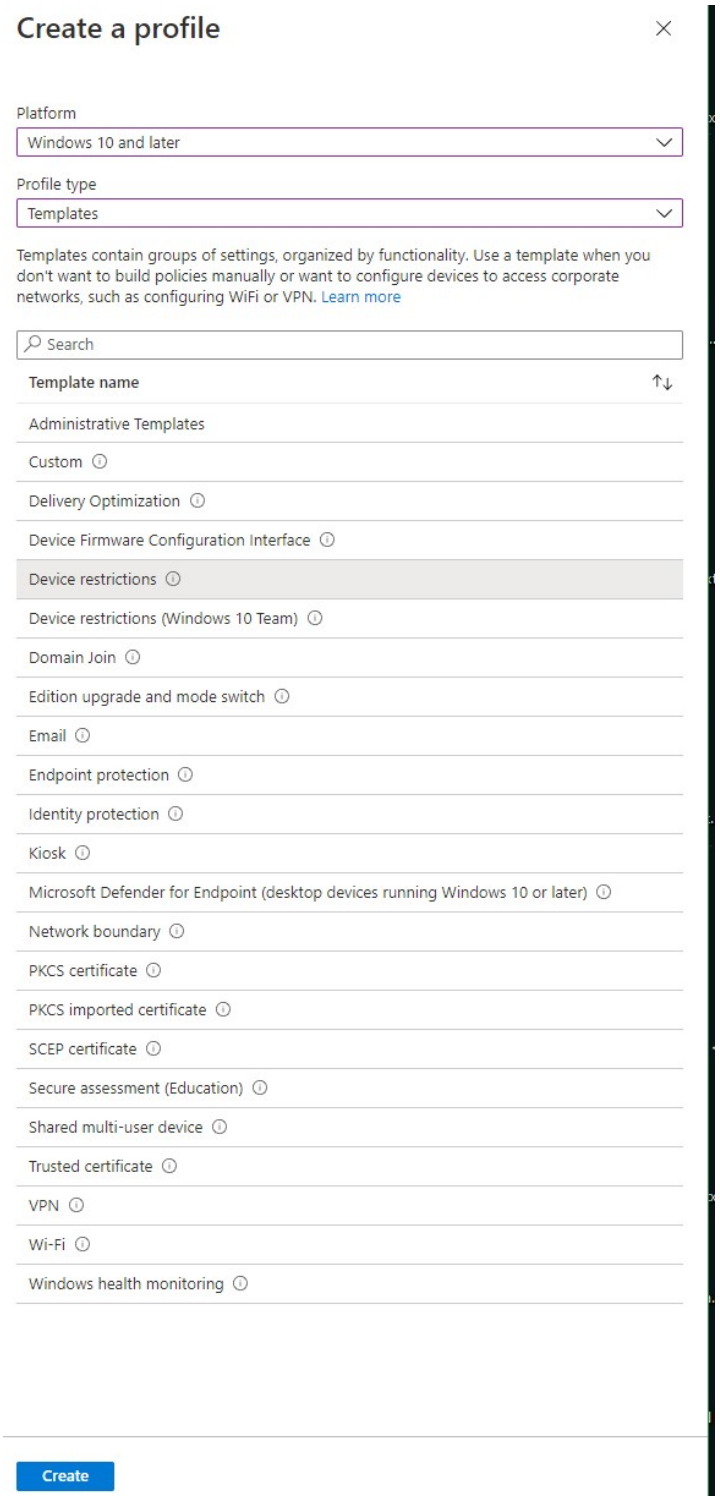
4) Cliquer ensuite sur « Create profile » dans la barre d'outils en haut de la page :

Figure 87 - MEM Création d'un nouveau profil pour la stratégie antivirus (Source : Auteur)



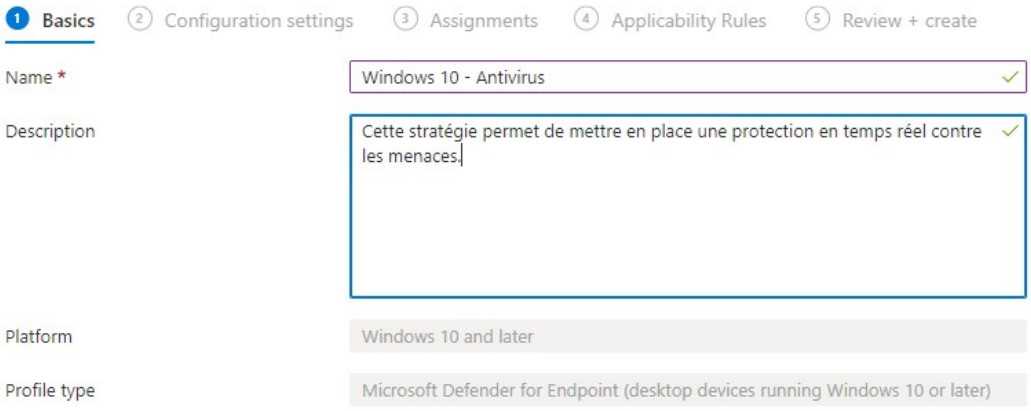
5) Remplir les informations et choisir « Device Restriction » tout comme l'image suivante, puis cliquer sur le bouton « Create » tout en bas :

Figure 88 - MEM Restriction de l'appareil pour la stratégie antivirus
(Source : Auteur)



6) Remplir selon les informations suivantes :

Figure 89 - MEM Information de base pour la stratégie antivirus
(Source : Acteur)



7) Sous la rubrique « Microsoft Defender Antivirus », remplir selon les informations suivantes et cliquer sur « Next » tout en bas de la page :

- Real-time monitoring : Permet d'activer la protection en temps réel de « Microsoft Defender Antivirus ».
- Behavior montoring : Permet de lancer un contrôle lors de comportement suspicieux.
- Network Inspection System (NIS) : En activant cette option, nous permettons de bloquer le trafic malicieux détecté via des signatures présentes dans le Network Inspection System[2].
- Scan all downloads : Si activé, l'option permet de scanner tous les fichiers téléchargés.
- Configure low CPU priority for scheduled scans : Cette option permet de lancer un scan programmé avec une priorité de processeur basse.
- Catch-up scan : Permet de configurer le « catch-up scan ». Celui-ci est un type de scan initié lorsqu'un scan programmé est manqué.

[2] Le NIS est le système de détection des malwares du trafic réseau chez Microsoft.

  - Quick-scan : Scan rapide qui couvre uniquement les zones les plus communes lors de l'infection par un malware. Par exemple, les fichiers temporaires.

  - Full-Scan : Scan qui couvre l'ensemble des fichiers du système.

- Scan scripts loaded in Microsoft web browser: Autorise « Microsoft Defender Antivirus » à scanner les scripts utilisés sur les pages internet via Edge.

- End-user access to Defender: Cette option permet de bloquer l'accès à l'utilisateur de la fenêtre « Windows Defender » dans les paramètres.

- Security intelligence update interval (in hours) : Permet d'entrer un intervalle autorisant l'antivirus à lancer une analyse des signatures des fichiers.

- Monitor file and program activity: Permet à l'antivirus de gérer l'activité des fichiers et des programmes sur l'appareil de l'utilisateur.

- Days before deleting quarantined malware: Ce paramètre permet de configurer le nombre de jours avant la suppression d'un malware mis en quarantaine.

- CPU usage limit during a scan: Permet de limiter l'utilisation du processeur lors d'un scan.

- Scan archive file: Permet d'autoriser le scan des fichiers archivés. Par exemple les fichiers en .rar ou .zip.

- Scan incoming mail messages: Laisse l'antivirus scanner les courriers électroniques lorsqu'ils arrivent sur la machine.

- Scan removable drives during a full scan: Permet de scanner également les disques amovibles lors d'un scan complet.

- Scan mapped network drives during a full scan: Permet de scanner également les disques réseaux lors d'un scan complet.

- Scan files opened from network folders: Permet de scanner les fichiers ouverts depuis un dossier partagé dans le réseau.

- Cloud delivered protection: Permet d'activer le service « Microsoft Active Protection Service » afin de recevoir des notifications sur le portail de gestion lorsque des appareils sont infectés.

- File Blocking Level: Cette option est utilisée lorsque l'administrateur souhaite configurer le niveau de détection des fichiers infectés de la protection Cloud. En donnant une forte détection, il est possible que des fichiers sains soient considérés comme étant malveillants.

- Time extension for file scanning by the cloud: Permet de spécifier le temps de blocage maximal d'un fichier que l'antivirus met pour avoir un résultat sur le cloud.

- Prompt users before sample submission: En activant cette option, l'utilisateur est averti de l'envoi d'un échantillon sur le cloud.

- Time to perform a daily quick scan: Permet de choisir l'heure à laquelle un scan rapide va être lancé dans la journée.

- Type of system scan to perform: Permet de choisir si le scan journalier sera rapide ou complet.

- Detect potentially unwanted applications: Permet d'empêcher l'utilisateur d'installer des applications qui sont considérées comme étant indésirables.

- Actions on detected malware threats: Permet de définir quelles actions sont entreprises lorsqu'un malware est détecté. Il est possible de configurer ces actions selon le niveau de sévérité de l'alerte.

Figure 90 - MEM Paramètres de Microsoft Defender Antivirus 1

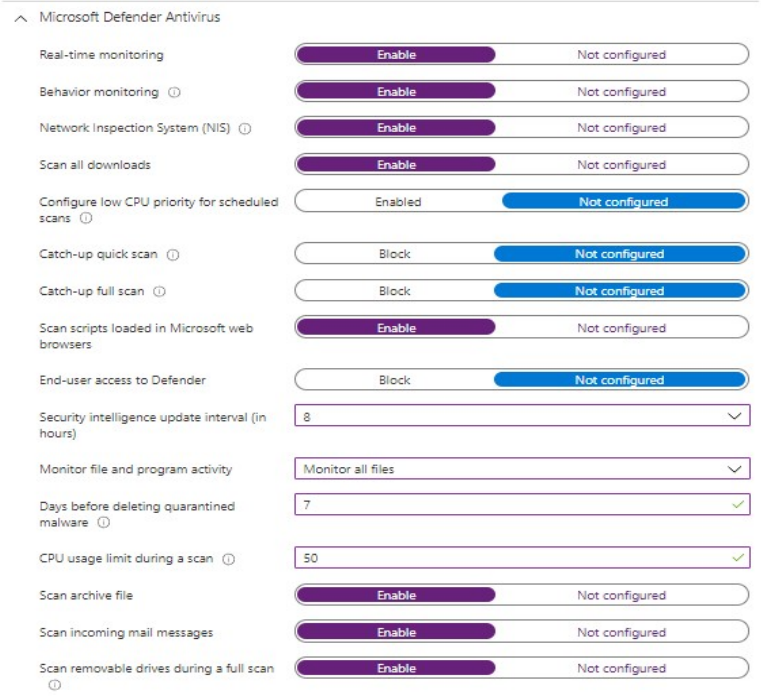
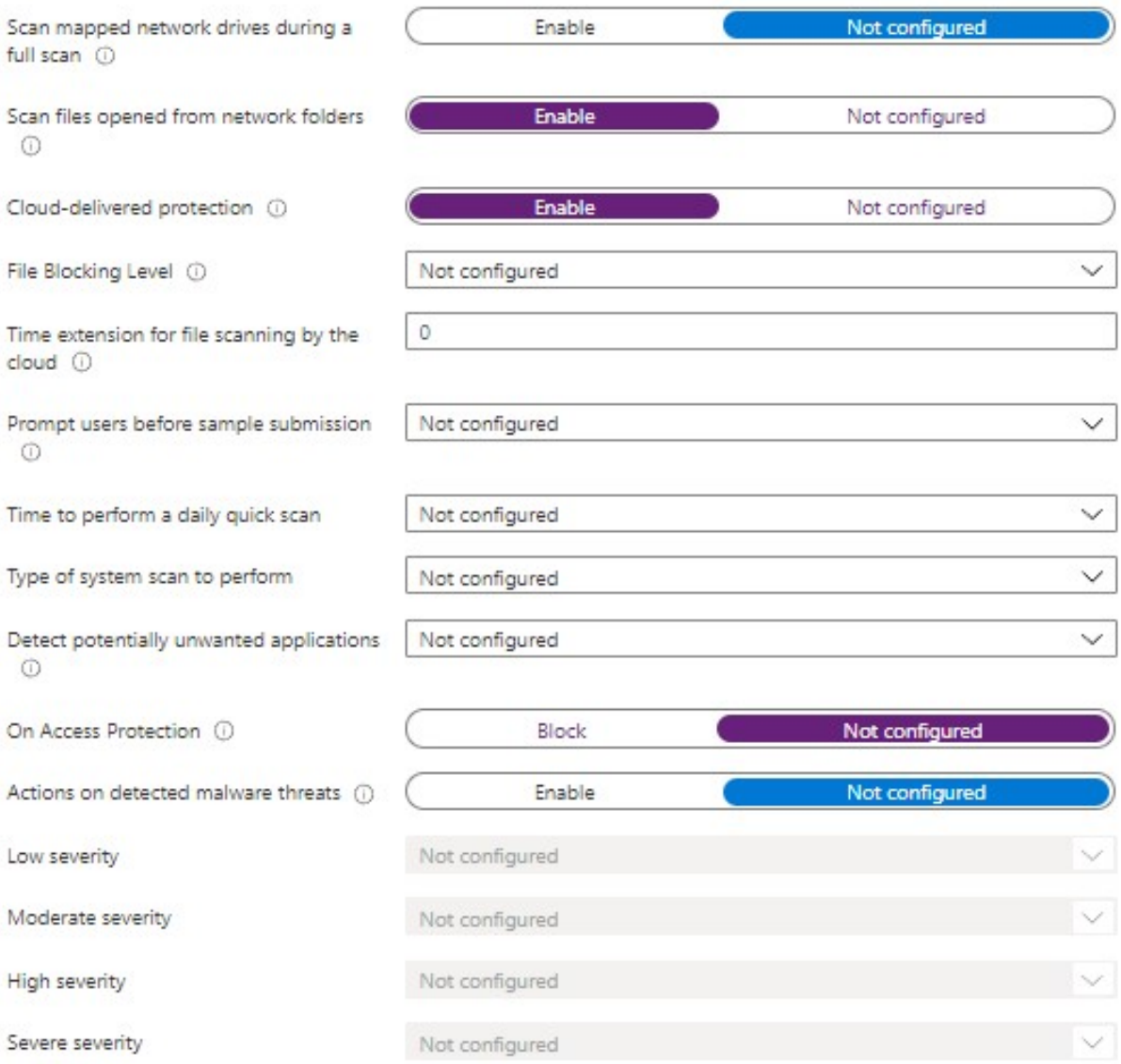
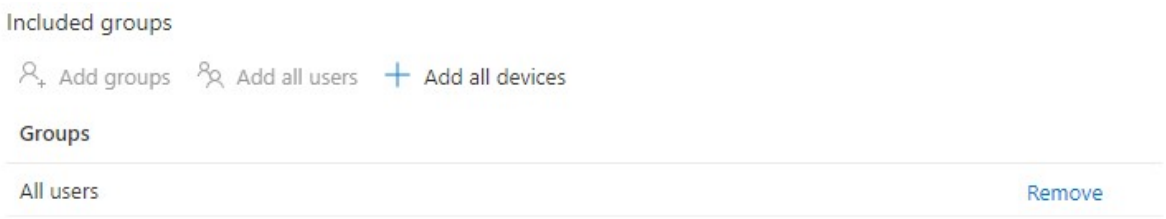


Figure 91 - MEM Paramètres de Microsoft Defender Antivirus 2
(Source : Auteur)



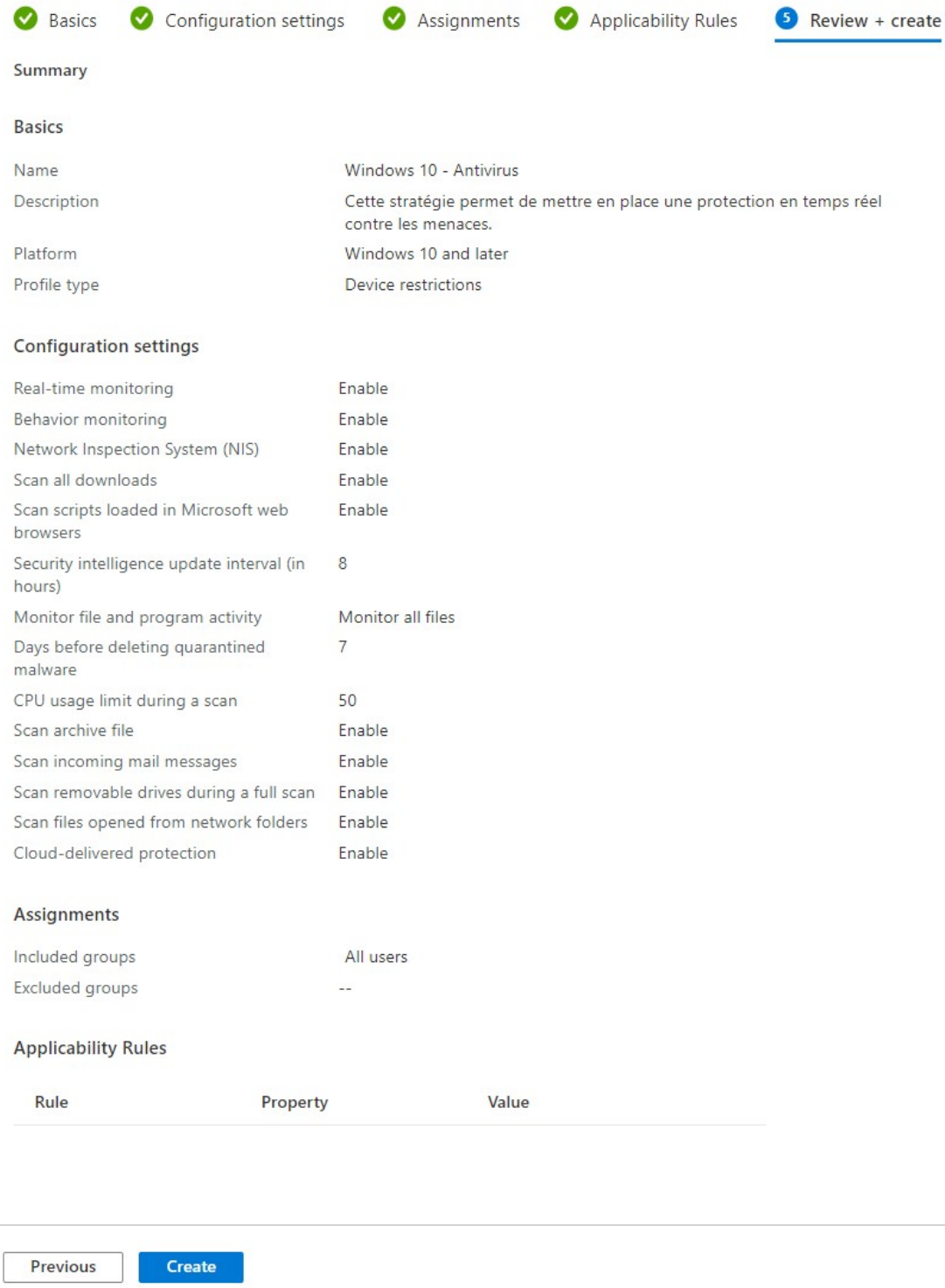
8) Sur la page suivante, cliquer sur « Add all users » :

Figure 92 - MEM Portée ajoutée pour la stratégie antivirus
(Source : Auteur)



9) Contrôler les informations de la stratégie et cliquer sur « Create » tout en bas de la page :

Figure 93 - Confirmation de la stratégie antivirus
(Source : Auteur)



10) Vérifier que la stratégie a bien été mise en place :

Figure 94 - MEM Notification de la stratégie antivirus
(Source : Auteur)

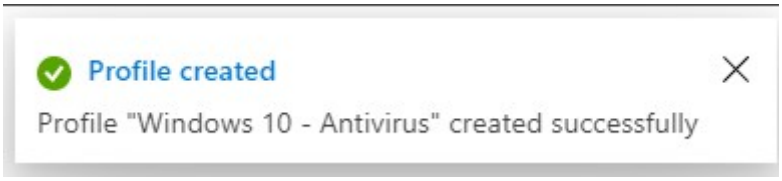


Figure 95 - MEM Vérification de la stratégie antivirus
(Source : Auteur)

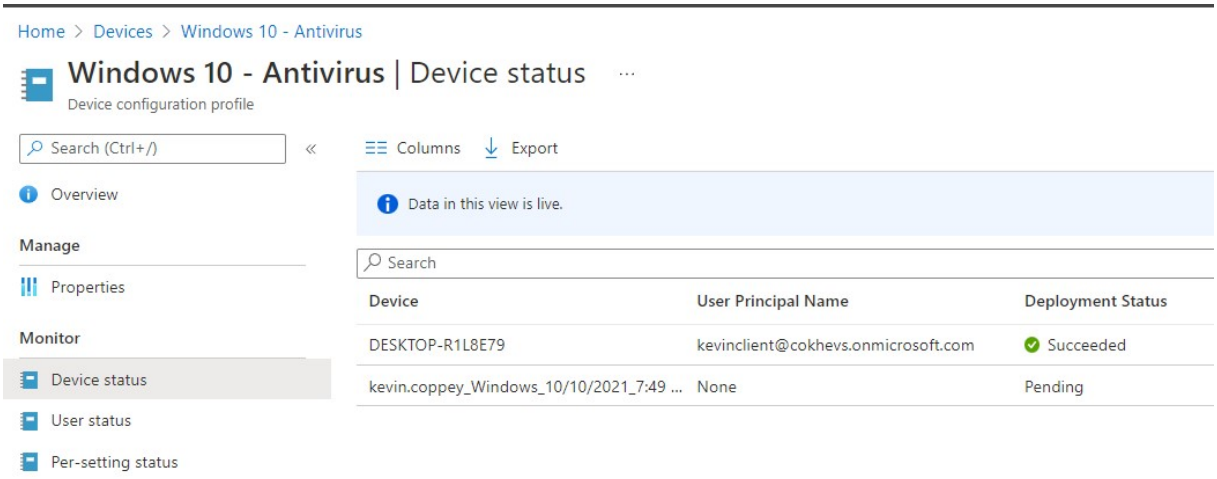
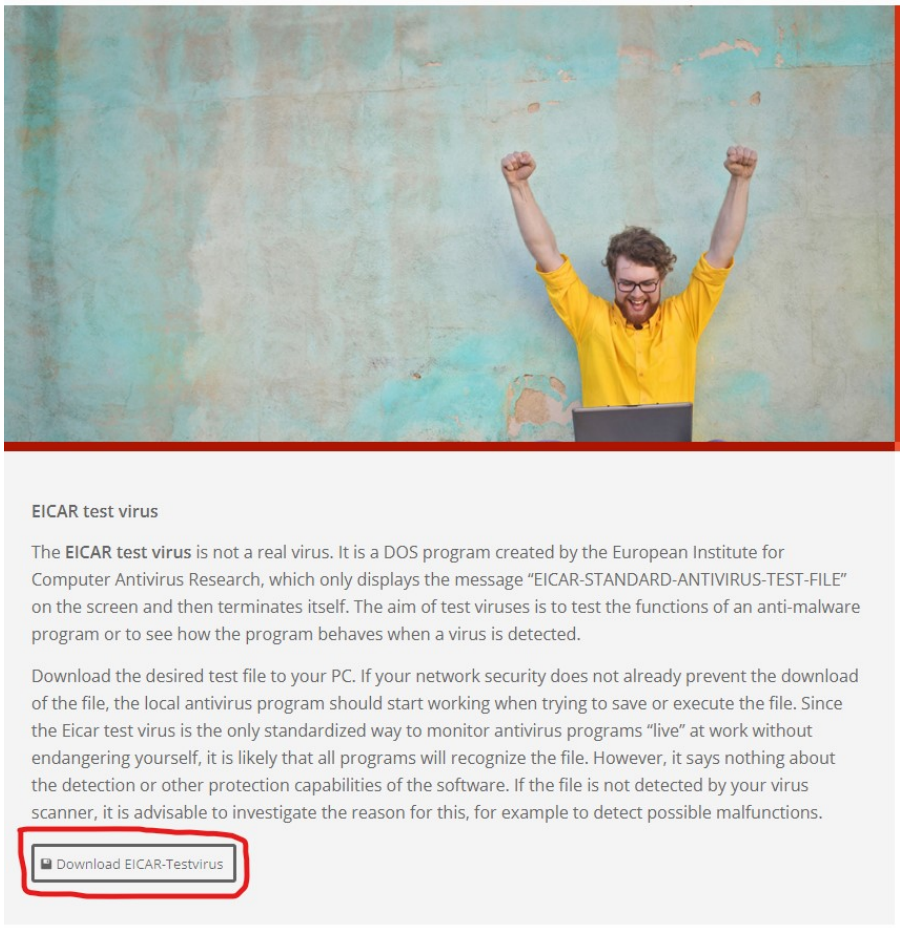


Figure 96 - Vérification sur le client de la stratégie antivirus
(Source : Auteur)

Testons maintenant notre stratégie d'antivirus sur le client Windows. Il existe un « virus » gratuit qui permet de tester l'efficacité de sa protection informatique.

11) Se rendre sur https://www.ikarussecurity.com/en/private-customers/download-test-viruses/

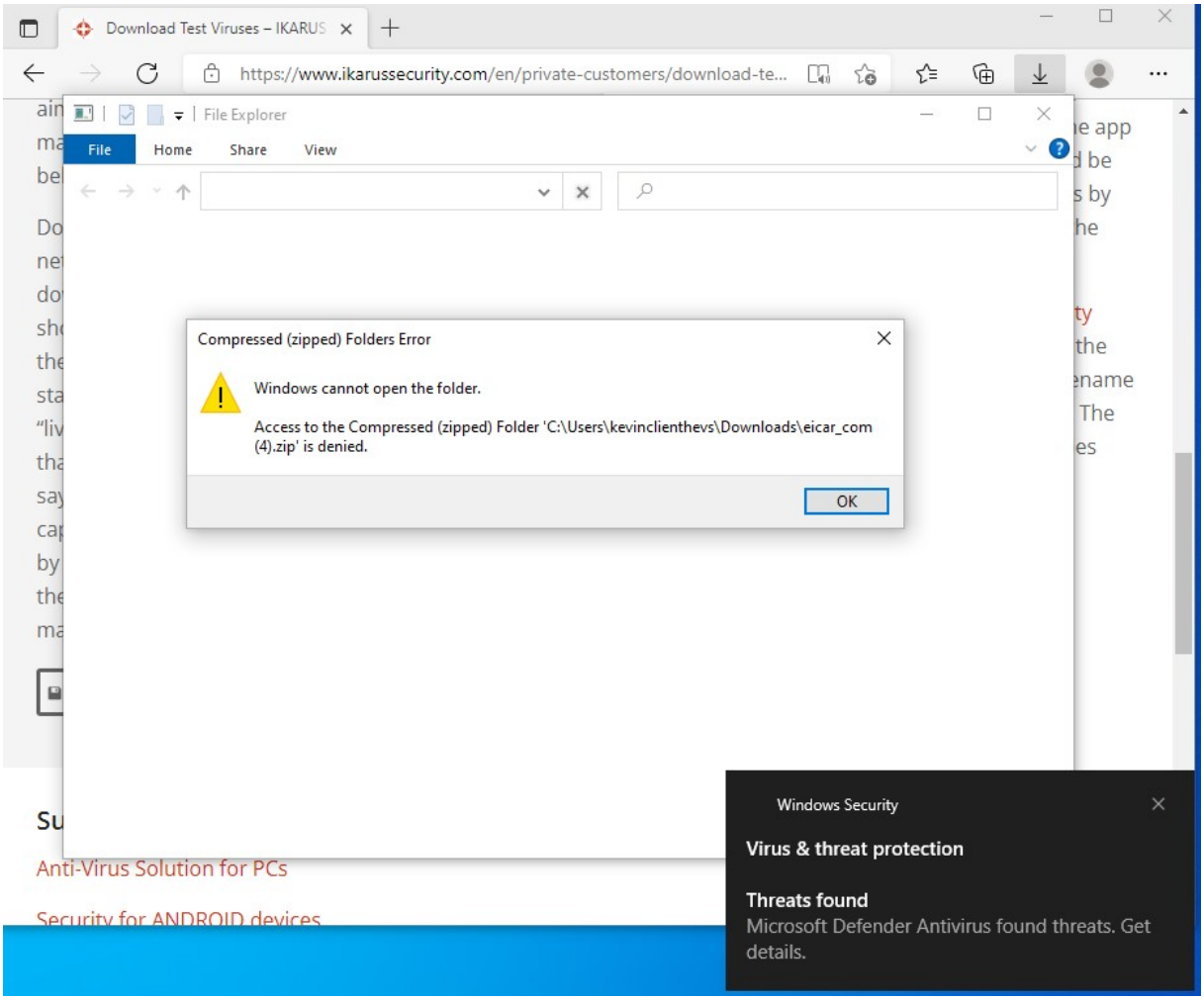
Figure 97 - Page de téléchargement du "virus"
(Source : Auteur)



12) Télécharger le « virus ».

13) Ouvrir le .zip :

Figure 98 - Test sur le client de la détection du "virus"
(Source : Auteur)



Nous remarquons bel et bien que l'antivirus a détecté la menace. La stratégie pour défendre un point de terminaison contre des menaces via une protection en temps réel est un succès.

3.1.4. Windows Hello for Business

Comme pour sa version tout public, « Windows Hello for Business » permet de remplacer le combo traditionnel de l'identifiant avec un mot de passe. Ce choix s'inscrit dans la stratégie de Microsoft de s'affranchir des mots de passe qui comportent plusieurs désavantages. Ceux-ci peuvent même engranger des problèmes de sécurité.

En effet, il est souvent compliqué pour les utilisateurs de se souvenir de leur mot de passe à travers tous les services qu'ils utilisent sans un gestionnaire, souvent payant.

De plus, beaucoup d'utilisateurs se limitent souvent à un seul mot de passe pour l'entièreté de leurs comptes. Il suffit de connaître un seul mot de passe et tous les comptes peuvent être perdus.

Pour se rendre compte de l'échec des mots de passe, voici plusieurs statistiques réalisées aux Etats-Unis (Poll & Google, 2019) :

- 24% de la population ont déjà utilisé un mot de passe tel que « password », « qwerty » ou encore « 123456 ».
- 66% d'américains avouent utiliser le même mot de passe pour plusieurs comptes.
- 43% ont déjà communiqué leur mot de passe.

Ainsi, Microsoft propose à ses clients d'utiliser sa solution « Windows Hello for Business ». Celle-ci est liée à un appareil et permet de s'authentifier de deux manières différentes :

- L'authentification biométrique (Reconnaissance faciale et digitale).
- Le code PIN (numérique ou alphanumérique).

De plus, la version business rajoute une couche de sécurité au système en chiffrant l'authentification via un certificat ou une clé cryptographique. Cela rend cette solution plus sécurisée (Microsoft, 2021l).

Nous développons maintenant un guide pour intégrer le service « Windows Hello for Business » dans une stratégie de sécurité utilisant le Cloud.

3.1.4.1. Informations

Ce guide est basé sur celui réalisé par Mark Dunkerley et Matt Tumbarello dans leur livre *Mastering Windows Security and Hardening* (2020, p. 328-330), qui représente les bonnes pratiques de sécurité à appliquer, et sur la documentation de Microsoft à ce sujet (2021l).

3.1.4.2. Exigences

- Une licence permettant d'utiliser Intune avec configuration du tenant (voir Annexe I).
- Une machine virtuelle ou un ordinateur physique sous Windows connecté à Internet.
- Un utilisateur préalablement crée sur le domaine « Azure Active Directory » avec sa machine enrôlée (voir Annexe II).

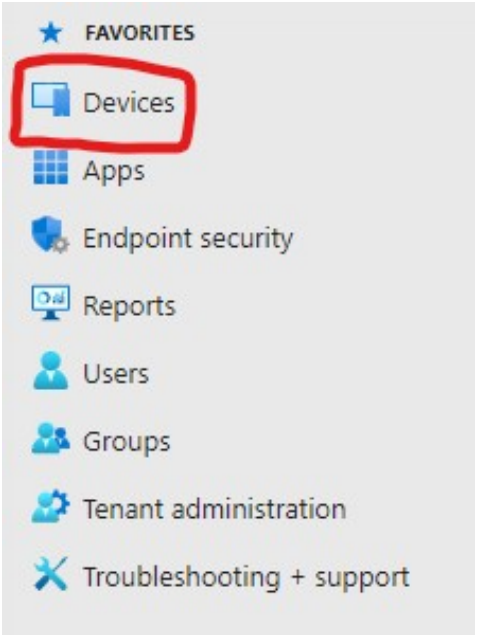
3.1.4.3. Configuration

1) Se connecter sur « Microsoft Endpoint Manager Admin Center » https://devicemanagement.microsoft.com

Figure 99 - MEM Accueil pour la stratégie Windows Hello
(Source : Auteur)

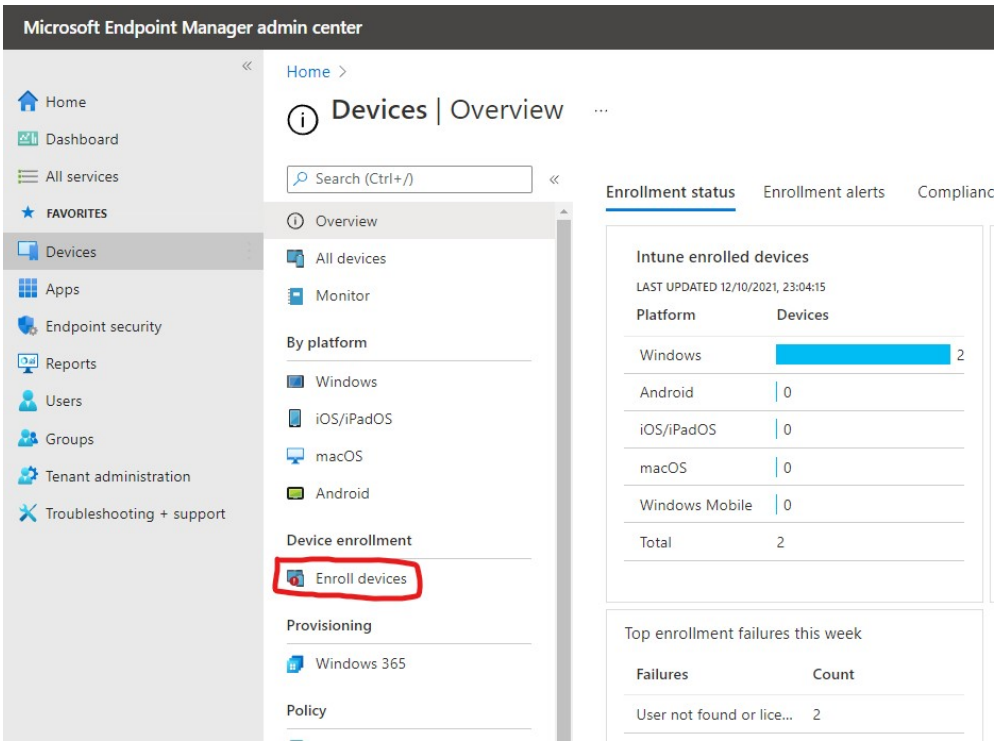
2) Dans le menu latéral droite, cliquer sur « Devices » :

Figure 100 - MEM Rubrique appareil pour la stratégie Windows Hello (Source : Auteur)



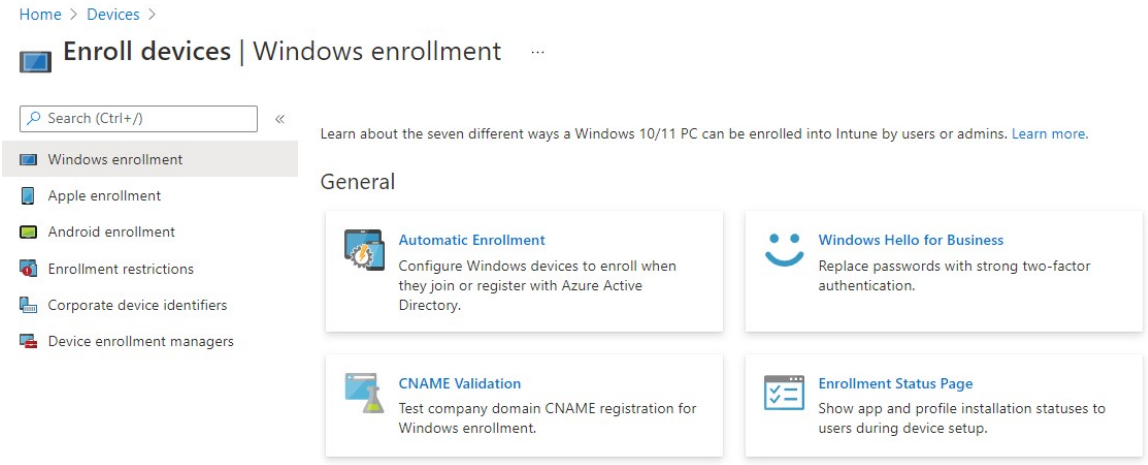
3) Sous la rubrique « Device enrollment », cliquer sur « Enroll devices » :

Figure 101 - MEM Rubrique enrôlement pour la stratégie Windows Hello (Source : Auteur)



4) Cliquer ensuite sur « Windows Hello for Business” :

Figure 102 - MEM Méthode d'enrôlement pour la stratégie Windows Hello (Source : Auteur)

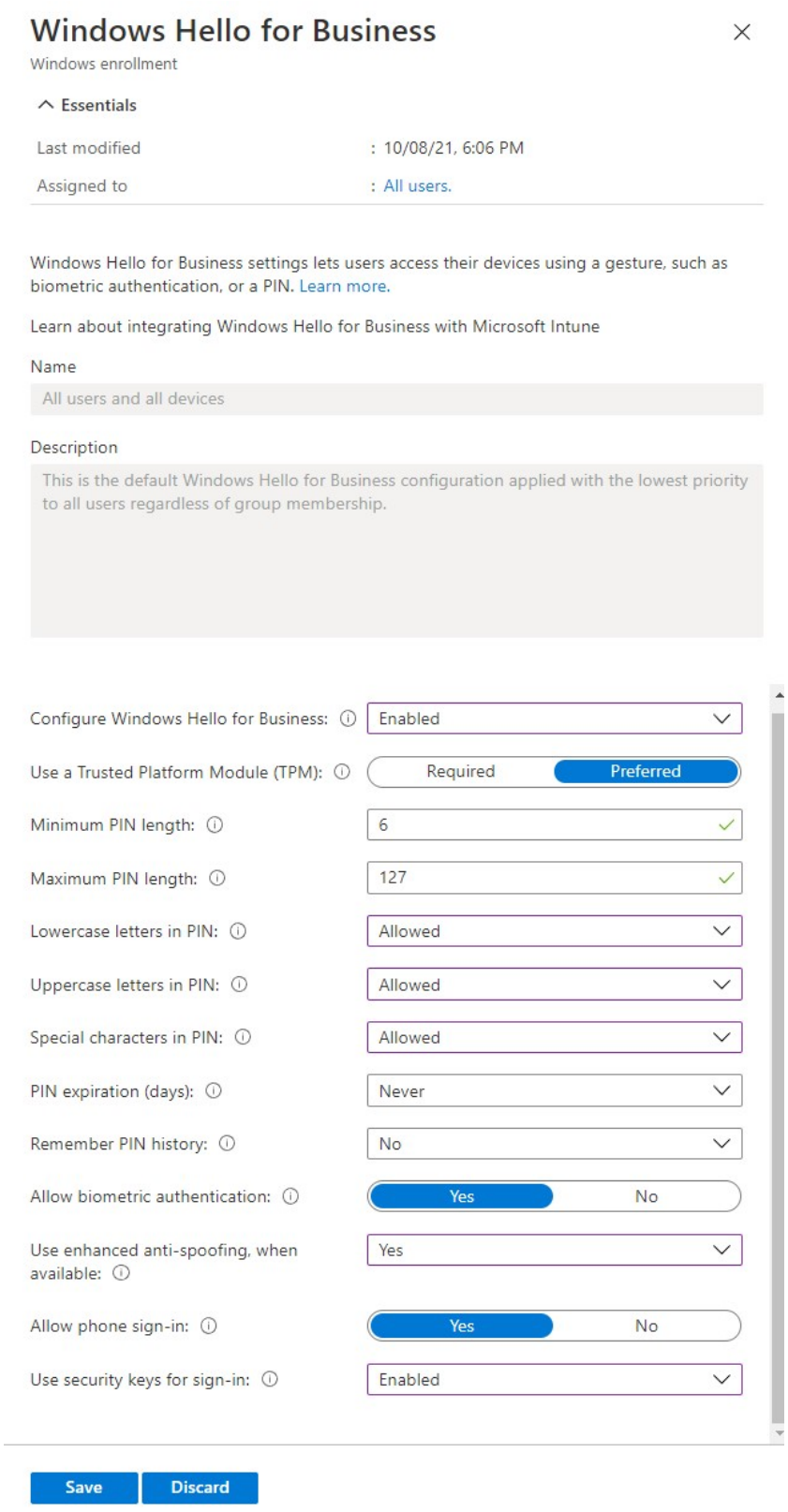


5) Dans le menu qui apparaît à droite, remplir selon les informations suivantes, puis cliquer sur « Save » en bas de l’écran :

- Use a Trusted Platform Module (TPM) : Cette option permet de laisser la provision du compte à la puce TPM si elle est présente.
- Minimum PIN length : Permet de déterminer une longueur minimale au PIN de l’utilisateur.
- Maximum PIN length : Permet de déterminer une longueur maximale au PIN de l’utilisateur.
- Lowercase letters in PIN : Permet à l’utilisateur d’utiliser des lettres minuscules dans le PIN.
- Uppercase letters in PIN : Permet à l’utilisateur d’utiliser des lettres majuscules dans le PIN.
- Special characters in PIN : Autorise l’utilisateur d’utiliser des caractères spéciaux dans le PIN.
- PIN expiration (days) : En activant cette option, le PIN peut s’expirer selon un nombre de jours.
- Remember PIN history : Si cette option est activée, l’utilisateur ne peut pas réutiliser un précédent PIN.

- Allow biometric authentication : Ce paramètre autorise ou non l'authentification biométrique.
- Use enhanced anti-spoofing, when available : Activer cette option permet à l'algorithme de Microsoft de ne pas accepter les photos pour s'authentifier.
- Allow phone sign-in : Permet l'utilisation de l'authentification à deux facteurs en utilisant un téléphone afin de vérifier l'identité de l'utilisateur s'il est inscrit sur « Azure Active Directory ».
- Use security keys for sign-in : Permet à l'administrateur de supprimer à distance l'authentification via clé usb.

Figure 103 - MEM Paramètres Windows Hello
(Source : Auteur)

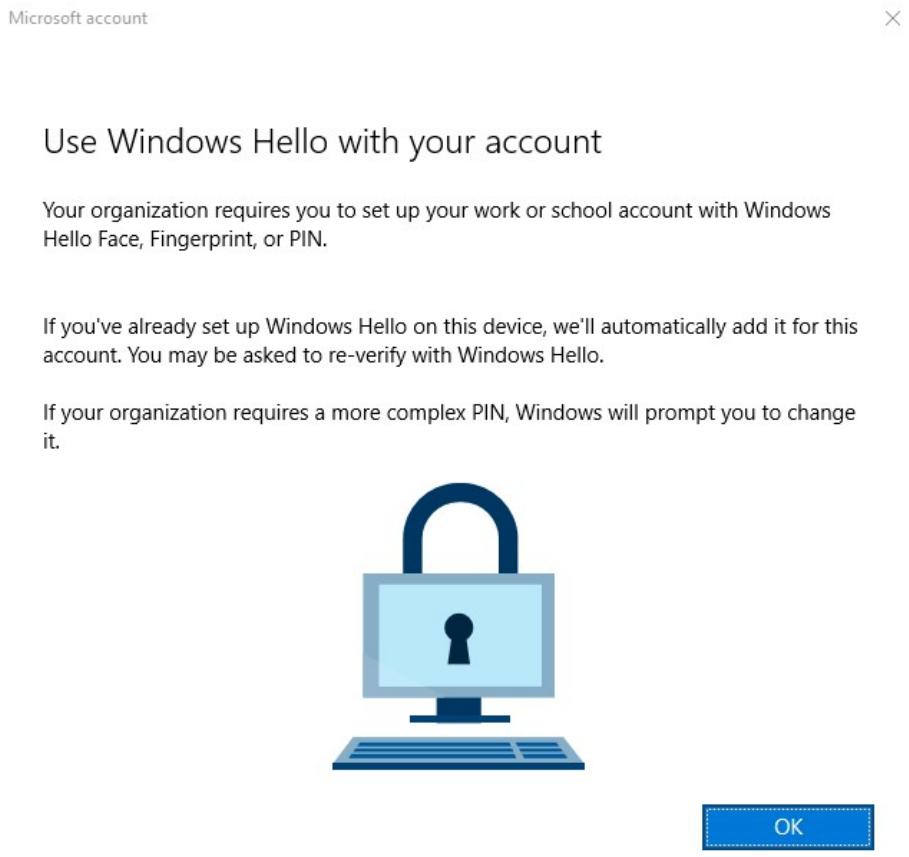


6) Vérifier que la notification est apparue :

Figure 104 - MEM Notification pour la stratégie Windows Hello (Source : Auteur)

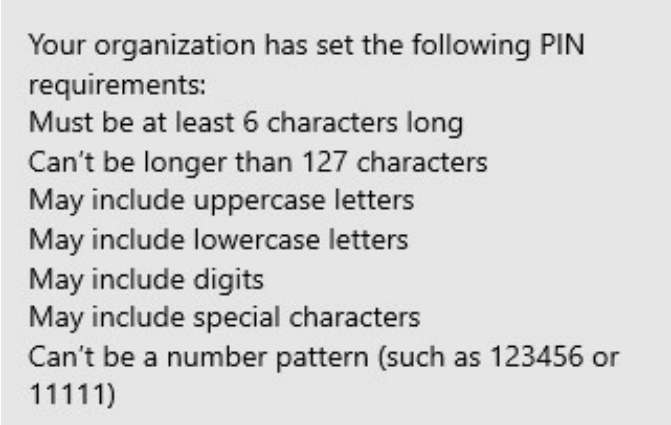
7) Se rendre sur le client Windows, un message apparaît pour nous expliquer que l'organisation requiert l'utilisation de « Windows Hello ». Cliquer sur OK :

Figure 105 - Début de configuration sur le client de la stratégie Windows Hello (Source : Auteur)



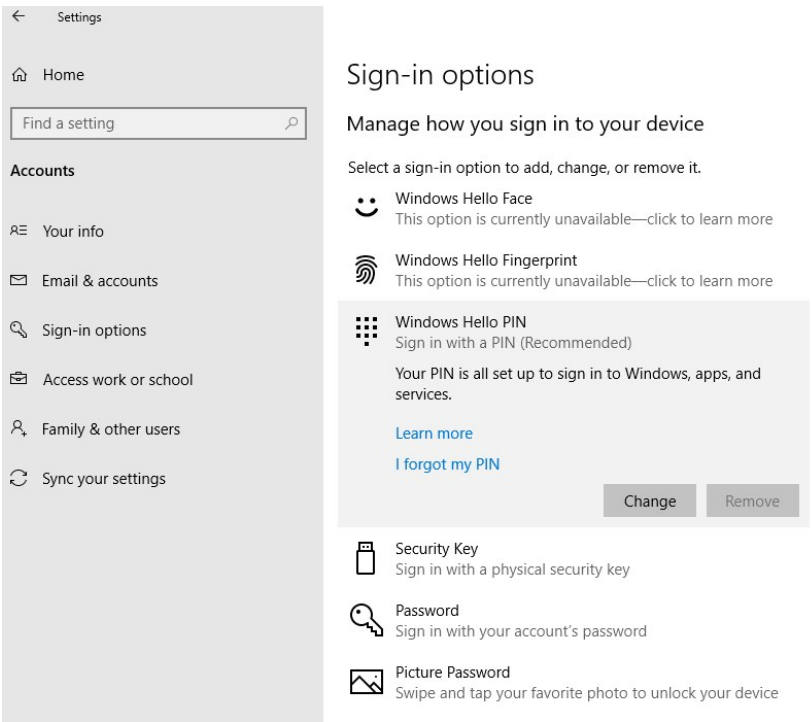
8) Dans les exigences, nous pouvons voir les paramètres que nous avons spécifiés dans la stratégie :

Figure 106 - Exigences sur le client de la stratégie Windows Hello
(Source : Auteur)



L'utilisateur a toujours la possibilité de changer son moyen d'authentification dans les paramètres de connexion de Windows :

Figure 107 - Options de connexion Windows Hello sur le client
(Source : Auteur)



La configuration est terminée, nous possédons maintenant un appareil plus sécurisé grâce à la fonctionnalité « Windows Hello for Business ».

3.1.5. Microsoft Defender SmartScreen

Lorsque nous utilisons internet, nous sommes confrontés à des menaces de toutes sortes. Le phishing, le téléchargement de fichiers malveillants ou encore les scripts malicieux se cachant dans des pages internet sont des pratiques communes faites par des personnes mal intentionnées pour dérober des informations ou simplement corrompre le système de l'utilisateur.

Selon une étude de l'antivirus Kaspersky (2020, "Figures of the year" section), l'organisme a identifié plus de 33'000 objets malveillants et plus de 173 millions d'URL considérées comme dangereuses sur le Web. En outre, 10,18% des ordinateurs ont connu une attaque ayant comme source la visite d'une page internet.

Par conséquent, Microsoft propose désormais une solution pour lutter contre les menaces présentes sur le Web qui peuvent menacer la sécurité des clients Windows.

Cette solution se nomme « Microsoft Defender Smart Screen ». Elle permet de protéger l'utilisateur via son navigateur « Microsoft Edge » de trois manières différentes (Microsoft, 2021g) :

- Une analyse des pages est effectuée avant leur visite. Si la recherche résulte sur des potentielles caractéristiques suspectes, l'outil va afficher une page d'avertissement qui notifie l'utilisateur sur le danger de la page qu'il tente d'accéder.

- Microsoft dispose d'une base de données de sites dangereux. Lorsque l'utilisateur souhaite ouvrir une page, « SmartScreen » va comparer le site souhaité avec la liste de Microsoft. Si une corrélation est trouvée, une notification apparaît pour signaler à l'utilisateur que cette page est potentiellement dangereuse.

- Toujours avec une base de données, Microsoft compare les fichiers téléchargés par l'utilisateur avec celle-ci. Si une correspondance est trouvée, le téléchargement est bloqué.

« Microsoft Defender SmartScreen » peut être déployé avec une stratégie sur le Cloud via Intune. Ainsi, nous développons ci-dessous la configuration de l'outil pour protéger les points de terminaison.

3.1.5.1. Informations

Ce guide est basé sur celui réalisé par Mark Dunkerley et Matt Tumbarello dans leur livre *Mastering Windows Security and Hardening* (2020, p. 336-337), qui représente les bonnes pratiques de sécurité à appliquer, et sur la documentation de Microsoft à ce sujet (2021g).

3.1.5.2. Exigences

- Une licence permettant d'utiliser Intune avec configuration du tenant (voir Annexe I).
- Une machine virtuelle ou un ordinateur physique sous Windows connecté à Internet.
- Un utilisateur préalablement créer sur le domaine « Azure Active Directory » avec sa machine enrôlée (voir Annexe II).

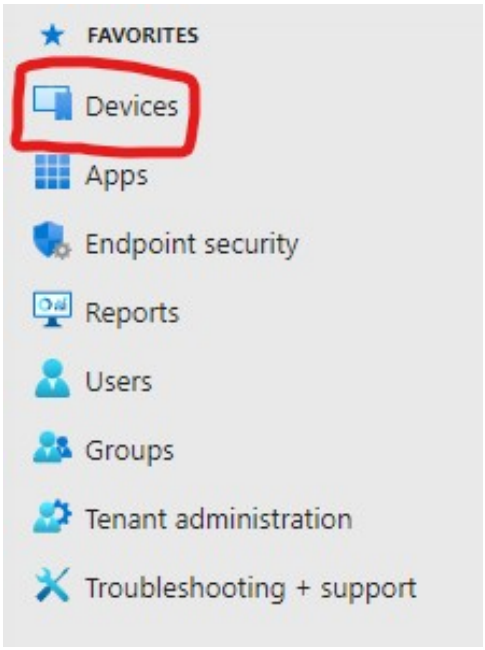
3.1.5.3. Configuration

1) Se connecter sur « Microsoft Endpoint Manager Admin Center » https://devicemanagement.microsoft.com

Figure 108 - MEM Accueil pour la stratégie SmartScreen
(Source : Auteur)

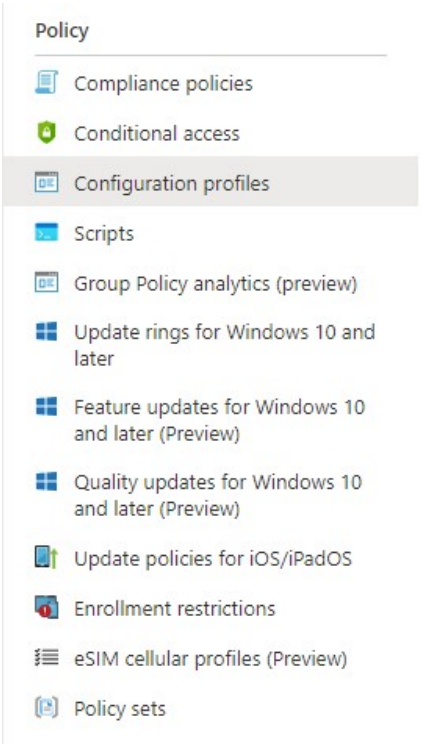
2) Dans le menu latérale droite, cliquer sur « Devices » :

Figure 109 - MEM Rubrique appareil pour la stratégie SmartScreen (Source : Auteur)



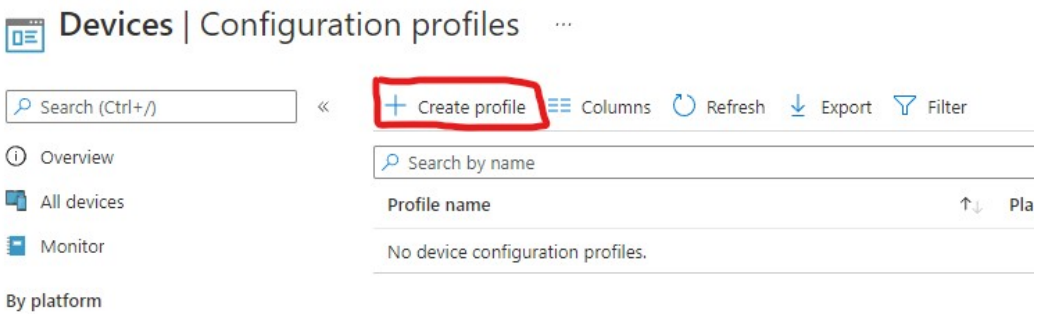
3) Sous la rubrique « Policy », cliquer sur « Configuration profiles » :

Figure 110 - MEM Configuration de profil pour la stratégie SmartScreen (Source : Auteur)



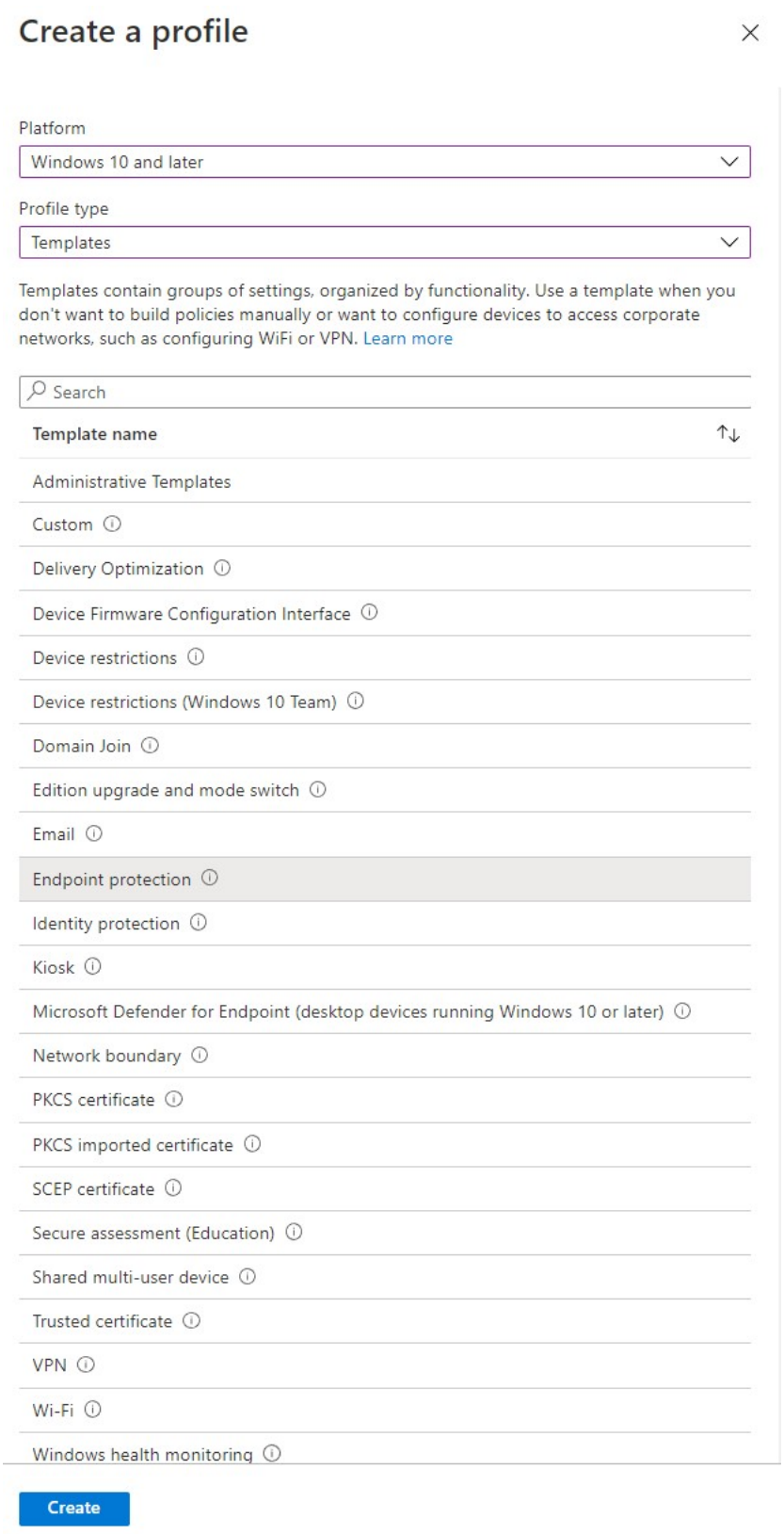
4) Cliquer ensuite sur « Create profile » dans la barre d'outils en haut de la page :

Figure 111 - MEM Création de profile pour la stratégie SmartScreen
(Source : Auteur)



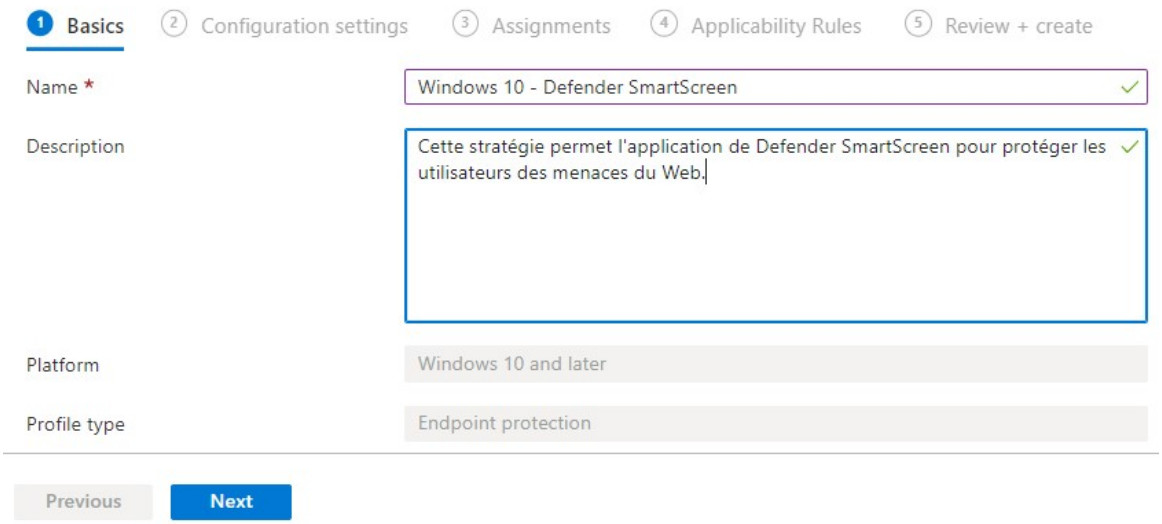
5) Remplir selon les informations suivantes, puis cliquer sur « Create » en bas de la page :

Figure 112 - MEM Protection du client pour la stratégie SmartScreen (Source : Auteur)



6) Remplir selon les informations suivantes et cliquer sur « Next » en bas de la page :

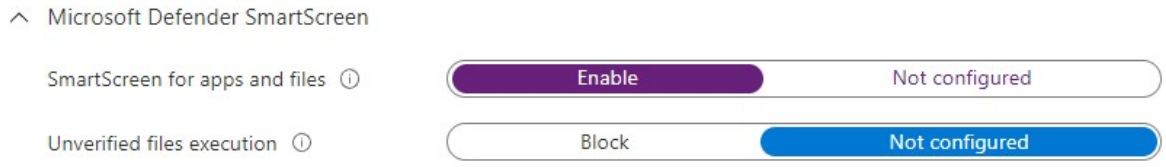
Figure 113 - MEM Information de base pour la stratégie SmartScreen 1
(Source : Auteur)



7) Remplir selon les informations de configuration suivantes, puis cliquer sur « Next » :

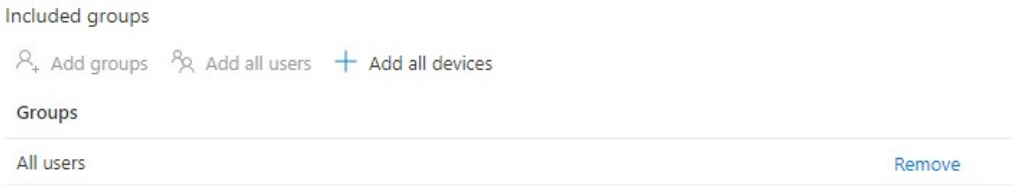
- SmartScreen for apps and files : Permet d'activer le service.
- Unverified files execution : Bloquer cette option implique que l'utilisateur ne puisse pas exécuter des fichiers qui ne sont pas vérifiés.

Figure 114 - Paramètres pour la stratégie SmartScreen 1
(Source : Auteur)



8) Sélectionner tous les utilisateurs dans la partie « Assignments » :

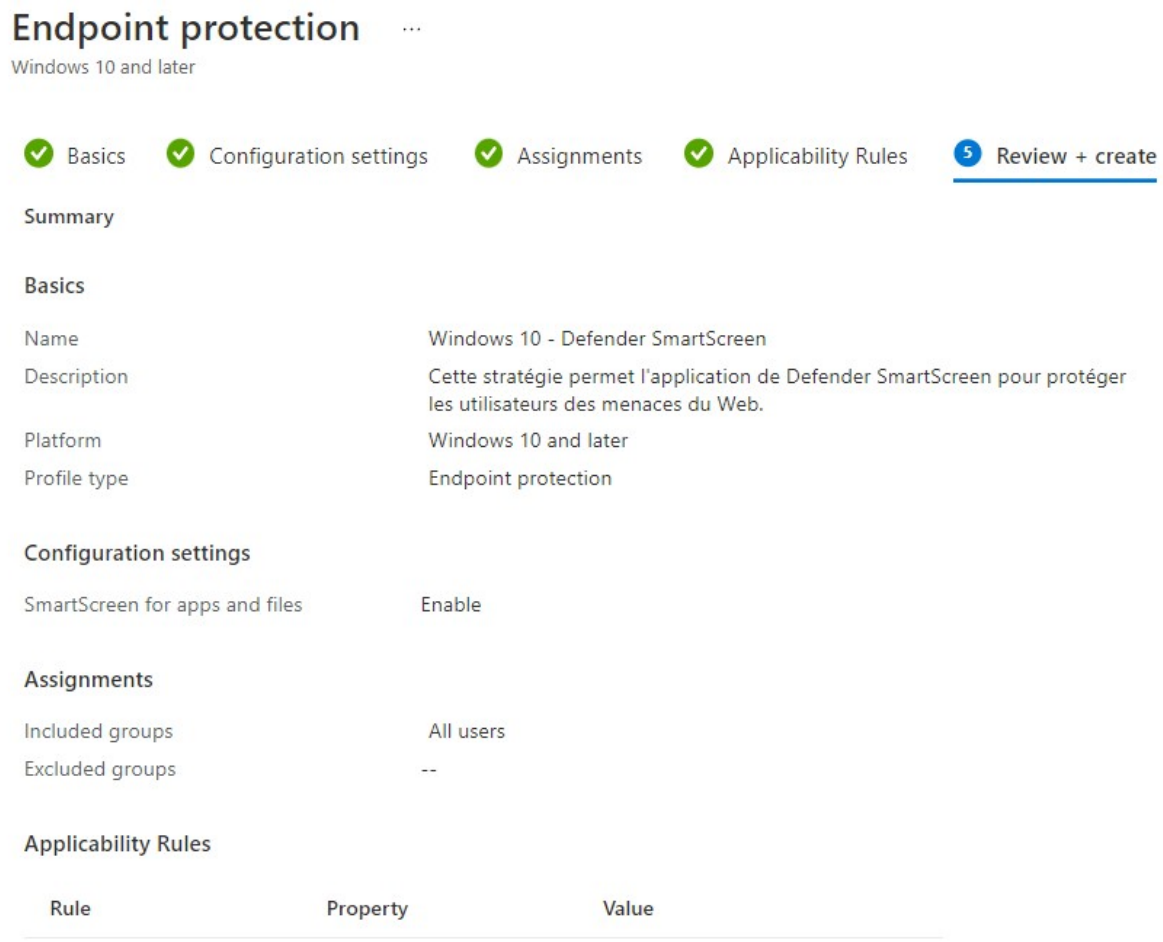
Figure 115 - MEM Portée appliquée pour la stratégie SmartScreen 1
(Source : Auteur)



9) Ne pas appliquer de règles étant donné que nous voulons appliquer SmartScreen à tous les utilisateurs. Cliquer sur « Next ».

10) Prendre connaissance des paramètres de la stratégie et appuyer sur le bouton « Create » en bas de la page :

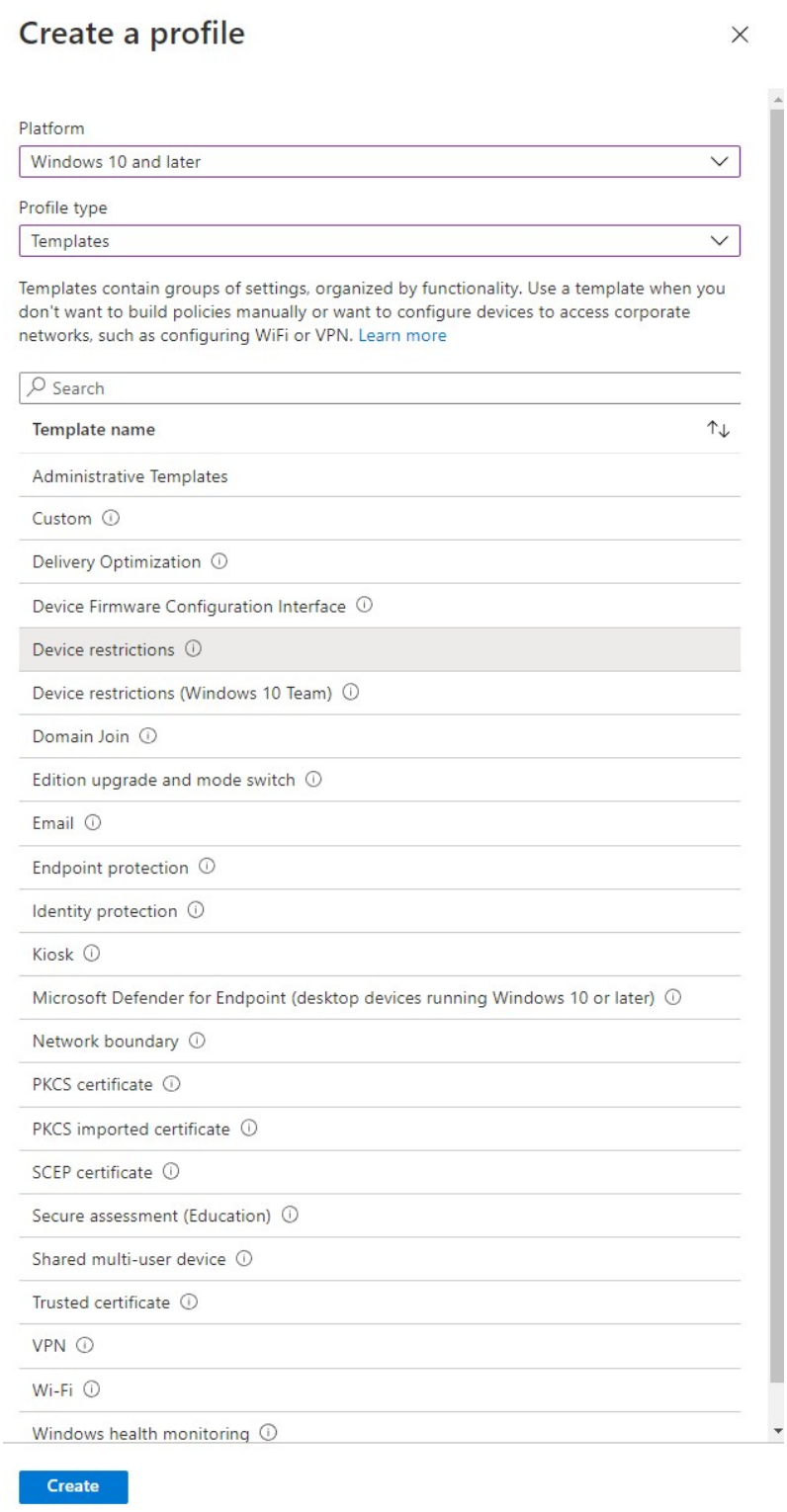
Figure 116 - MEM Confirmation de la stratégie SmartScreen 1
(Source : Auteur)



11) Répéter les étapes 1 à 4 pour créer un autre profil.

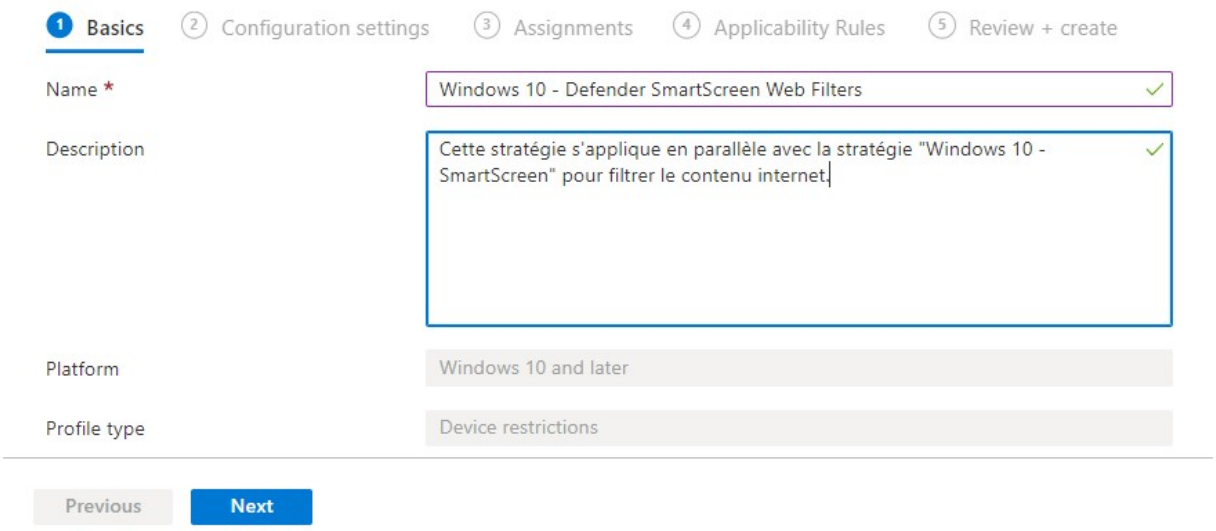
12) Cette fois, nous choisissons « Device restrictions » comme modèle :

Figure 117 - MEM Restriction de l'appareil pour la stratégie SmartScreen
(Source : Auteur)



13) Remplir selon les informations suivantes et cliquer sur « Next » :

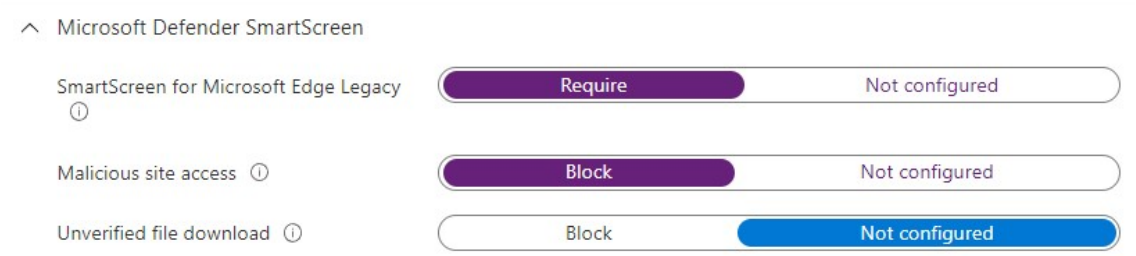
Figure 118 - MEM Information de base pour la stratégie SmartScreen 2
(Source : Auteur)



14) Remplir selon les informations de configuration suivants, puis cliquer sur « Next » :

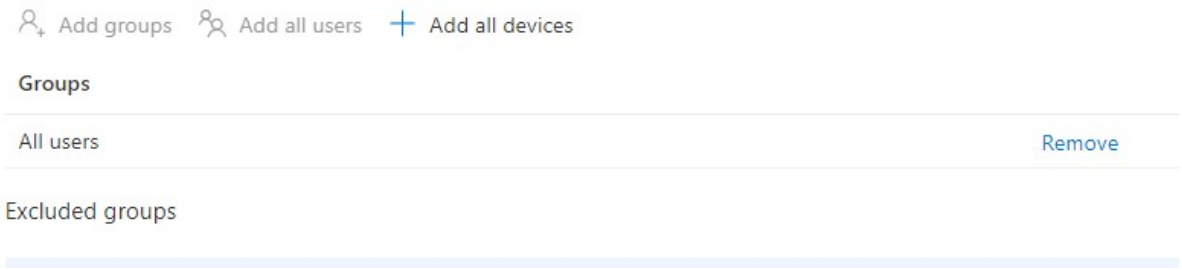
- SmartScreen for Microsoft Edge Legacy : Permet d'activer « Microsoft SmartScreen » pour le navigateur « Microsoft Edge ».
- Malicious site access : Permet de bloquer l'accès à des sites malveillants.
- Unverified file download : Permet d'empêcher l'utilisateur d'ignorer le filtre de l'outil et de télécharger des fichiers non-vérifiés.

Figure 119 - MEM Paramètres pour la stratégie SmartScreen 2
(Source : Auteur)



15) Appliquer la stratégie à tous les utilisateurs, puis cliquer sur « Next » :

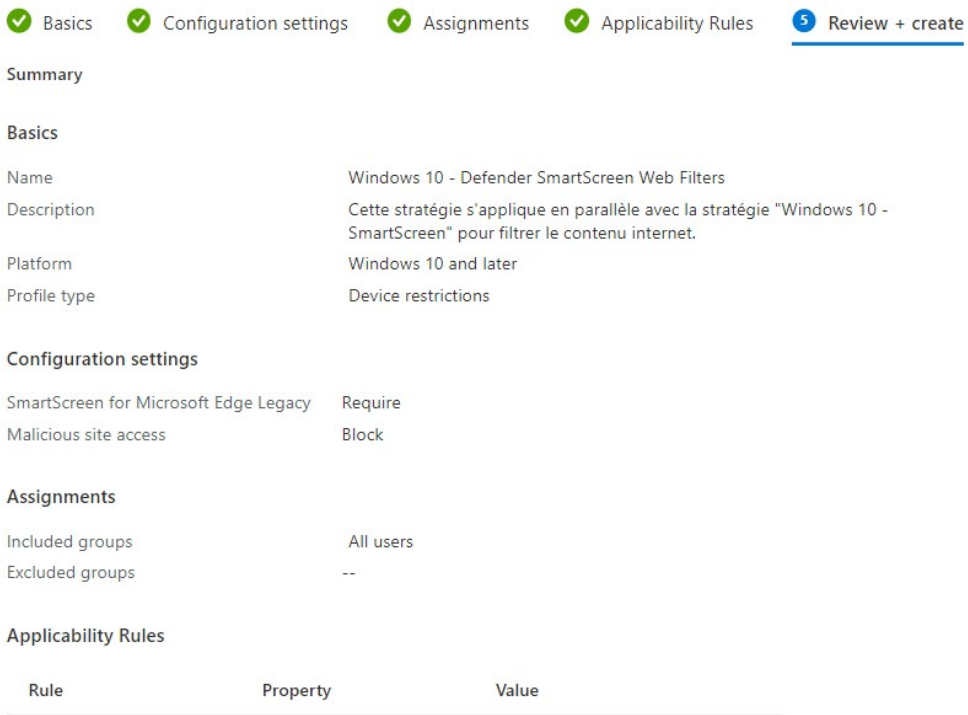
Figure 120 - MEM Portée appliquée pour la stratégie SmartScreen 2
(Source : Auteur)



16) Ne pas ajouter de règles.

17) Consulter les paramètres de la stratégie et cliquer sur « Create » :

Figure 121 - MEM Confirmation de la stratégie SmartScreen 2
(Source : Auteur)



18) Maintenant que la configuration est terminée, il est temps de tester la stratégie sur notre client. Se rendre sur https://demo.smartscreen.msft.net :

19) Testons la fonctionnalité contre les pages contenant potentiellement une tentative malveillante de récolte de données. Cliquer sur « Phishing Page » :

Figure 122 - Page de test SmartScreen de Microsoft
(Source : Auteur)

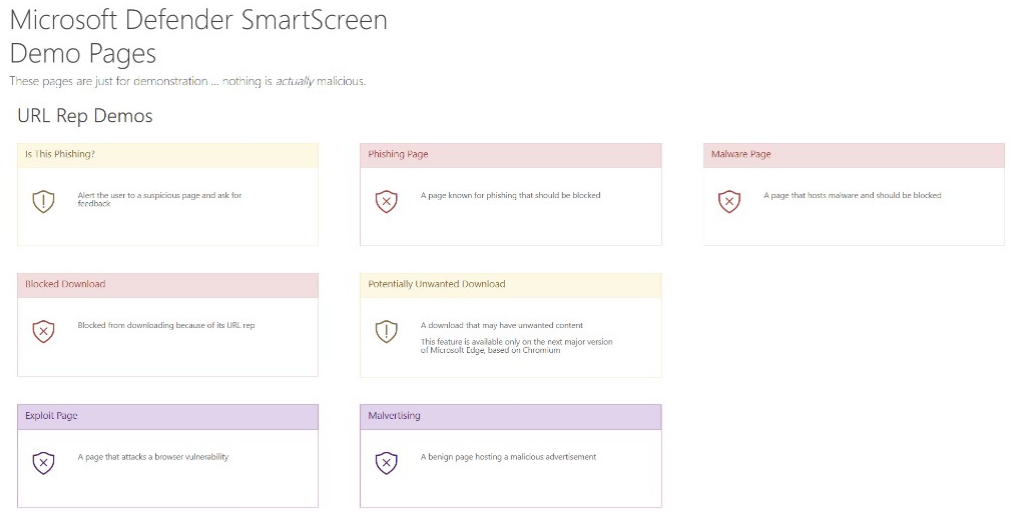
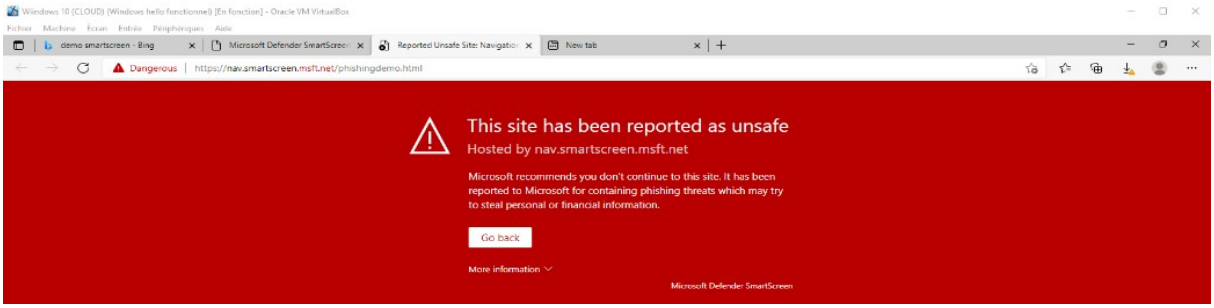


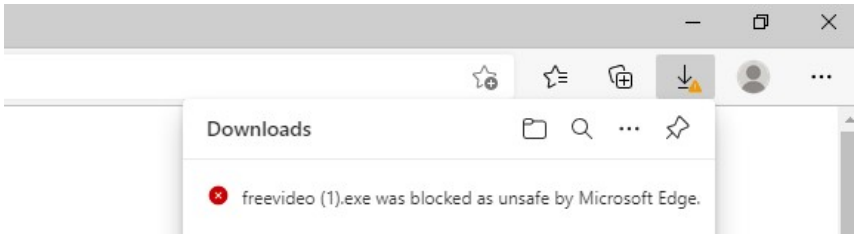
Figure 123 - Application de SmartScreen sur le client
(Source : Auteur)



Nous remarquons que la page a bien été bloquée et l'utilisateur est notifié du caractère dangereux de la page souhaitée.

20) Tentons maintenant de télécharger un fichier malicieux en cliquant cette fois sur « Blocked Download » :

Figure 124 - Téléchargement bloqué par SmartScreen
(Source : Auteur)



Également, le téléchargement du fichier est bloqué par la stratégie que nous avons mise en place.

En conclusion, nous avons ajouté une couche de sécurité à la navigation web de l'utilisateur afin de garantir le bon fonctionnement de son ordinateur.

4. Pour aller plus loin

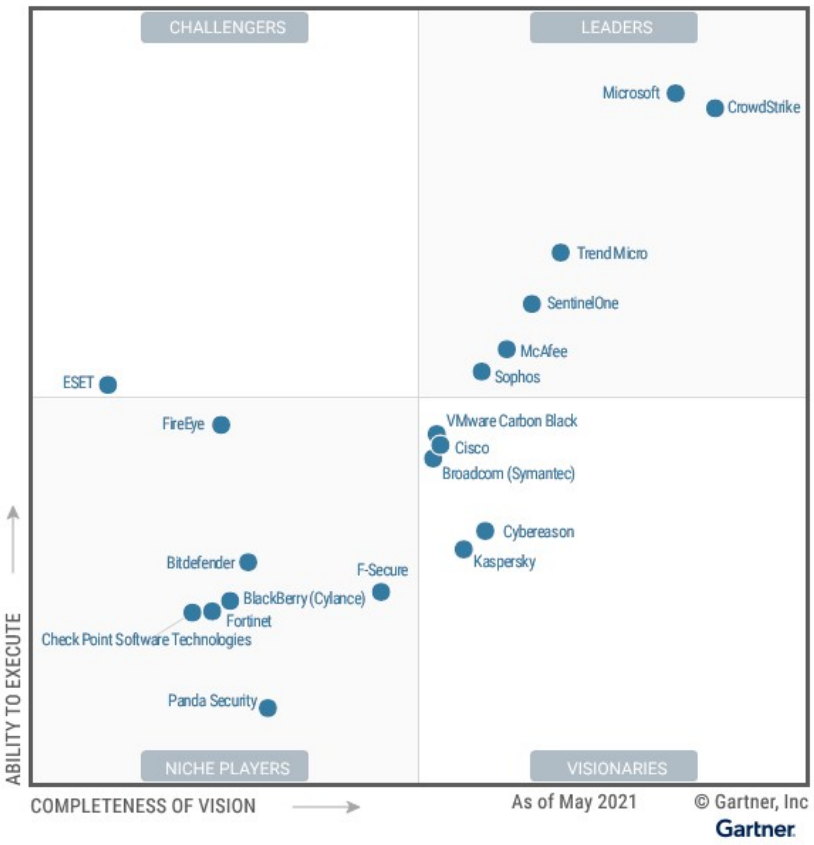
4.1. Comparaison des services Microsoft avec la concurrence

Dans cette partie du travail de Bachelor, nous mettons en relation les produits Microsoft et les produits des principaux concurrents concernant la protection des clients d'une infrastructure.

Malheureusement, par manque de temps et parce que nous ne disposons pas des licences requises, nous ne pouvons pas tester les solutions des concurrents.

Par conséquent, nous nous basons sur une récente étude réalisée par le groupe Gartner (Webber et al., 2021).

Figure 125 - Graphique de comparaison des solutions de protection des clients
(Source : Webber et al., 2021)



Ainsi, nous pouvons remarquer que les principaux leaders du marché des plateformes de protection des clients sont : « CrowdStrike », « TrendMicro », « SentinelOne », « McAfee » et « Sophos ».

Pour déterminer la position de Microsoft face à ses concurrents, nous décrivons tout d'abord le service des entreprises tierces, puis, finalement, nous les confrontons au service de protection de Microsoft.

4.1.1. CrowdStrike

CrowdStrike est présent en tant que leader sur le marché de la protection des clients avec sa suite « Falcon Endpoint Protection ». Tout comme Azure, ce produit est basé sur une protection via le cloud. Le service de CrowdStrike dispose d'un antivirus de nouvelle-génération et une protection des clients basée sur la détection et la réponse. Également, il permet d'organiser l'ensemble de l'infrastructure pour lutter contre les menaces et garantir la sécurité de l'environnement.

De plus, le produit Falcon intègre une solution basée sur le machine learning et l'intelligence artificielle pour détecter très tôt les menaces potentielles présentes sur les clients.

Tableau 2 - Qualités et Faiblesses CrowdStrike
(Source : Webber et al., 2021)

Qualités	Faiblesses
• Présence de toutes les composantes essentielles sur une seule plateforme facile d'utilisation.	• Coûts supplémentaires pour bénéficier de l'ensemble de protection
• Excellente réputation sur le marché	• Pas de possibilités « On-Premise »
• Grande cible d'attaque, ce qui a amélioré l'algorithme de détection	• Ne possède pas la meilleure détection et réponse étendue du marché

4.1.2. TrendMicro

La société TrendMicro est également présentée en tant que leader. Elle propose une solution de sécurité avec son produit « Smart Protection ». Cette suite dispose d'un composant de protection des clients se nommant « Apex One ». Celle-ci remplace l'ancienne solution « OfficeScan ».

« Apex One » dispose de plusieurs fonctionnalités utilisables tels que :

- Une protection basée sur la détection et la réponse.
- Une détection basée sur l'intelligence artificielle (avant exécution et en temps réel).

- Un chiffrement des données.
- Un système de mise à jour pour lutter contre les failles.

La solution de TrendMicro est disponible autant sur le cloud que pour les infrastructures On-Premise.

Tableau 3 - Qualités et Faiblesses TrendMicro
(Source : Webber et al., 2021)

Qualités	Faiblesses
• Grande capacité d'intégration (ex : container cloud)	• Beaucoup de mises à jour à effectuer
• Progrès en constante expansion	• L'automation et l'orchestration ne sont pas aussi efficace que la concurrence
• Système de « patching » via des mises à jour	• Ne dispose pas d'une très bonne réputation

4.1.3. SentinelOne

« Singularity » est le nom du produit de la société pour assurer la protection des clients Windows. Dans cette optique, celui-ci axe sa protection en proposant à leurs utilisateurs plusieurs fonctionnalités :

- Intelligence artificielle : Grâce au machine learning, « Singularity » permet de délivrer une protection nouvelle-génération des menaces connues et celles émergentes.
- Monitoring : Le service permet également de bénéficier d'une solution de monitoring comme aide à la décision pour les administrateurs. Lorsqu'une menace est détectée, une alerte est notifiée au responsable informatique pour traitement.
- Expertise : « Singularity » offre tout un panel d'experts en cybersécurité via une assistance 24 heures sur 24 et sept jours sur sept.
- Protection en temps réel : Le module « ActiveEDR » permet d'assurer une protection en temps réel. Celui-ci implique une détection et une réponse aux menaces potentielles avec un traitement automatique totalement personnalisable.

Tableau 4 - Qualités et Faiblesses SentinelOne
(Webber et al., 2021)

Qualités	Faiblesses
• Très bonne qualité du support à la clientèle	• Dépend énormément de ses partenariats
• Haute détection des malwares	• Manque de fonctionnalités comparé à la concurrence
• Facilité de déploiement	• Le service hybride et On-Premise ne dispose pas des mêmes métriques que les architectures full-cloud.

4.1.4. McAfee

Le célèbre antivirus dispose également d'une solution de protection des clients. Celle-ci est sobrement intitulée « McAfee Endpoint Security ».

La protection de McAfee permet d'améliorer la sécurité de Windows déjà présente en ajoutant une protection supplémentaire grâce à la base de données de l'entreprise.

De plus, cette solution repose également sa détection de menace sur le machine learning afin de procurer une protection complète aux utilisateurs Windows.

La sécurité de McAfee permet de protéger les fichiers de l'utilisateurs. De plus, elle rend possible la protection de la navigation internet, des mails entrants et procure même une protection au niveau du réseau.

Tableau 5 - Qualités et Faiblesses McAfee
(Webber et al., 2021)

Qualités	Faiblesses
• Permet une stratégie de réduction de la surface d'attaque « pre-breach »	• Les fonctionnalités On-Premise sont en retard face à celles du Cloud
• Interface utilisateur agréable	• Manque de fonctionnalités (ex : analyse du trafic réseau)
• McAfee prend en charge les infrastructures On-Premise	• Pas très populaire

4.1.5. Sophos

La dernière solution que nous analysons est celle de l'entreprise Sophos avec ses solutions « Intercept X » et « Managed Threat Response ».

La première solution permet de disposer d'une protection traditionnelle des points de terminaison mais également d'une protection plus moderne grâce à l'ajout de fonctionnalité telle que le deep learning dans la détection des malware.

La deuxième solution « Managed Threat Response » permet à un utilisateur de disposer de l'expertise des employés en cybersécurité de Sophos. Cette expertise est disponible à toutes les heures et tous les jours.

Ces deux solutions sont disponibles et agrégées sur une seule plateforme pour faciliter l'organisation des administrateurs.

Tableau 6 - Qualités et Faiblesses Sophos
(Webber et al., 2021)

Qualités	Faiblesses
• Services constamment améliorés avec l'ajout de nouvelles fonctionnalités	• Le service de gestion On-Premise n'est pas très développé.
• Très efficace contre les ransomwares	• Souvent des problèmes techniques de synchronisation
• Grande popularité	• Peu d'évaluation concernant son efficacité contre les malwares

4.1.6. Concurrents VS Microsoft

Comme nous l'avons vu dans la rubrique précédente, tous les services de protection présents sur le marché se ressemblent énormément. Nous pouvons partir du principe qu'ils sont tous performant dans leur domaine.

Cependant, le choix de reposer sa protection des clients dépendra principalement de l'infrastructure qu'une entreprise possède, ainsi que des fonctionnalités dont elle a besoin pour concilier ses activités avec sa stratégie de sécurité.

Nous présentons les résultats de notre analyse avec un tableau pour comparer l'efficacité des solutions de Microsoft avec sa concurrence. Pour ce faire, nous nous basons sur les analyses de l'agrégateur de notes de l'entreprise Gartner :

Tableau 7 - Agrégateur des notes des acteurs du marché (Source : Gartner, s. d.)

	Facilité d'utilisation	Efficacité de la prévention	Fonctionnalités	Prix	Service et support	Volonté de recommandation	Score globale
CrowdStrike (Falcon)	4,8	4,9	4,9	18,99$ par clients (Falcon premium)	4,8	92%	4,88 ★★★★★
McAfee (Endpoint Protection)	4,5	4,5	4,4	96,13$ par année (Avanced Suite)	4,4	82%	4,47 ★★★★☆
SentinelOne (Singularity)	4,8	4,9	4,8	85$ par année (Complete Suite)	4,8	96%	4,87 ★★★★★
Sophos (Managed Thread Reponse)	4,8	4,8	4,8	75$ par année (Managed Threat Reponse)	4,5	88%	4,75 ★★★★★
TrendMicro (Apex One)	4,5	4,7	4,5	33$ par clients (Apex One with XDR)	4,5	86%	4,61 ★★★★☆
Microsoft (Enteprise Mobility + Security E3)	4,7	4,3	4,3	10,60$ par mois (Microsoft Defender)	4,3	77%	4,32 ★★★★☆

Nous pouvons donc remarquer que Microsoft dispose du score global le plus bas quand on compare sa solution avec la concurrence.

Le service de CrowdStrike semble faire l'unanimité chez les utilisateurs selon Gartner.

Cependant, il est important de noter que ce tableau n'est pas forcément une réponse directe quant au choix à privilégier. En effet, le service doit être déterminé en fonction de l'infrastructure et des besoins de l'entreprise concernant la protection des points de terminaison.

Par exemple, il est intéressant de savoir que CrowdStrike est uniquement disponible sur le Cloud. Il n'existe pas d'alternative pour une utilisation On-Premise. Cela peut potentiellement rebuter certains consommateurs qui souhaitent disposer d'une telle infrastructure. De plus, nous avons vu, dans ce document, que Microsoft dispose de plusieurs solutions de gestion dans un cadre On-Premise.

En outre, Microsoft a l'avantage d'être beaucoup plus mature sur le marché que d'autres concurrents. Cela implique une certaine expertise et une capacité de réaction beaucoup plus grande. Également, Microsoft dispose de grandes ressources financières et, par conséquent, matérielles qui continuent de grandir au fur et à mesure des années. Plusieurs partenariats sont accessoirement bénéfiques à Microsoft.

En conclusion de cette analyse, nous recommandons de définir des objectifs de sécurité afin de sélectionner le prestataire qui répondra au mieux aux besoins de l'organisation.

4.2. Guide de migration vers un environnement Cloud

La partie d'analyse du document détermine que le Cloud est la solution que nous choisissons.

Dans le cadre de ce travail, nous proposons, dans cette partie, un guide afin de procéder à la migration de l'infrastructure vers un environnement entièrement Cloud.

Le but de ce guide est d'atteindre un état de gestion et de contrôle de la protection des points de terminaison entièrement basés sur les produits de Microsoft et dans le Cloud. Ainsi, nous partons du principe qu'une infrastructure de gestion de la sécurité On-Premise est déjà mise en place soit par :

- Active Directory et GPO
- Configuration Manager

4.2.1. Active Directory et GPO

Ici, nous développons le scénario dans lequel une entreprise est d'ores et déjà dans la possession d'une infrastructure de gestion de la sécurité de ses clients par le biais d'un Active Directory complété par l'utilisation de GPO.

Après analyse de ses besoins, l'entreprise décide de passer sur le Cloud pour bénéficier de ses fonctionnalités.

4.2.1.1. Informations

Ce guide est basé entièrement sur la documentation de Microsoft (2021m).

Il permet d'analyser les GPO mise en place grâce à l'outil « Group Policy analytics » et de trouver les possibles correspondances sur le service Intune.

4.2.1.2. Exigences

- Une machine Windows Serveur sur lequel un Active Directory et des GPO sont correctement installés et configurés.
- Une machine Windows Client.
- Un tenant configuré (voir Annexe I et II).

4.2.1.3. Configuration

Windows Serveur

1) Ouvrir l'application Group Policy management (GPMC.msc) :

Figure 126 - Ouverture de Group Policy Management
(Source : Auteur)

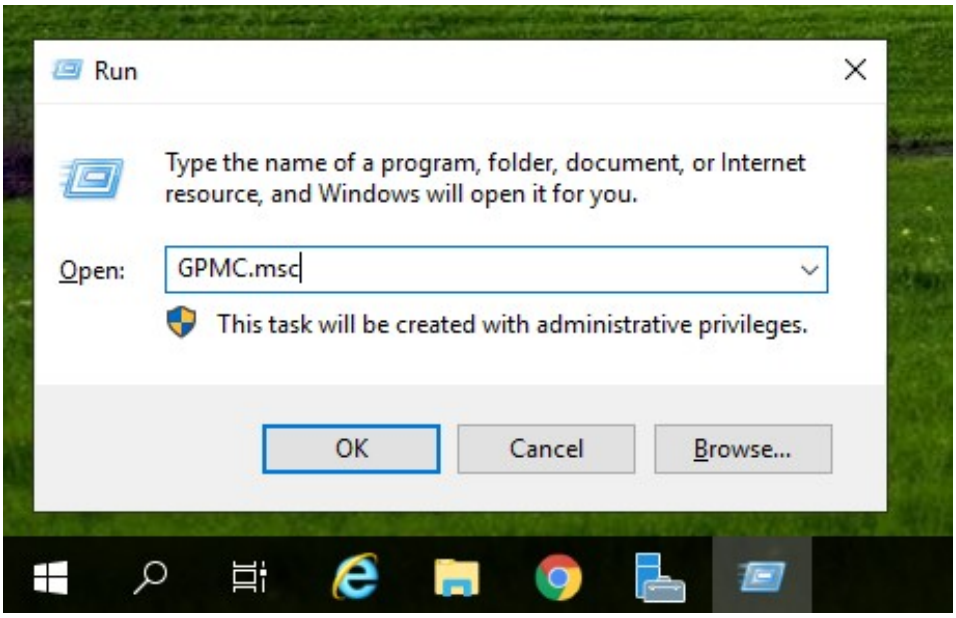
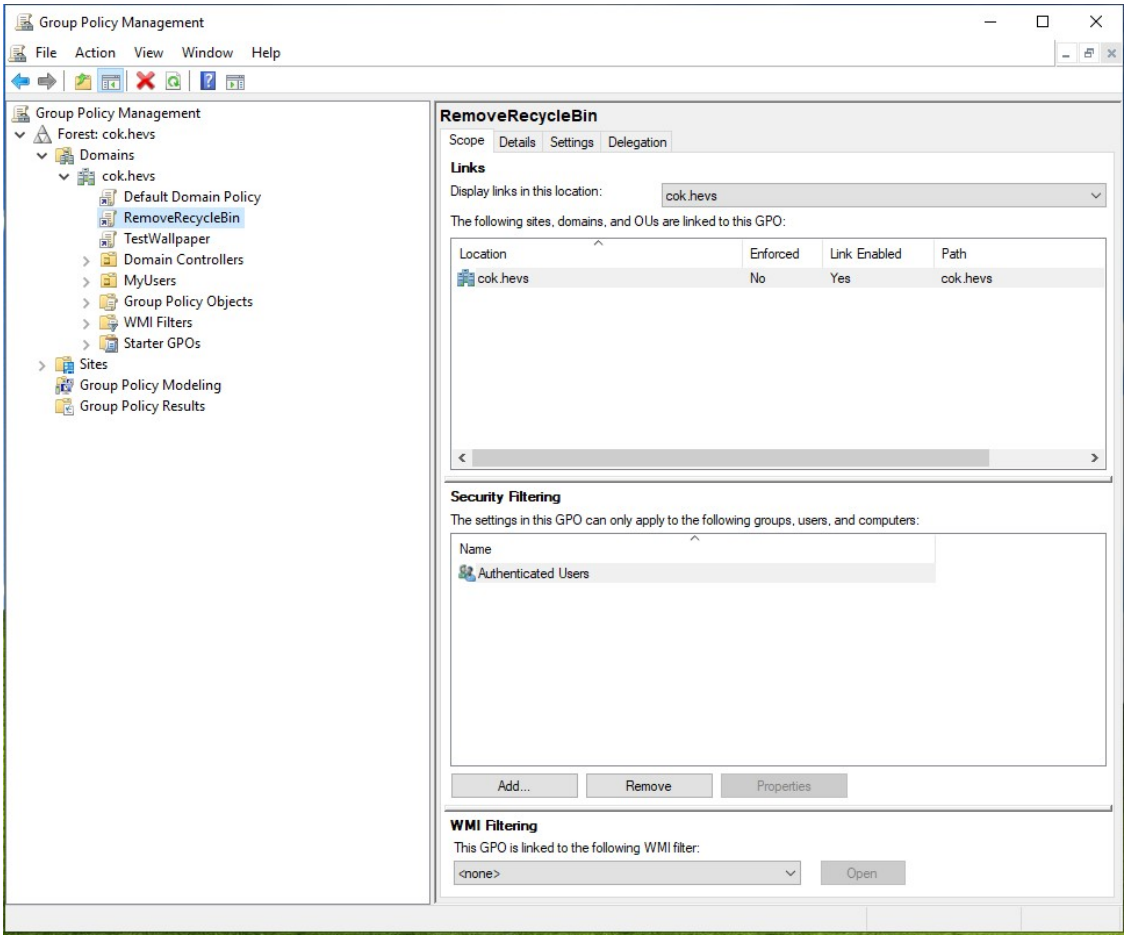
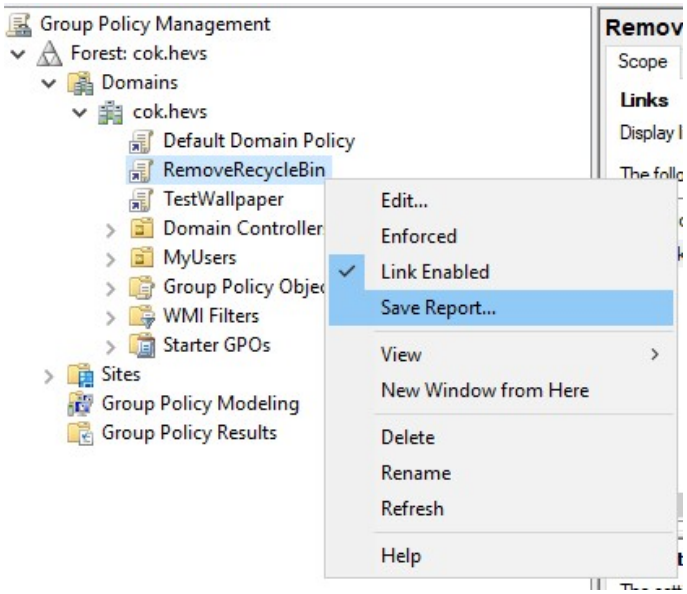


Figure 128 - Fenêtre Group Policy Management
(Source : Auteur)



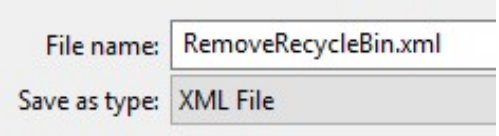
2) Faire un clic-droit sur le GPO que nous voulons exporter et sélectionner « Save Report » :

Figure 127 - Exportation d'une police
(Source : Auteur)



3) Enregistrer le fichier au format XML dans le répertoire souhaité :

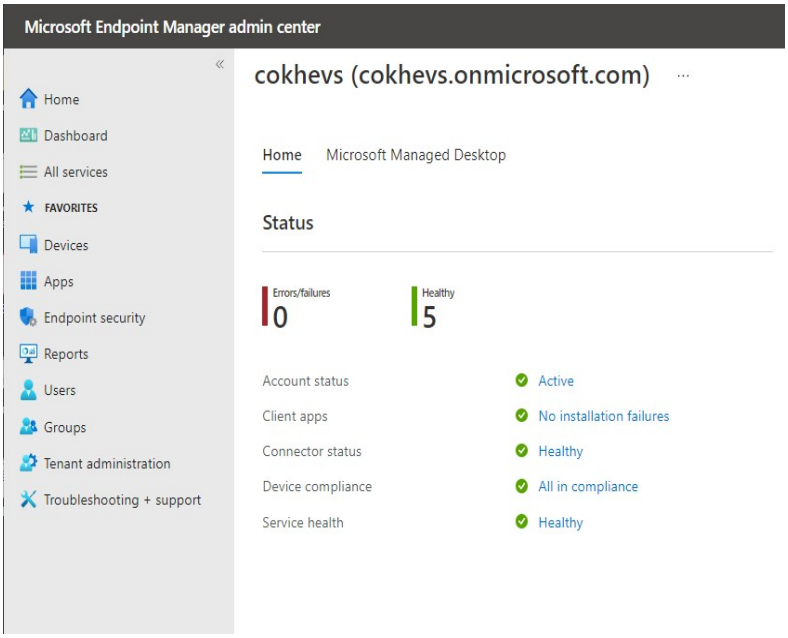
Figure 129 - Enregistrement de la police exportée
(Source : Auteur)



MEMAC

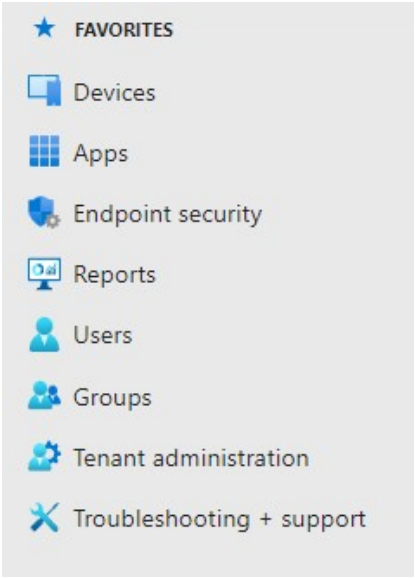
1) Ouvrir Microsoft Endpoint Manager Admin Center :

Figure 130 - Accueil MEM pour migration Cloud
(Source : Auteur)



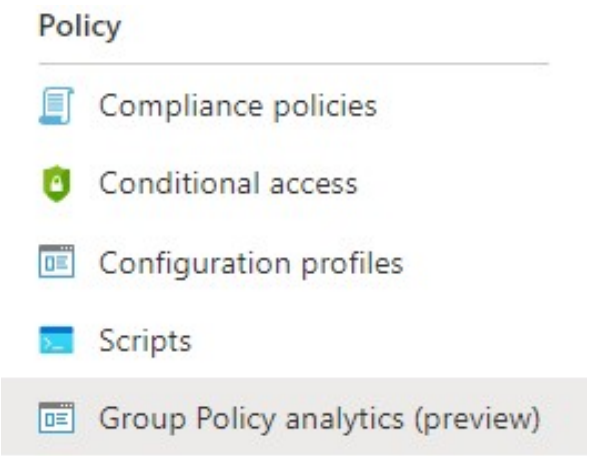
2) Se rendre dans le menu « Devices » :

Figure 131 - MEM Menu pour la migration Cloud
(Source : Auteur)



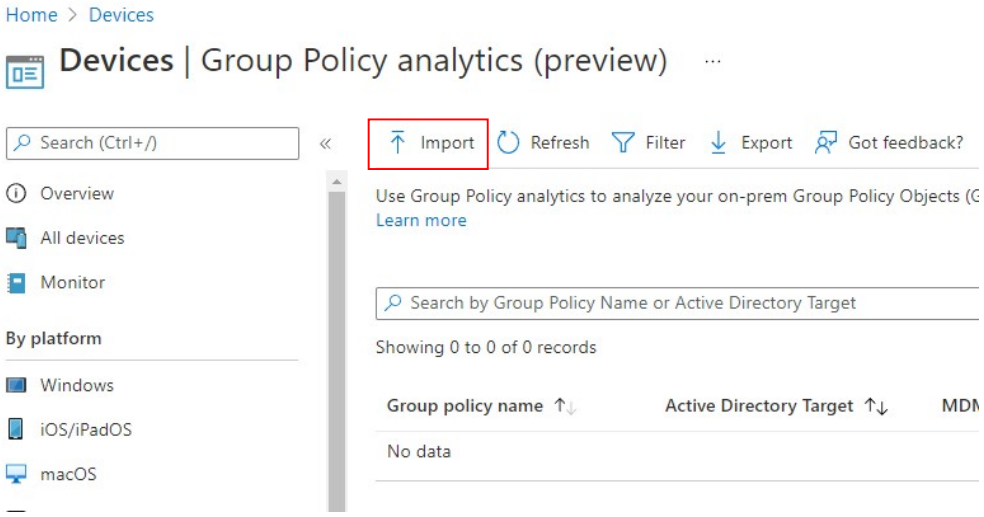
3) Sous la rubrique « Policy », ouvrir « Group Policy analytics » :

Figure 132 - MEM Menu Policy
(Source : Auteur)



4) Au sommet de la page, sélectionner le bouton « Import » :

Figure 133 - MEM Bouton Import
(Source : Auteur)



5) Dans le menu d'importation, cliquer sur l'icône de dossier et choisir le fichier XML généré précédemment :

Figure 134 - MEM Menu d'importation du GPO
(Source : Auteur)

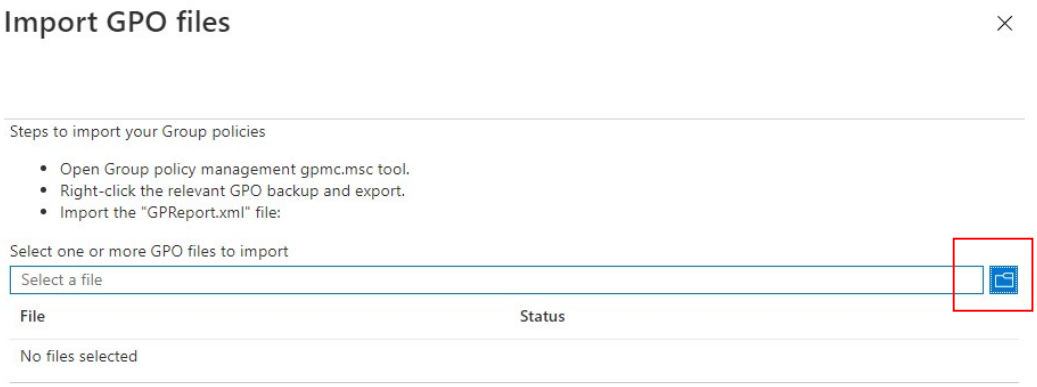
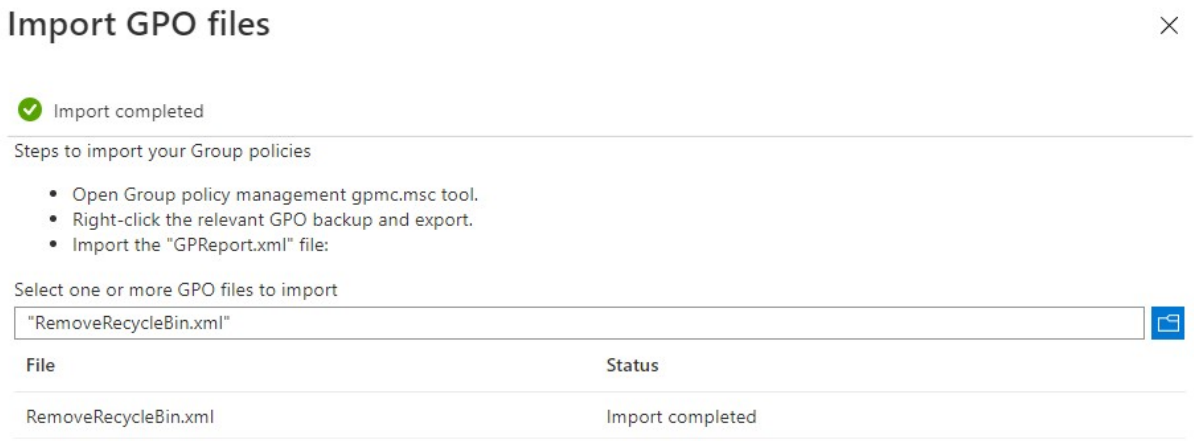
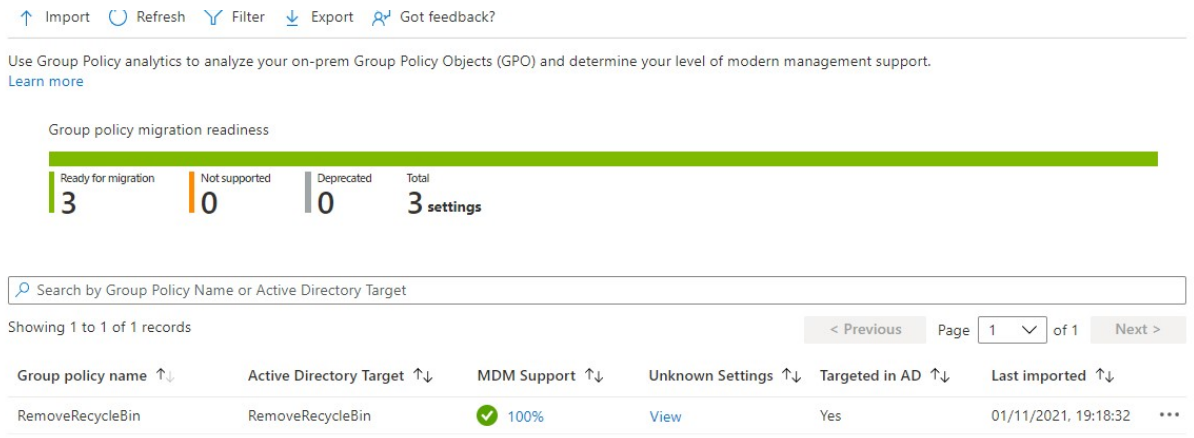


Figure 135 - MEM Import du GPO complété
(Source : Auteur)



6) Vérifier que l'import s'est correctement déroulé :

Figure 136 - MEM Résultat de l'import
(Source : Auteur)



7) Cliquer sur le pourcentage en dessous de « MDM Support » :

Figure 137 - Pourcentage du support MDM
(Source : Auteur)

Ce pourcentage nous indique l'ensemble des paramètres disponibles sur Intune. Lorsque le pourcentage n'est pas à 100%, il est nécessaire d'inspecter et de déterminer quels GPO sont incompatibles.

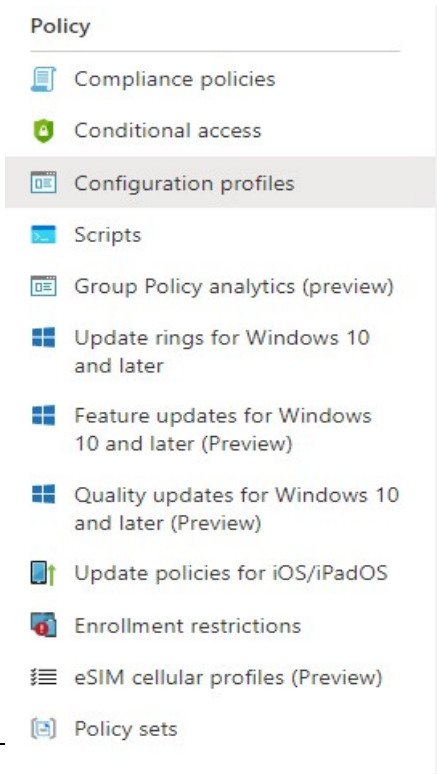
Dans notre cas, les différents résultats de l'analyse nous permettent de retrouver le profil correspondant sur Intune.

Figure 138 - Nom de la police CSP
(Source : Auteur)

Étant donné que nous connaissons le CSP[3] correspondant, nous pouvons maintenant l'appliquer à nos appareils. Le nom du CSP se trouve à la fin du mapping : « NoRecycleBinIcon ».

8) Se rendre dans « Configuration profiles » sous « Policy » :

Figure 139 - MEM Menu de configuration des profiles pour la migration Cloud
(Source : Auteur)



[3] Le CSP est l'équivalent d'un GPO mais sur Intune.

9) Cliquer sur « Create profile » :

Figure 140 - MEM Bouton Création profile
(Source : Auteur)

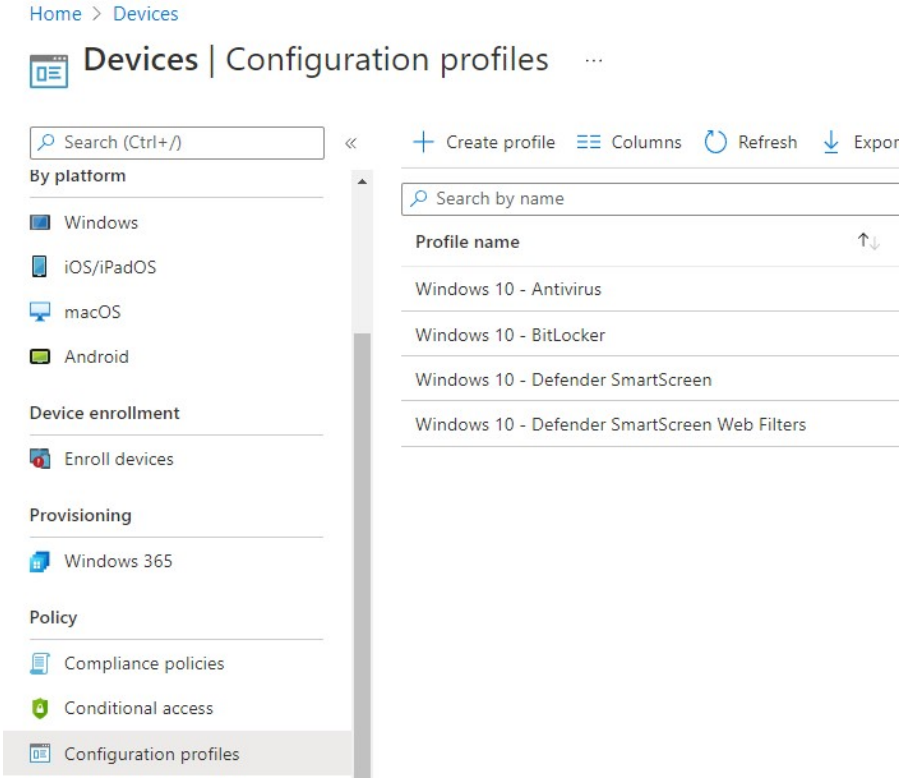
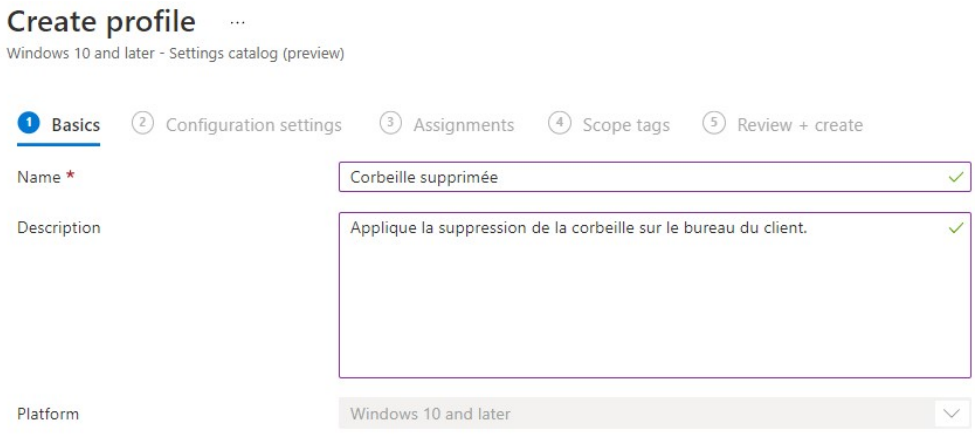


Figure 141 - MEM Création du profile de la migration Cloud
(Source : Auteur)

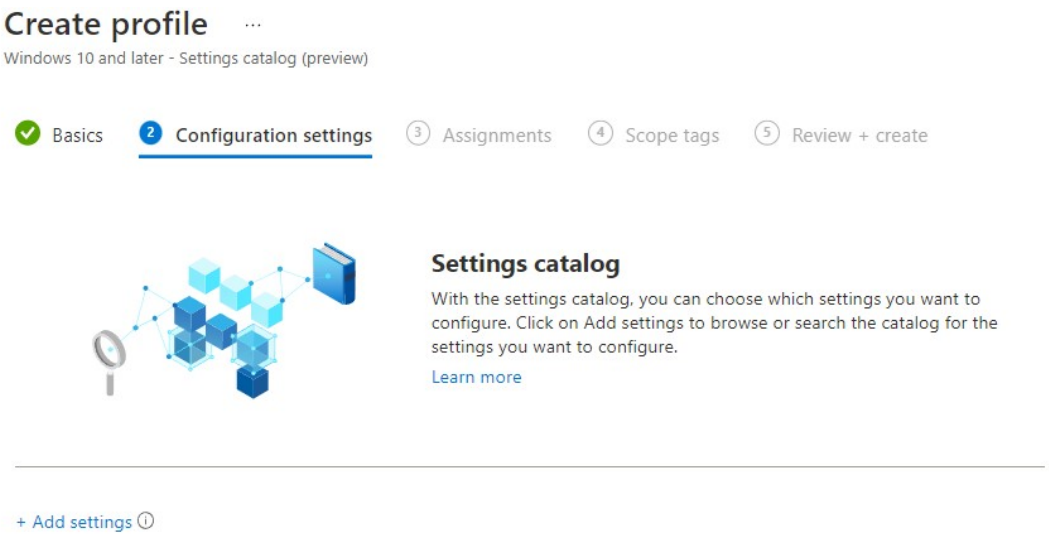
10) Remplir comme suivant :

Figure 142 - MEM Informations de base profile migration Cloud
(Source : Auteur)



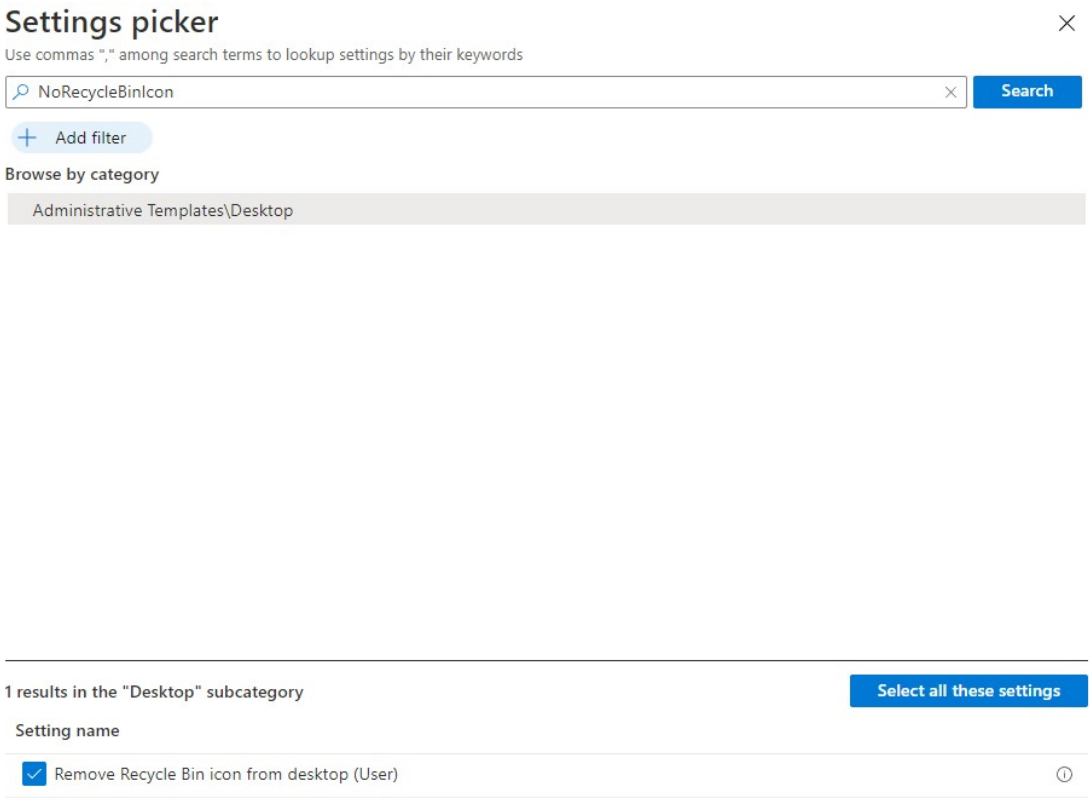
11) Sur la page suivante, cliquer sur « Add settings » pour ajouter notre paramètre :

Figure 143 - MEM Configuration des paramètres de catalogue
(Source : Auteur)



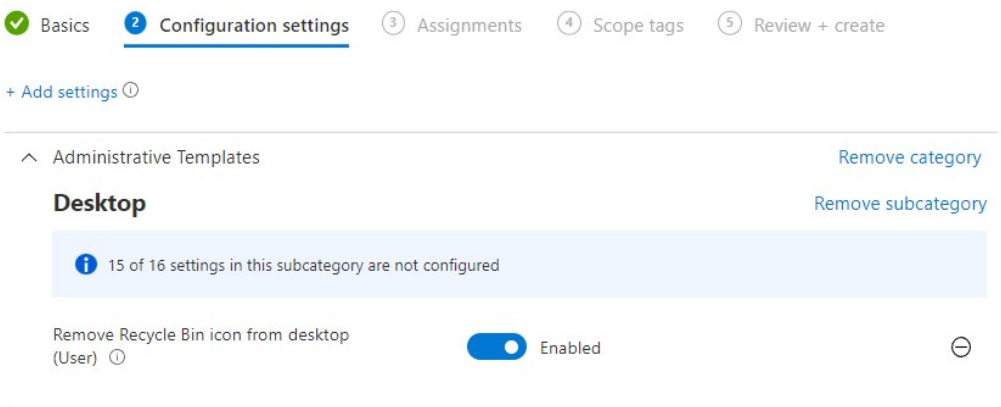
12) Taper le nom du CSP que nous avons trouvé tout à l'heure et le sélectionner :

Figure 144 - MEM Recherche par nom du CSP
(Source : Auteur)



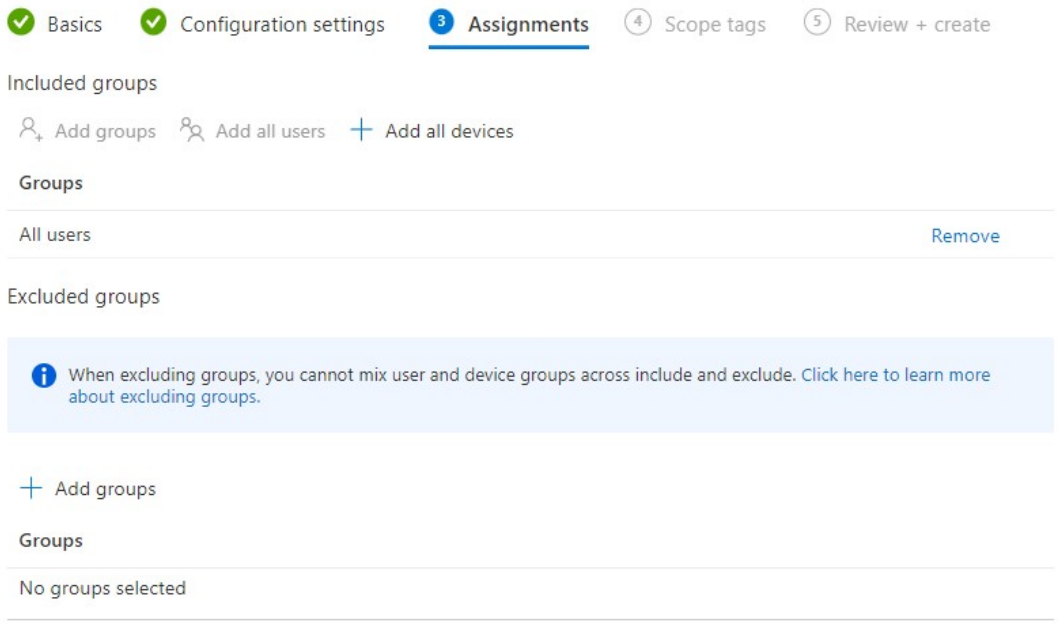
13) Fermer la page latérale et activer le paramètre :

Figure 145 - MEM Activation du CSP
(Source : Auteur)



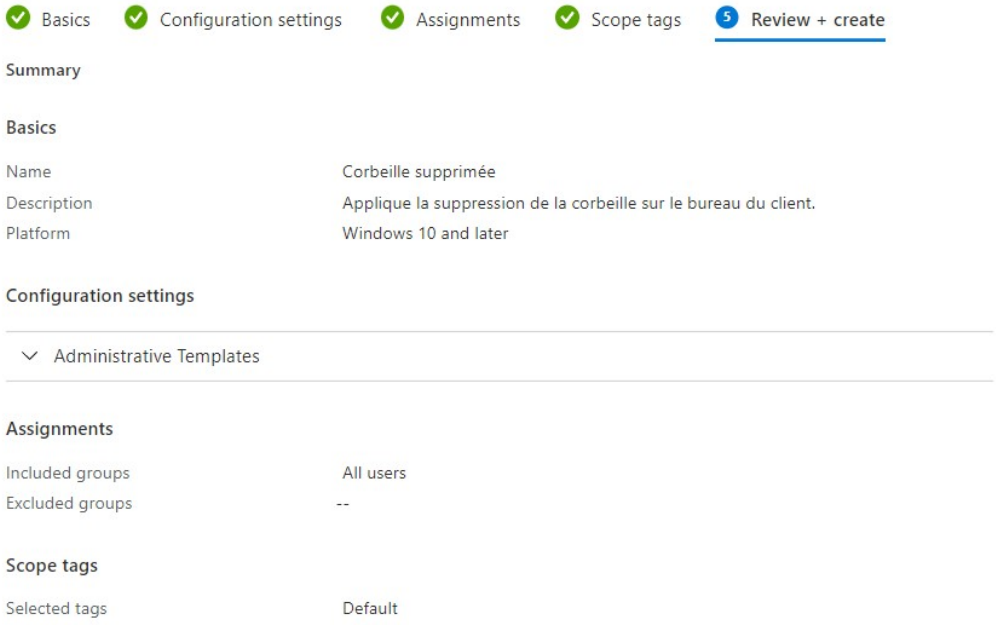
14) Appliquer aux utilisateurs souhaités :

Figure 146 - MEM Application du CSP à tous les utilisateurs
(Source : Auteur)



15) Confirmer les paramètres et créer le profile :

Figure 147 - MEM Confirmation et création du CSP
(Source : Auteur)



Nous disposons maintenant de la même stratégie prête à être déployée sur notre client via le service Intune.

A noter qu'il n'est malheureusement pas encore possible d'automatiser le processus pour le moment. Par conséquent, il est nécessaire de faire la manipulation pour chaque type de GPO que nous souhaitons migrer. Il est cependant intéressant de procéder ainsi car cela peut mener à une reconsidération de la stratégie de sécurité On-Premise mise en place.

Également, il existe un grand nombre de CSP utilisable uniquement sur une version spécifique de Windows. Le site de la documentation officielle de Microsoft nous permet de prendre connaissance de ces exigences pour chaque police :

https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider

4.2.2. Configuration Manager

Dans le cas d'une volonté d'abandonner le Configuration Manager et de partir sur une solution de gestion entièrement basée sur le cloud, il est possible de basculer complètement la charge de travail sur Intune.

Cette fonctionnalité utilise le principe de Co-Management.

4.2.2.1. Informations

Ce guide est basé entièrement sur la documentation de Microsoft (2021d).

Il permet d'abandonner une utilisation sur site de la gestion de la sécurité des clients au profit d'une gestion 100% Cloud.

4.2.2.2. Exigences

- Une machine Windows Serveur sur laquelle SCCM est correctement installé et fonctionnel.
- Une machine Windows Client.
- Un tenant configuré.

4.2.2.3. Configuration

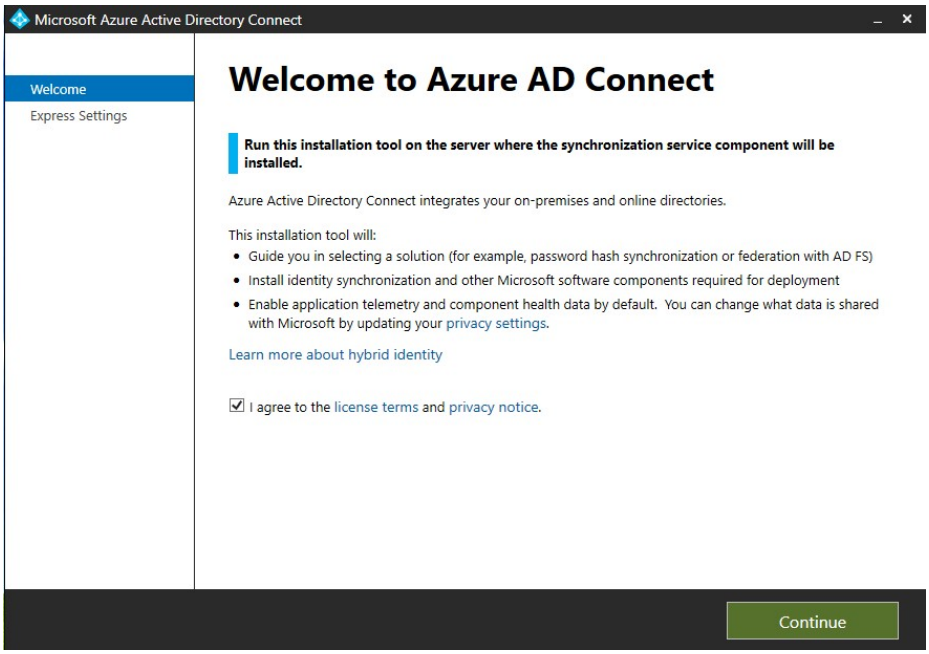
Afin de rendre la migration plus facile, il est préférable de lier notre Active Directory On-Premise à notre Azure Active Directory pour un déploiement unifié de tous nos comptes utilisateurs. Pour ce faire, nous utilisons l'outil « Azure Active Directory Connect ».

AD Connect

1) Télécharger et installer Azure AD Connect :
   https://www.microsoft.com/en-us/download/details.aspx?id=47594

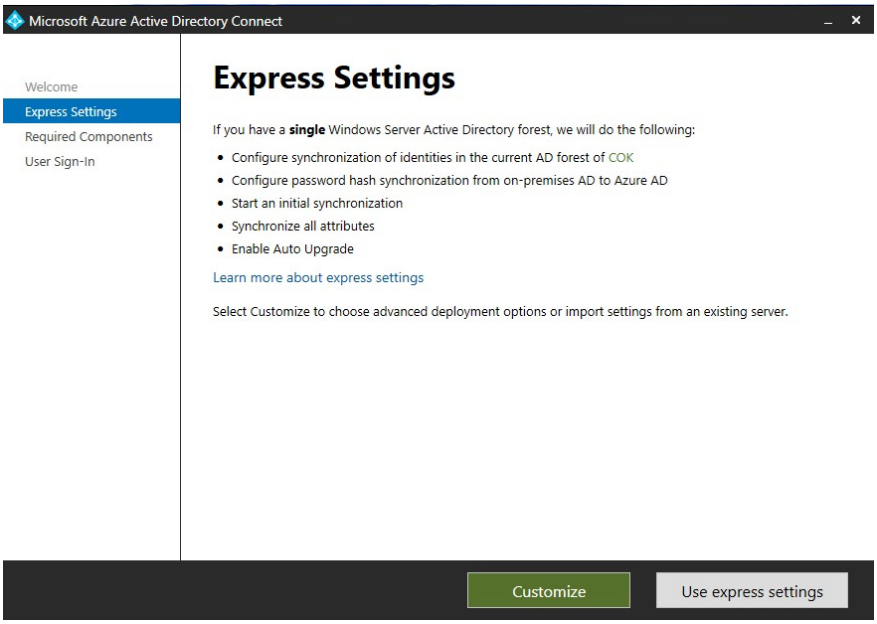
2) Cliquer sur Continuer :

Figure 148 - Accueil Azure AD Connect
(Source : Auteur)



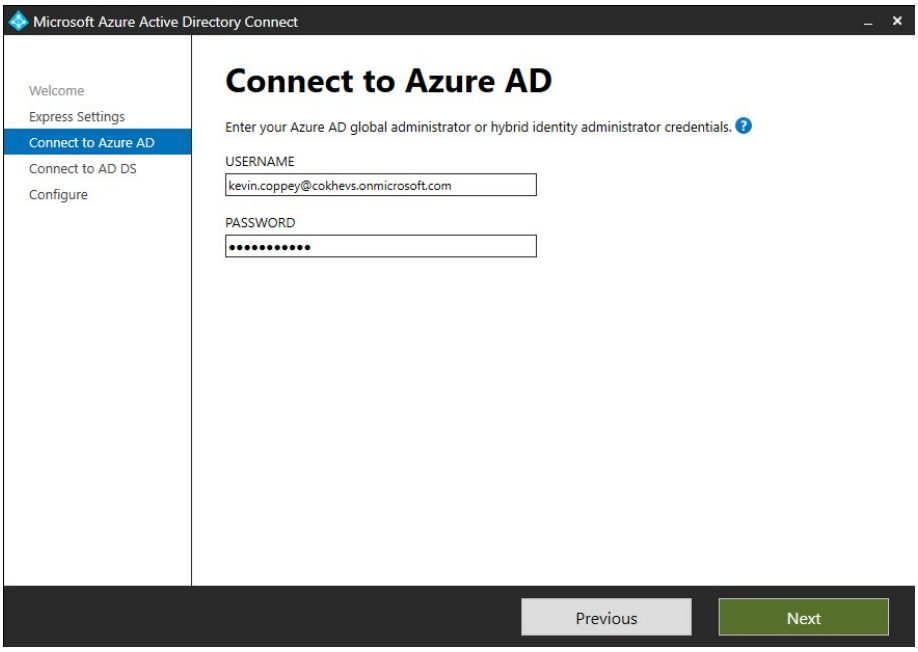
3) Cliquer sur « Use Express settings »

Figure 149 - Paramètres express AD Connect
(Source : Auteur)



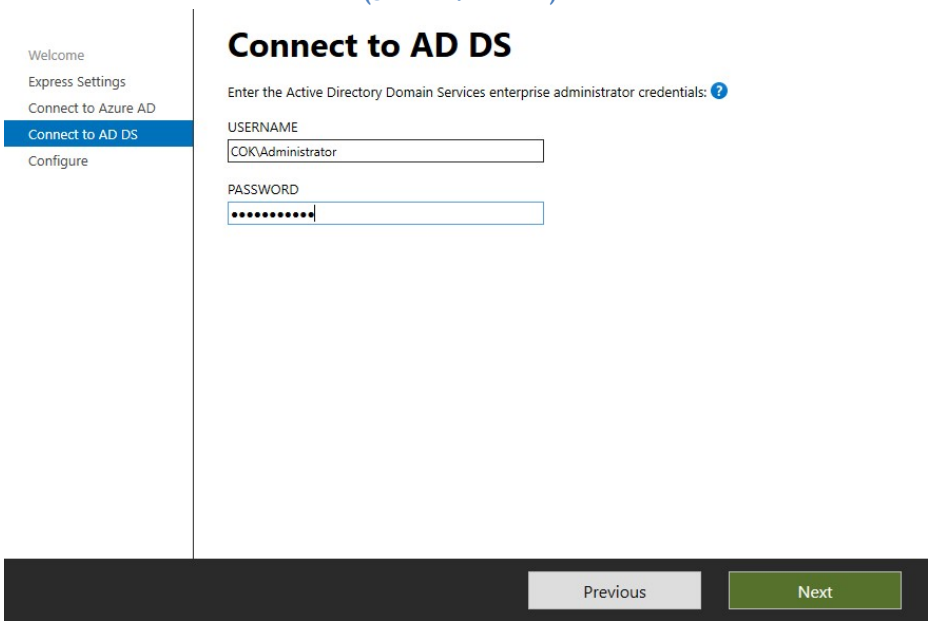
4) Entrer ses informations de connexion du compte administrateur du tenant :

Figure 150 - Liens vers le tenant AD Connect 1
(Source : Auteur)



5) Entrer les informations de connexion administrateurs du contrôleur de domaine :

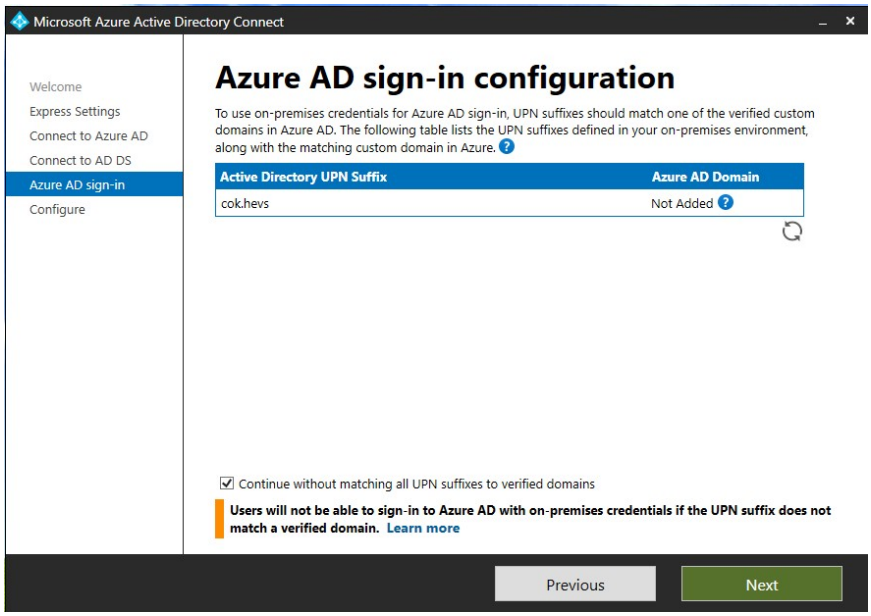
Figure 151 - Connexion sur l'AD DS
(Source : Auteur)



Il est possible de proposer aux utilisateurs du domaine d'utiliser leurs identifiants de connexion On-Premise sur les services du Cloud de Microsoft. Dans un cas réel, il est recommandé de le faire. Cependant, dans le cas de notre test, nous ne mettons pas cette fonctionnalité en place.

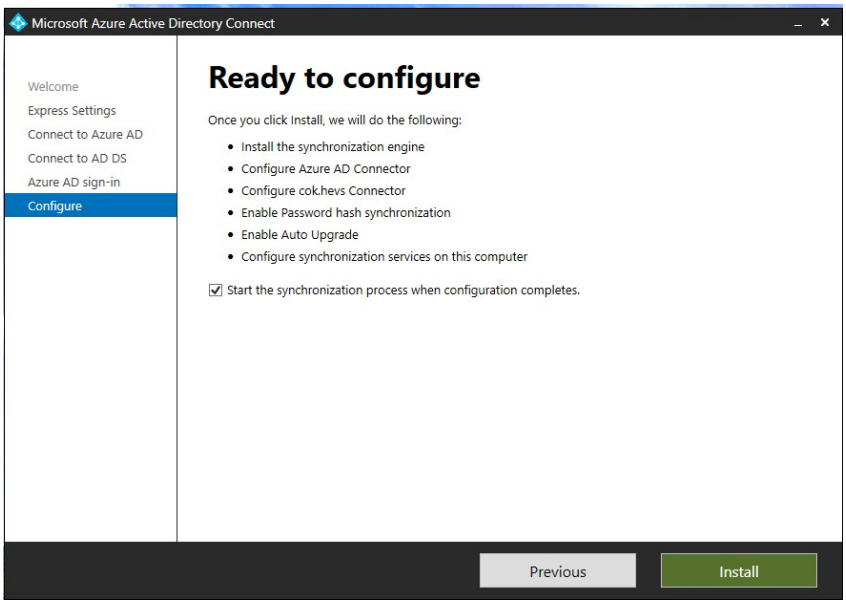
6) Cocher « Continue without matching all UPN suffixes to verified domains » et passer à l'écran suivant :

Figure 152 - Utilisation des informations de connexion de l'AD On-Premise
(Source : Auteur)



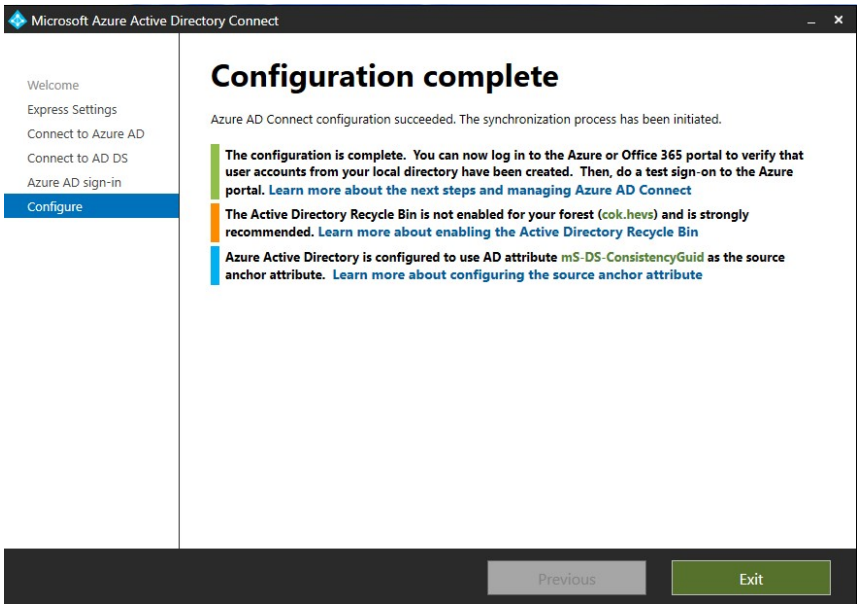
7) Cliquer sur « Install » :

Figure 153 - Fin de l'installation d'AD Connect
(Source : Auteur)



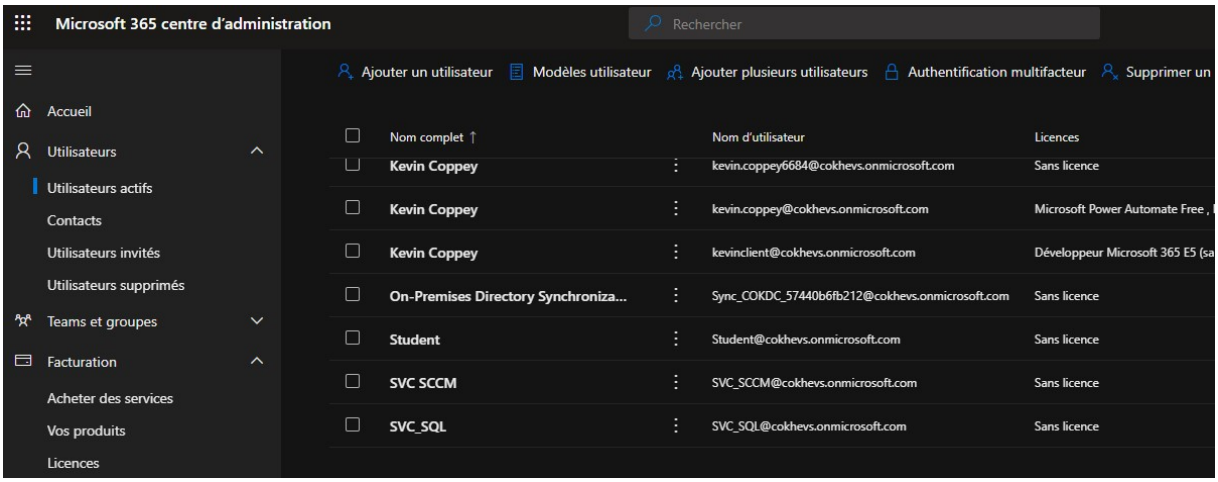
8) Lorsque l'installation est terminée, quitter l'installateur :

Figure 154 - Configuration complétée AD Connect
(Source : Auteur)



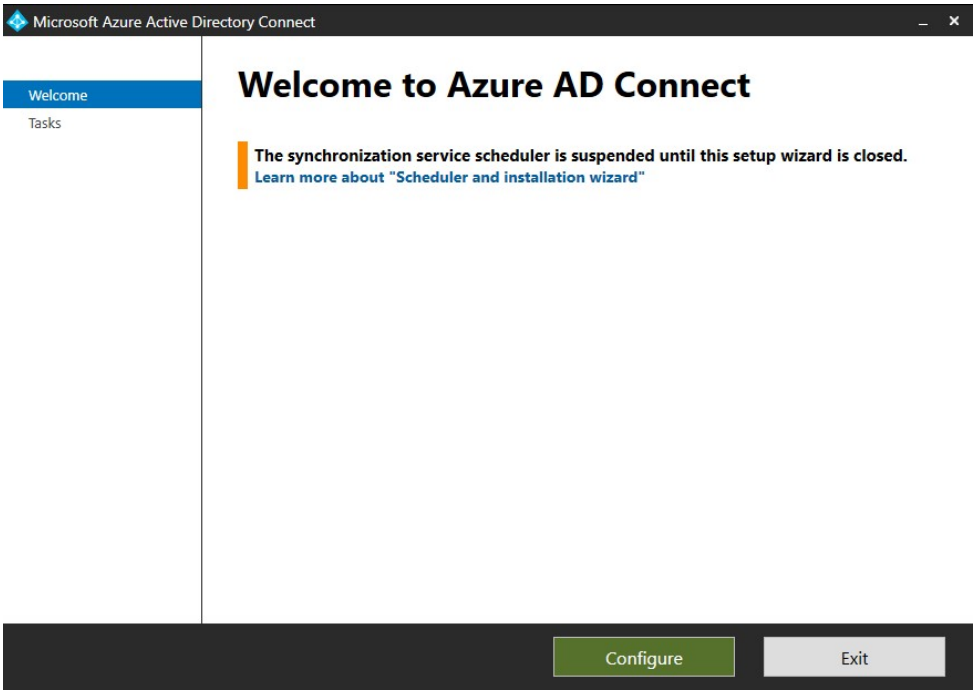
9) Vérifier que la synchronisation a bien eu lieu en consultant le centre d'administration Microsoft 365, sous « Utilisateur actifs » :

Figure 155 - Utilisateurs On-Premise synchronisé sur le Cloud
(Source : Auteur)



10) Relancer l'installateur de Azure AD Connect et cliquer sur « Configure » :

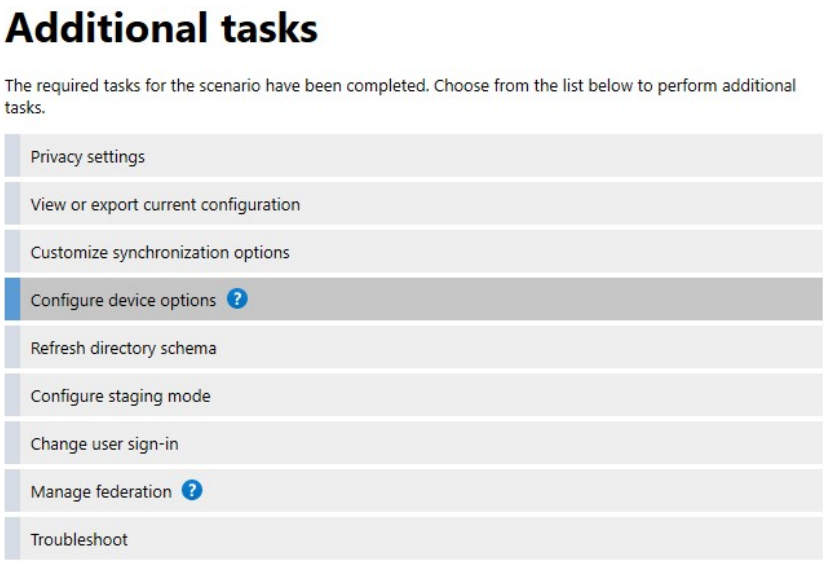
Figure 156 - Accueil après installation AD Connect
(Source : Auteur)



Nous passons maintenant à l'enrôlement de l'ensemble des machines présentes sur l'Active Directory.

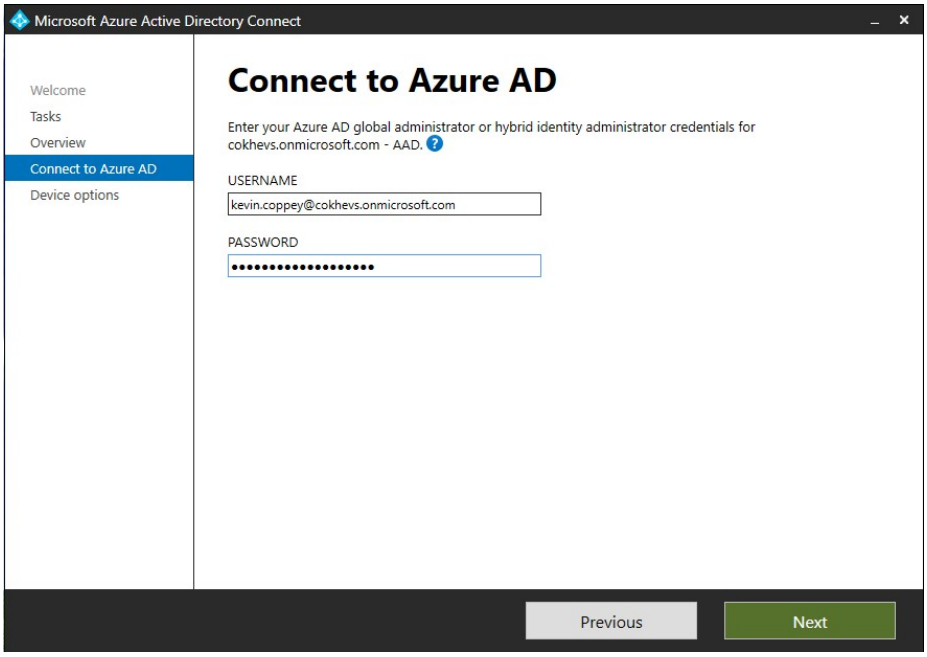
11) Sélectionner « Configure device options » :

Figure 157 - Tâches additionnels AD Connect
(Source : Auteur)



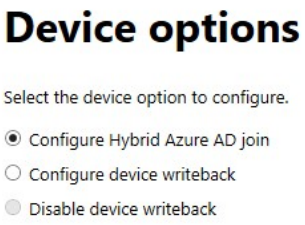
12) Entrer les identifiants administrateurs du tenant :

Figure 158 - Lien vers le tenant AD Connect 2
(Source : Auteur)



13) Sélectionner la première option et faire suivant :

Figure 159 - Options d'appareil
(Source : Auteur)

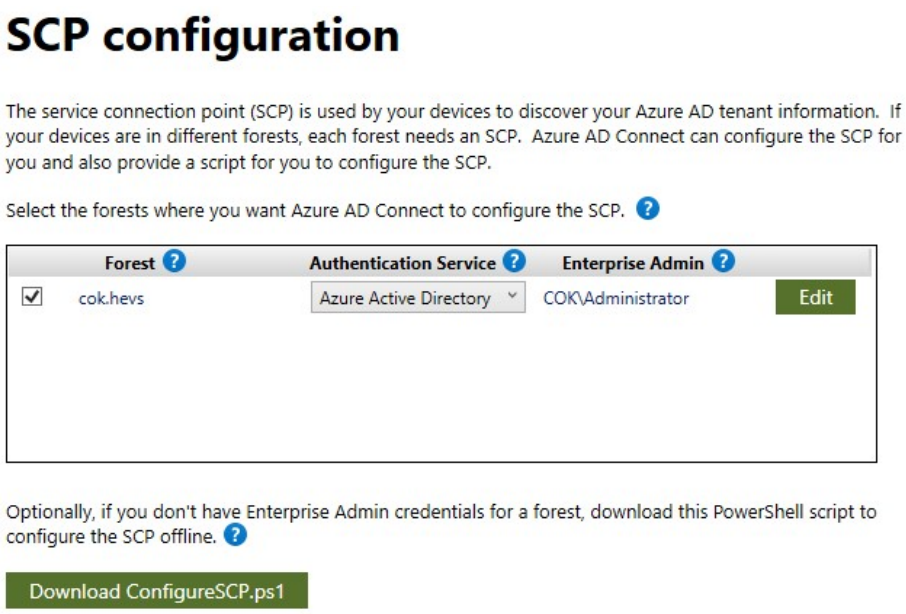


14) Choisir d'appliquer la stratégie sur les appareils Windows 10 et plus récent :

Figure 160 - Choix du système d'exploitation ciblé
(Source : Auteur)

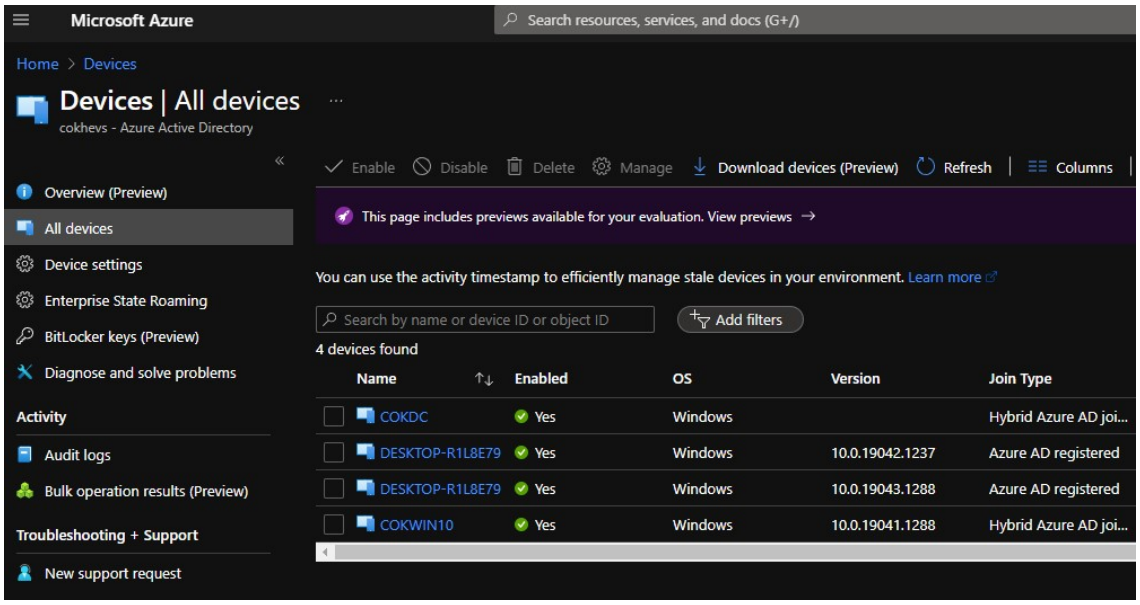
15) Sélectionner la forêt sur laquelle les appareils doivent être enrôlés et choisir Azure Active Directory en tant que service d'authentification. Cliquer sur le bouton « Add » et faire suivant :

Figure 161 - Configuration SCP
(Source : Auteur)



16) Vérifier maintenant qu'un appareil client de notre domaine Active Directory soit inscrit sur Azure AD :

Figure 162 - Machines On-Premise ajoutée
(Source : Auteur)



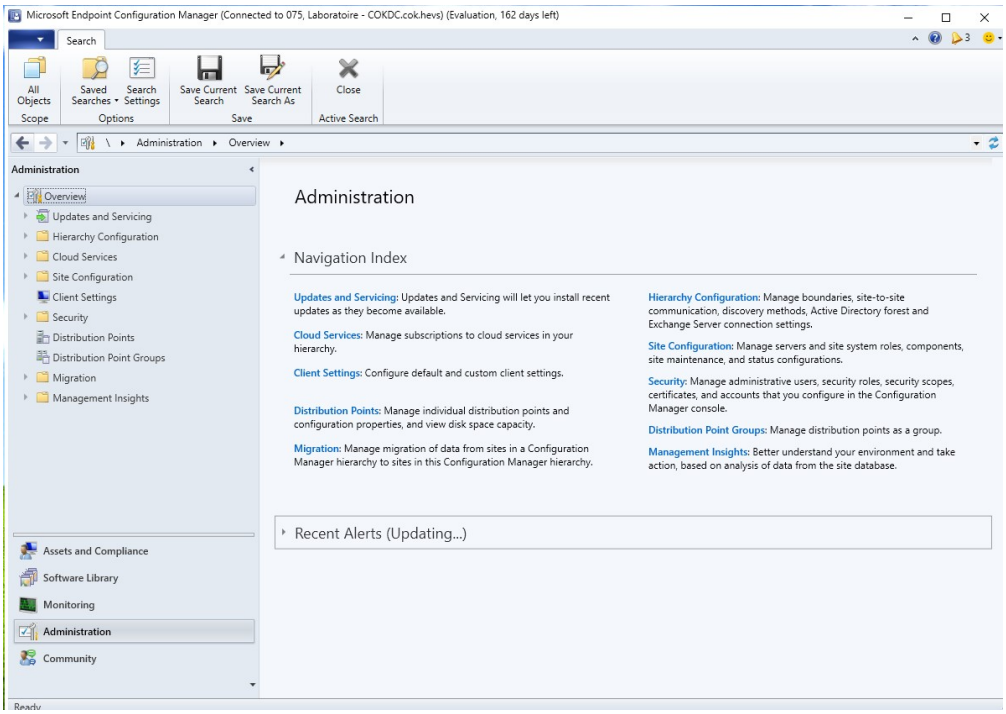
Nous remarquons que notre machine COKWIN10, qui est notre machine cliente, dans notre domaine AD On-Premise est apparu dans la liste des appareils gérables.

Configuration Manager

Nous passons maintenant sur la machine serveur pour configurer SCCM de sorte que l'ensemble de la charge de travail soit sur le Cloud.

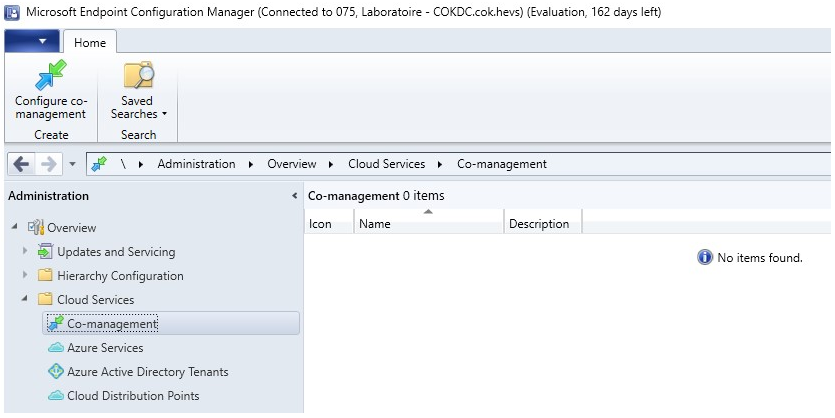
17) Lancer SCCM et se rentre dans l'espace de travail « Administration » :

Figure 163 - SCCM Ecran Administration
(Source : Auteur)



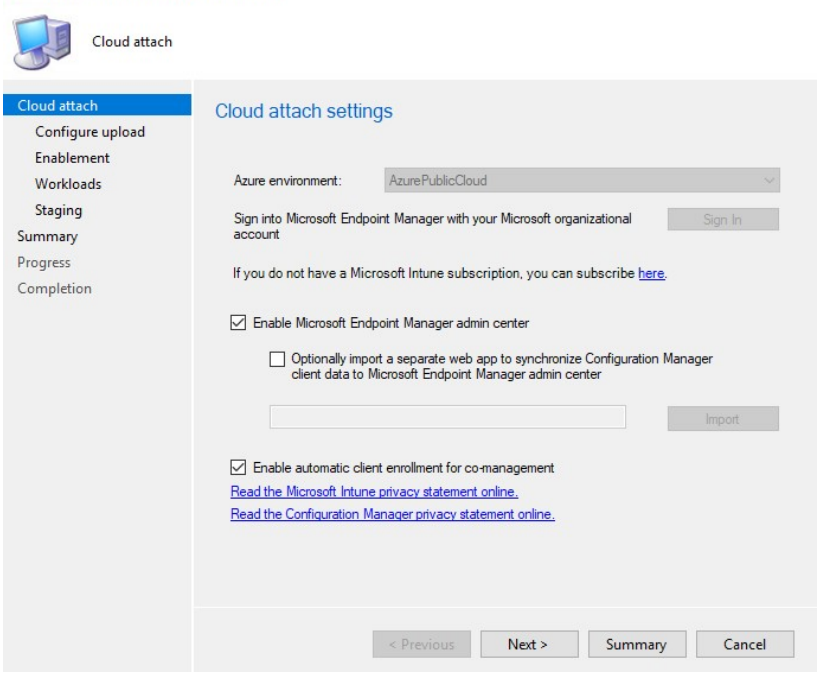
18) Etendre le dossier « Cloud services », sélectionner le nœud « Co-management » et cliquer sur « Configure Co-management » :

Figure 164 - SCCM onglet Co-management
(Source : Auteur)



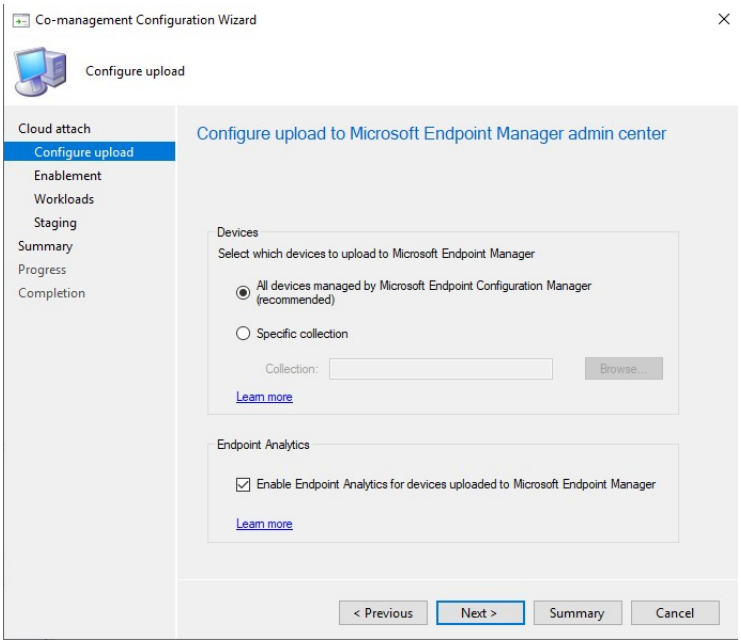
19) Remplir comme l'image suivante (Ne pas oublier de s'authentifier avec le bouton « Sign-in ») :

Figure 165 - Lien avec le tenant SCCM
(Source : Auteur)



20) Choisir de configurer le Co-management pour tous les appareils :

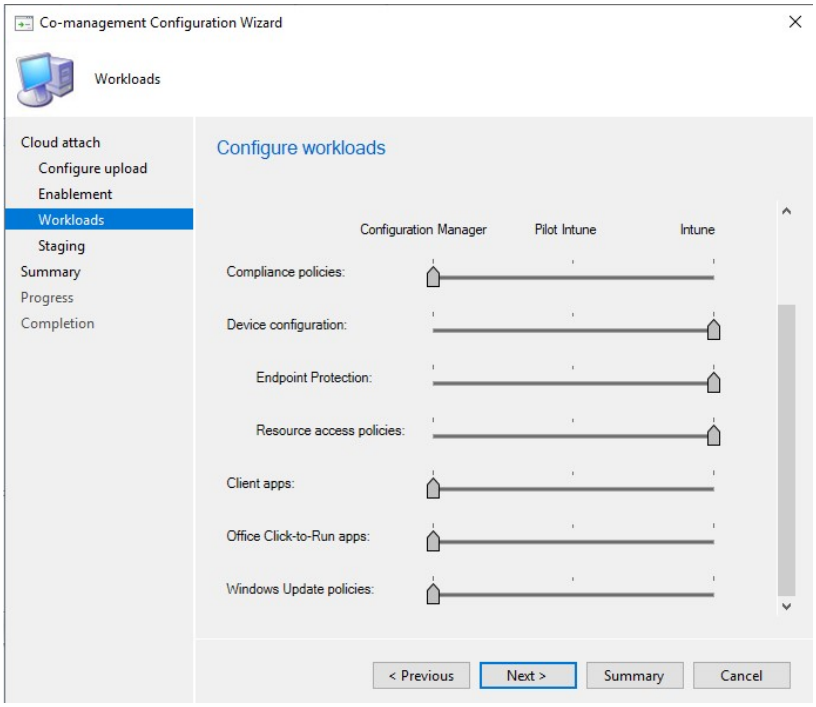
Figure 166 - Ajout des machines de SCCM sur MEM
(Source : Auteur)



21) Dans la fenêtre « Enablement », activer l'enrôlement automatique pour tous les appareils.

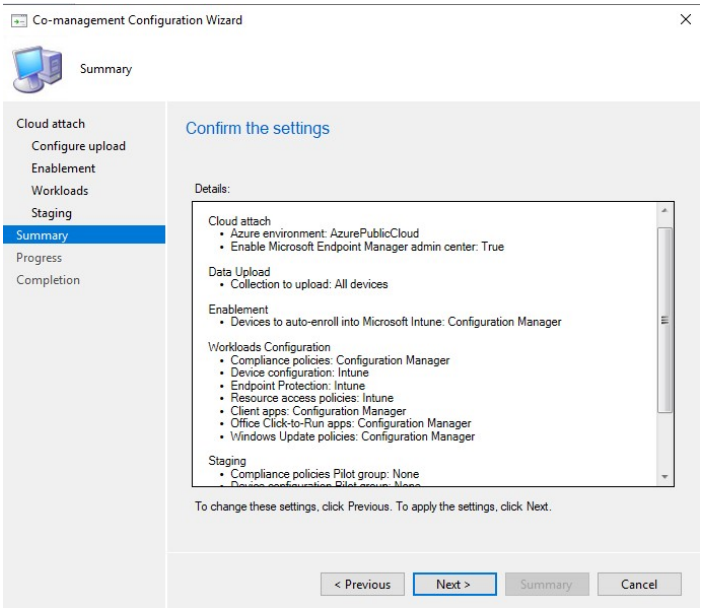
22) Dans la fenêtre « Workloads », basculer la gestion des paramètres « Device configuration », « Endpoint Protection » et « Resources access policies » vers Intune :

Figure 167 - Configuration de la charge de travail SCCM
(Source : Auteur)



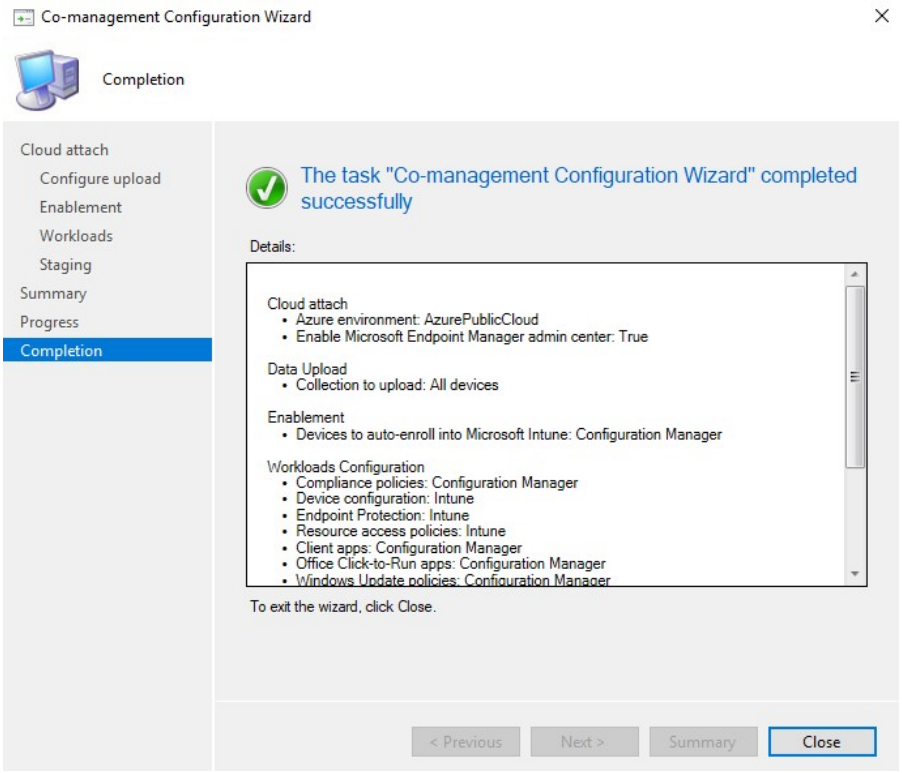
23) Dans l'écran du résumé de la configuration, faire suivant :

Figure 168 - Confirmation des paramètres de Co-management
(Source : Auteur)



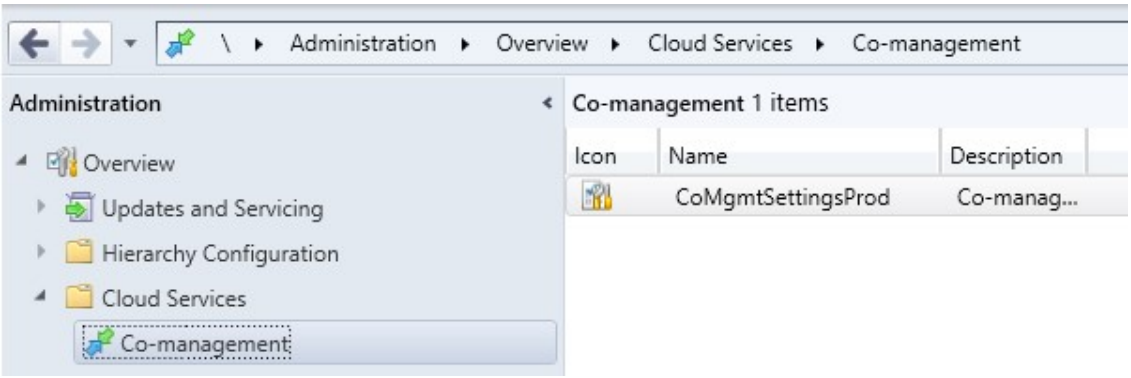
24) Vérifier que l'installation s'est correctement déroulée :

Figure 169 - Fin de la configuration Co-management
(Source : Auteur)



25) Une entrée de configuration de Co-Management apparaît :

Figure 170 - Ajout de la stratégie Co-management
(Source : Auteur)



L'ensemble de la charge de travail concernant la protection des points de terminaison et passée sur Intune. Il est dorénavant possible de supprimer le client SCCM. Cependant, nous ne recommandons pas de le faire, car ce logiciel est très utile pour plein d'autres tâches que celles en rapport avec la protection des clients.

Conclusion

Ce travail de Bachelor nous a permis de prendre connaissance des différentes solutions de sécurité native proposées par Microsoft. Nous avons confronté le lecteur a un choix entre une infrastructure sur site, sur le Cloud et dans un environnement hybride. Cette décision s'est articulée autour de plusieurs critères retenus qui nous ont permis finalement de valider notre hypothèse de recherche en retenant le Cloud.

Cette hypothèse a été formulée dans le but de répondre aux questions posées au tout début de ce travail. L'architecture Cloud s'est révélée optimale pour garantir une protection accrue en dehors et à l'intérieur d'un environnement professionnel dans le cas d'une start-up.

Bien qu'une solution Cloud fût privilégiée, un modèle hybride est également une bonne façon pour une entreprise d'avoir d'ores et déjà une présence sur le Cloud et de bénéficier de ses fonctionnalités. Ainsi, nous recommandons aux administrateurs, dans le cadre d'une migration vers le cloud, de garder leur infrastructure On-Premise et de la moderniser en optant pour une solution hybride. Cette hypothèse peut être considérée dans le but d'approfondir le sujet de ce travail.

Par l'utilisation de machines virtuelles, nous avons pu construire un laboratoire démontrant les fonctionnalités du Cloud. Cependant, à cause des limites techniques imposées par la virtualisation des composants, il n'a pas été possible de tester toutes les fonctionnalités. Par conséquent, en tant que perspectives de recherches ultérieures, nous proposons l'utilisation de machines physiques. De plus, la limite temporelle de 360 heures ne nous a pas permis de plus développer la partie application du document en présentant d'autres bonnes pratiques de sécurité.

Nous concluons ce document en invitant le lecteur à prendre conscience de la forte évolution des produits Microsoft. Les utilisateurs doivent se mettre au courant des dernières mises à jour et communications de la part de l'entreprise pour faire le meilleur choix d'infrastructure à un moment donné. En effet, il est probable qu'un jour Microsoft décide de proposer uniquement des solutions dans le Cloud, d'où l'importance pour les entreprises d'être prêtes à négocier ce virage en bénéficiant d'ores et déjà d'une présence sur le Cloud.

Références

Aggarwal, M. (2018). *Network Security with PfSense* (Packt Publishing éd.). Packt Publishing. Consulté le 10 octobre 2021, à l'adresse https://univ.scholarvox.com/catalog/book/docid/88861407

AV-Comparatives. (2020, 15 décembre). *Business Security Test 2020 (August - November)*. Consulté le 12 octobre 2021, à l'adresse https://www.av-comparatives.org/tests/business-security-test-2020-august-november/

Bastien L., B. L. (2017a, février 6). *PaaS Définition : Qu'est-ce que c'est ? Quels avantages ?* LeBigData.fr. Consulté le 11 octobre 2021, à l'adresse https://www.lebigdata.fr/definition-paas

Bastien L., B. L. (2017b, février 10). *Cloud Computing – Définition, Avantages et Exemples d'utilisation*. LeBigData.fr. Consulté le 5 octobre 2021, à l'adresse https://www.lebigdata.fr/definition-cloud-computing

Bastien L., B. L. (2017c, mai 31). *IaaS Définition : Qu'est-ce que c'est ? Quels avantages ?* LeBigData.fr. Consulté le 11 octobre 2021, à l'adresse https://www.lebigdata.fr/definition-iaas#Comment_fonctionne_une_IaaS

Bastien L., B. L. (2017d, octobre 2). *SaaS Définition : Qu'est-ce que c'est ? Quels avantages ?* LeBigData.fr. Consulté le 11 octobre 2021, à l'adresse https://www.lebigdata.fr/definition-saas

Belcic, I. (2021, 19 mai). *Présentation des rootkits et guide pour les supprimer*. Définition des rootkits : ce qu'ils font, comment ils fonctionnent et comment les supprimer. Consulté le 7 octobre 2021, à l'adresse https://www.avast.com/fr-fr/c-rootkit

Bilan. (2021, 19 avril). Le télétravail s'est répandu en 2020 en raison du coronavirus. *Bilan*. Consulté le 8 octobre 2021, à l'adresse https://www.bilan.ch/economie/le-teletravail-sest-repandu-en-2020-en-raison-du-coronavirus

Clayton, M. (2012, 23 juin). Stuxnet cyberweapon set to stop operating. *The Christian Science Monitor*. Consulté le 8 octobre 2021, à l'adresse https://www.csmonitor.com/USA/2012/0623/Stuxnet-cyberweapon-set-to-stop-operating

Desktop Operating System Market Share Worldwide | Statcounter Global Stats. (2021, septembre). StatCounter Global Stats. Consulté le 3 octobre 2021, à l'adresse https://gs.statcounter.com/os-market-share/desktop/worldwide

Dunkerley, M., & Tumbarello, M. (2020). *Mastering Windows Security and Hardening : Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats*. Packt Publishing. Consulté le 8 octobre 2021, à l'adresse https://univ.scholarvox.com/catalog/book/docid/88900516

Empey, C. (2018, août 15). *How to create a strong password*. Avast. Consulté le 6 octobre 2021, à l'adresse Consulté le 10 octobre 2021, à l'adresse https://blog.avast.com/strong-password-ideas

ESET. (2020). *Threat Report Q3 2020*. Consulté le 11 octobre 2021, à l'adresse https://www.welivesecurity.com/wp-content/uploads/2020/10/ESET_Threat_Report_Q32020.pdf

FBI. (2020, 25 mai). *Internet Fraud*. Federal Bureau of Investigation. Consulté le 6 octobre 2021, à l'adresse https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud

Futura Sciences. (s. d.). *Cloud computing : qu'est-ce que c'est ?* Futura. Consulté le 10 octobre 2021, à l'adresse https://www.futura-sciences.com/tech/definitions/informatique-cloud-computing-11573/

Gartner. (s. d.). *CrowdStrike vs McAfee vs Microsoft vs SentinelOne vs Sophos vs Trend Micro : Gartner Peer Insights 2021*. Consulté le 19 octobre 2021, à l'adresse https://www.gartner.com/reviews/market/endpoint-protection-platforms/compare/crowdstrike-vs-mcafee-vs-microsoft-vs-sentinelone-vs-sophos-vs-trend-micro

Identity Theft Resource Center. (2020, janvier). *2019 End-of-Year Data Breach Report*. Consulté le 8 octobre 2021, à l'adresse https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

IONOS. (2020, 20 octobre). *On-Premises : le modèle de licence pour les logiciels basés sur serveur*. IONOS Digitalguide. Consulté le 9 octobre 2021, à l'adresse https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-on-premises/

Jackson, K., & Goessling, S. (2018). *Architecting Cloud Computing Solutions : Build cloud strategies that align technology and economics while effectively managing risk*. Packt Publishing. Consulté le 8 octobre 2021, à l'adresse https://univ.scholarvox.com/catalog/book/docid/88856921?searchterm=Cloud%20computing

Jumelet, A., Quastana, S., Saulière, P., & Ourghanlian, B. (2013). Qu'est-ce qu'un TPM ? Dans *Sécurité et mobilité Windows 8 pour les utilisateurs nomades : UEFI, BitLocker et AppLocker, DirectAccess, VPN, SmartScreen, Windows Defender*. . . (p. 24-25). Eyrolles. Consulté le 9 octobre 2021, à l'adresse https://univ.scholarvox.com/catalog/book/docid/88813766?searchterm=TPM

Kaspersky. (2020). *Kaspersky Security Bulletin - 2020 Statistiques*. Consulté le 18 octobre 2021, à l'adresse https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

Know-how. (2020, 20 octobre). *On-Premises : le modèle de licence pour les logiciels basés sur serveur*. IONOS Digitalguide. Consulté le 5 octobre 2021, à l'adresse https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-on-premises/

Luxner, T. (2021, 15 mars). *Cloud Computing Trends : 2021 State of the Cloud Report*. Flexera Blog. Consulté le 11 octobre 2021, à l'adresse https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/

McFarland, S. (2021, 21 mai). *Security Best Practices for Your Windows 10 Computer*. Securicy. Consulté le 5 octobre 2021, à l'adresse https://www.securicy.com/blog/security-best-practices-hardening-windows-10/#password-manager

Microsoft. (s. d.-a). *Découvrir, puis configurer Windows Hello*. Consulté le 6 octobre 2021, à l'adresse https://support.microsoft.com/fr-fr/windows/d%C3%A9couvrir-puis-configurer-windows-hello-dae28983-8242-bb2a-d3d1-87c9d265a5f0

Microsoft. (s. d.-b). *Désactivez la protection antivirus Defender dans Sécurité Windows*. Consulté le 5 octobre 2021, à l'adresse https://support.microsoft.com/fr-fr/windows/d%C3%A9sactivez-la-protection-antivirus-defender-dans-s%C3%A9curit%C3%A9-windows-99e6004f-c54c-8509-773c-a4d776b77960

Microsoft. (s. d.-c). *EMET mitigations guidelines*. Consulté le 6 octobre 2021, à l'adresse https://support.microsoft.com/en-us/topic/emet-mitigations-guidelines-b529d543-2a81-7b5a-d529-84b30e1ecee0

Microsoft. (s. d.-d). *Isolation principale*. Consulté le 7 octobre 2021, à l'adresse https://support.microsoft.com/fr-fr/windows/isolation-principale-e30ed737-17d8-42f3-a2a9-87521df09b78

Microsoft. (s. d.-e). *Protéger mon PC avec Microsoft Defender hors ligne*. Consulté le 9 novembre 2021, à l'adresse https://support.microsoft.com/fr-fr/windows/prot%C3%A9ger-mon-pc-avec-microsoft-defender-hors-ligne-9306d528-64bf-4668-5b80-ff533f183d6c

Microsoft. (s. d.-f). *Rester protégé avec Sécurité Windows*. Consulté le 5 octobre 2021, à l'adresse https://support.microsoft.com/fr-fr/windows/rester-prot%C3%A9g%C3%A9-avec-s%C3%A9curit%C3%A9-windows-2ae0363d-0ada-c064-8b56-6a39afb6a963

Microsoft. (2015, 12 mars). *Active Directory Maximum Limits Scalability Capacity*. Microsoft Docs. Consulté le 9 novembre 2021, à l'adresse https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc756101(v=ws.10)

Microsoft. (2018, 26 janvier). *BitLocker (Windows 10) - Windows security*. Microsoft Docs. Consulté le 11 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

Microsoft. (2019a, février 28). *BitLocker Management Recommendations for Enterprises (Windows 10) - Windows security*. Microsoft Docs. Consulté le 11 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-management-for-enterprises

Microsoft. (2019b, mars 1). *Comment une Windows Defender System Guard contribue à protéger les Windows 10 - Windows security*. Microsoft Docs. Consulté le 7 octobre 2021, à l'adresse https://docs.microsoft.com/fr-ch/windows/security/threat-protection/windows-defender-system-guard/how-hardware-based-root-of-trust-helps-protect-windows

Microsoft. (2019c, juillet 29). *Démarrage sécurisé*. Microsoft Docs. Consulté le 7 octobre 2021, à l'adresse https://docs.microsoft.com/fr-ch/windows-hardware/design/device-experiences/oem-secure-boot

Microsoft. (2019d, septembre 9). *Verrouillage dynamique - Microsoft 365 Security*. Microsoft Docs. Consulté le 6 octobre 2021, à l'adresse https://docs.microsoft.com/fr-fr/windows/security/identity-protection/hello-for-business/hello-feature-dynamic-lock

Microsoft. (2021a, mars 30). *New Security Signals study shows firmware attacks on the rise ; here's how Microsoft is working to help eliminate this entire class of threats*. Microsoft Security Blog. Consulté le 7 octobre 2021, à l'adresse https://www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/

Microsoft. (2021b, avril 16). *Windows for Business Update settings for Microsoft Intune*. Https://Docs.Microsoft.Com/En-Us/Mem/Intune/Protect/Windows-Update-Settings. Consulté le 11 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-settings

Microsoft. (2021c, juillet 14). *What is Azure Active Directory ? - Azure Active Directory*. Microsoft Docs. Consulté le 14 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Microsoft. (2021d, juillet 23). *Setup guide for Microsoft Intune*. Microsoft Docs. Consulté le 10 novembre 2021, à l'adresse https://docs.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-intune-setup#currently-use-on-premises-group-policy

Microsoft. (2021e, août 9). *Encrypt Windows devices with BitLocker in Intune - Microsoft Intune*. Microsoft Docs. Consulté le 12 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices#silently-enable-bitlocker-on-devices

Microsoft. (2021f, août 13). *Cogestion pour les appareils Windows 10 - Configuration Manager*. Microsoft Docs. Consulté le 17 octobre 2021, à l'adresse https://docs.microsoft.com/fr-ch/mem/configmgr/comanage/overview

Microsoft. (2021g, août 21). *Qu'est-ce que Microsoft Intune*. Microsoft Docs. Consulté le 15 octobre 2021, à l'adresse https://docs.microsoft.com/fr-ch/mem/intune/fundamentals/what-is-intune

Microsoft. (2021h, septembre 15). *Microsoft Defender SmartScreen vue d'ensemble (Windows) - Windows security*. Microsoft Docs. Consulté le 6 octobre 2021, à l'adresse https://docs.microsoft.com/fr-ch/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview

Microsoft. (2021i, septembre 17). *Endpoint Protection - Configuration Manager*. Microsoft Docs. Consulté le 14 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/endpoint-protection

Microsoft. (2021j, septembre 17). *How to manage Windows Defender Application Control - Configuration Manager*. Microsoft Docs. Consulté le 14 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager

Microsoft. (2021k, septembre 17). *Size and scale - Configuration Manager*. Microsoft Docs. Consulté le 9 novembre 2021, à l'adresse https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/size-and-scale-numbers#bkmk_clientnumbers

Microsoft. (2021l, septembre 17). *What is Configuration Manager ? - Configuration Manager*. Microsoft Docs. Consulté le 14 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/mem/configmgr/core/understand/introduction

Microsoft. (2021m, septembre 20). *Windows Hello for Business Overview (Windows) - Windows security*. Microsoft Docs. Consulté le 9 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

Microsoft. (2021n, septembre 24). *Use group policy analytics to import GPOs in Microsoft Intune*. Microsoft Docs. Consulté le 10 novembre 2021, à l'adresse https://docs.microsoft.com/en-us/mem/intune/configuration/group-policy-analytics

Microsoft. (2021o, septembre 26). *Vue d'ensemble de la technologie du Module de plateforme sécurisée (TPM) (Windows) - Microsoft 365 Security*. Microsoft Docs. Consulté le 7 octobre 2021, à l'adresse https://docs.microsoft.com/fr-ch/windows/security/information-protection/tpm/trusted-platform-module-overview

Microsoft. (2021p, septembre 30). *Windows sécurité matérielle - Microsoft 365 Security*. Microsoft Docs. Consulté le 7 octobre 2021, à l'adresse https://docs.microsoft.com/fr-fr/windows/security/hardware

Microsoft. (2021q, octobre 6). *Microsoft Defender for Endpoint*. Microsoft Docs. Consulté le 15 octobre 2021, à l'adresse https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide

Microsoft. (2021r, octobre 7). *Détections en temps réel et de l'Explorateur de menaces - Office 365*. Microsoft Docs. Consulté le 15 octobre 2021, à l'adresse https://docs.microsoft.com/fr-fr/microsoft-365/security/office-365-security/threat-explorer?view=o365-worldwide

Microsoft. (2021s, octobre 27). *Surveiller la co-gestion - Configuration Manager*. Microsoft Docs. Consulté le 30 octobre 2021, à l'adresse https://docs.microsoft.com/fr-ch/mem/configmgr/comanage/how-to-monitor

Microsoft. (2021t, novembre 2). *Manage antivirus settings with endpoint security policies in Microsoft Intune*. Microsoft Docs. Consulté le 10 novembre 2021, à l'adresse https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-antivirus-policy

Morris, G. (2021, 15 juin). *The Ultimate Guide to Microsoft Defender for Endpoint Protection (2021)*. Datalink Networks, Inc. Consulté le 15 octobre 2021, à l'adresse https://www.datalinknetworks.net/dln_blog/the-ultimate-guide-to-microsoft-defender-for-endpoint-protection

Poll, H. & Google. (2019, octobre). *The United States of P@$w0rd$*. Consulté le 8 novembre 2021, à l'adresse https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

Redhat. (s. d.). *Quelle est la différence entre un cloud public, privé et hybride ?* Redhat.com. Consulté le 11 octobre 2021, à l'adresse https://www.redhat.com/fr/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud

RedHat. (2020, 25 novembre). *Une CVE, qu'est-ce que c'est ?* Redhat.com. Consulté le 11 octobre 2021, à l'adresse https://www.redhat.com/fr/topics/security/what-is-cve

Rosenthal, M. (2021, 16 septembre). *Must-Know Phishing Statistics : Updated 2021*. Tessian. Consulté le 6 octobre 2021, à l'adresse https://www.tessian.com/blog/phishing-statistics-2020/

Rubenstein, B. (2020, 23 octobre). *Microsoft System Center Configuration Manager (SCCM)*. SearchWindowsServer. Consulté le 14 octobre 2021, à l'adresse https://searchwindowsserver.techtarget.com/definition/Microsoft-System-Center-Configuration-Manager-2012

Savill, J. (2016, août 30). *What is Credential Guard*. IT Pro. Consulté le 13 octobre 2021, à l'adresse https://www.itprotoday.com/windows-10/what-credential-guard

Saxton, A. (2015, 9 mars). *What is a Tenant ? | Microsoft Power BI Blog | Microsoft Power BI*. Microsoft PowerBI. Consulté le 14 octobre 2021, à l'adresse https://powerbi.microsoft.com/fr-fr/blog/what-is-a-tenant/

Sophos. (2021, avril). *The State of Ransomware 2021* (No 2096520). Consulté le 8 novembre 2021, à l'adresse https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

Spiceworks Ziff Davis. (2021). Consulté le 7 novembre 2021 *https://swzd.com/resources/state-of-it/?utm_source=swemail&utm_medium=email&utm_campaign=stateofit2021&content=blog*. https://swzd.com/resources/state-of-it/?utm_source=swemail&utm_medium=email&utm_campaign=stateofit2021&content=blog

Thurrott, P. (2006, 24 octobre). *Finally, Microsoft Ships Windows Defender*. Itprotoday. Consulté le 5 octobre 2021, à l'adresse http://archive.wikiwix.com/cache/index2.php?url=http%3A%2F%2Fwww.windowsitpro.com%2FArticle%2FArticleID%2F93991%2F93991.html

Toroman, M. (2018). *Hands-On Cloud Administration in Azure*. Van Haren Publishing. Consulté le 28 2021, à l'adresse https://univ.scholarvox.com/catalog/book/docid/88865345?searchterm=Azure%20Active%20Directory

van der Woude, P. (2021, 12 avril). *Working with Exploit Protection to protect devices from being exploited*. All about Microsoft Endpoint Manager. Consulté le 6 octobre 2021, à l'adresse https://www.petervanderwoude.nl/post/working-with-exploit-protection-to-protect-devices-from-being-exploited/

Webber, P., Firstbrook, P., Smith, R., Harris, M., & Bhajanka, P. (2021, mai). *Magic Quadrant for Endpoint Protection Platforms*. Consulté le 2 novembre 2021, à l'adresse https://www.gartner.com/doc/reprints?id=1-2435Z2CX&ct=200903&st=sb

Windows 10 Famille (Version 21H1). (2021). [Système d'exploitation]. Microsoft. https://www.microsoft.com/fr-ch

Annexe I : Guide pour obtenir la licence Microsoft 365 Developer avec un compte HES-SO AAI (Source : Auteur)

Guide to get the Microsoft 365 Developer license with AAI account at HES-SO

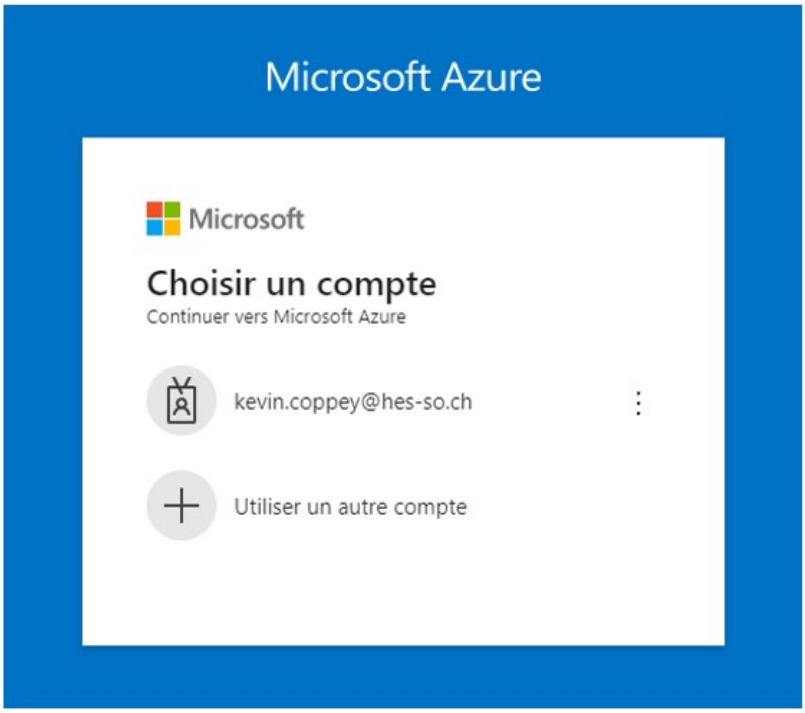
Table of contents

Introduction

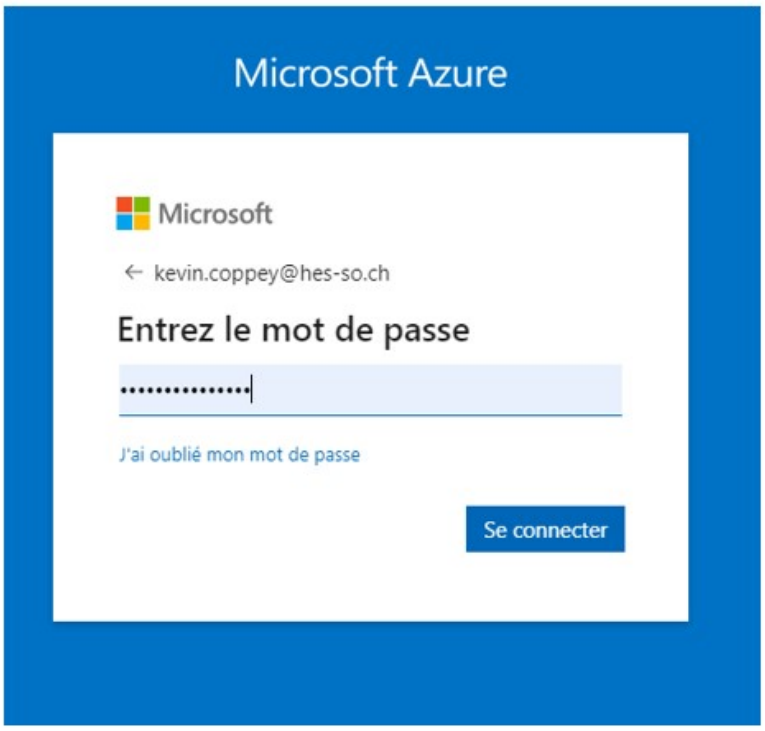
This guide has been created in order to get the possibility to use Microsoft Azure products as part of the bachelor's thesis: "Microsoft Security".

Configuration

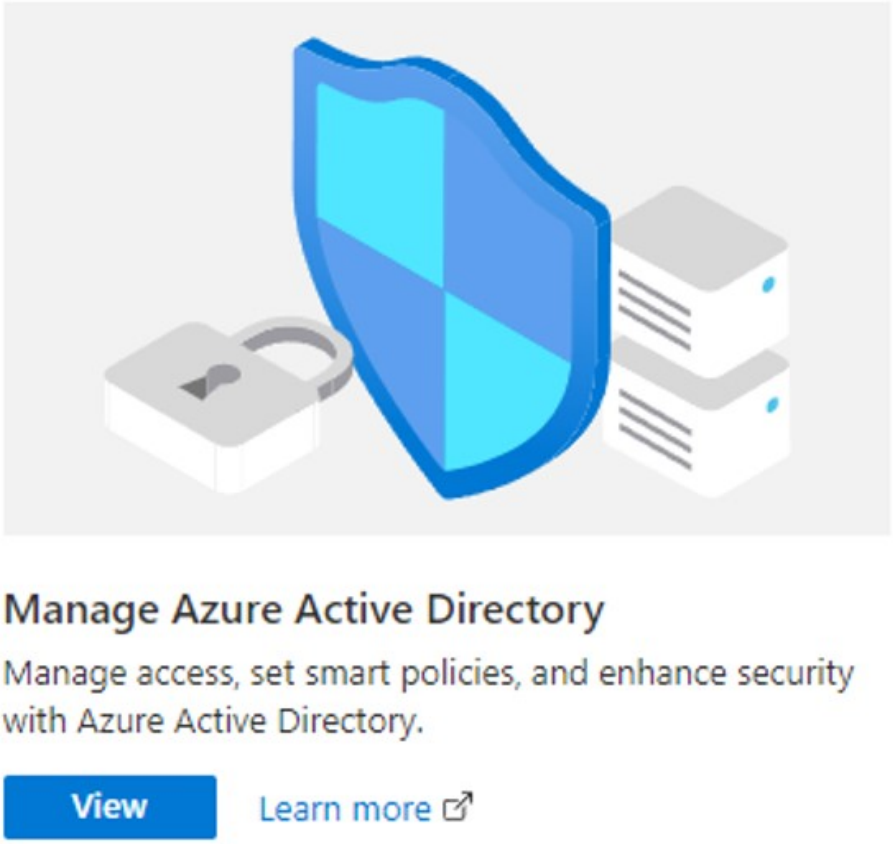
1) Go to portal.azure.com:



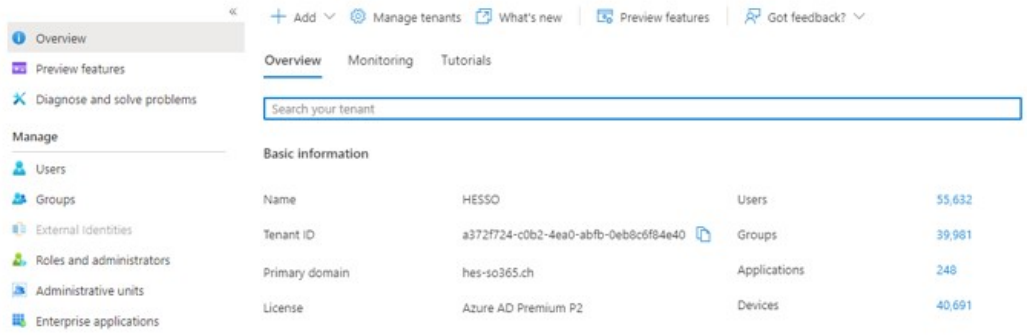
2) Sign in with AAI account:



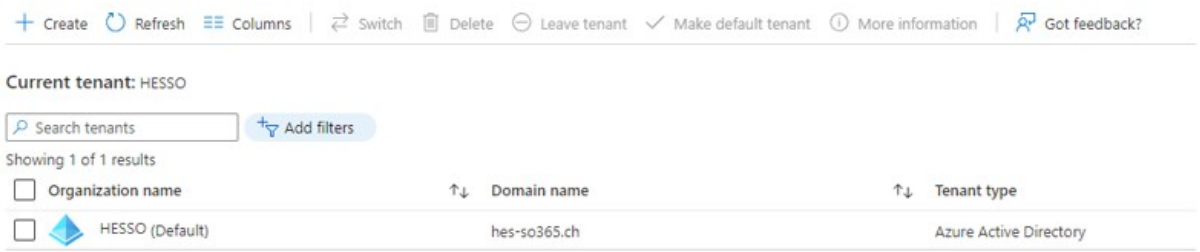
3) On the home page, click on button “View” in the “Manage Azure Active Directory”:



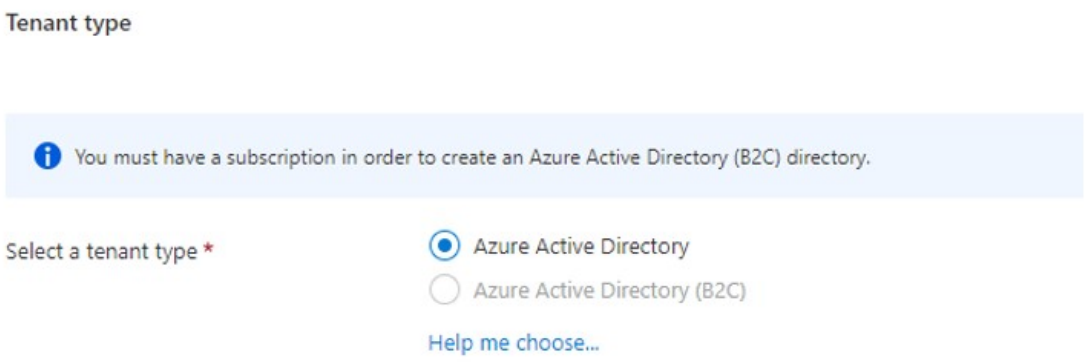
4) At the top of the Active Directory home page, click on “Manage tenants”:



5) Create a new tenant by clicking “Create”:

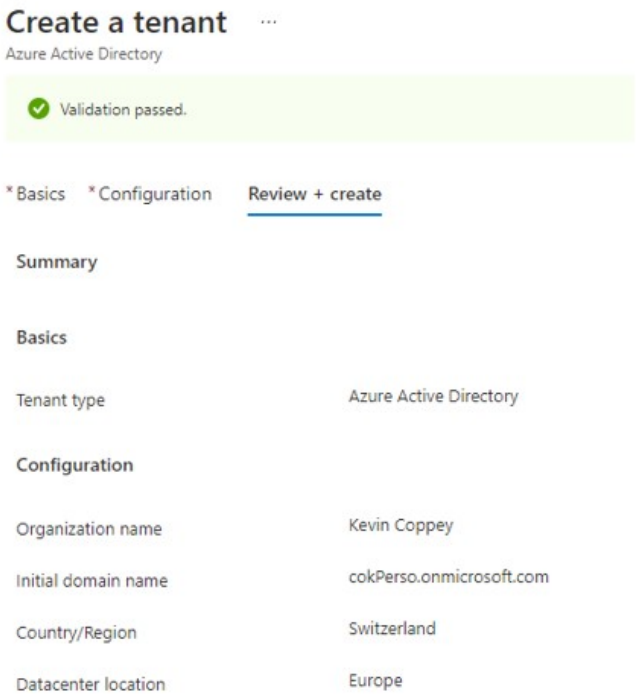


6) Choose Azure Active Directory as tenant type:

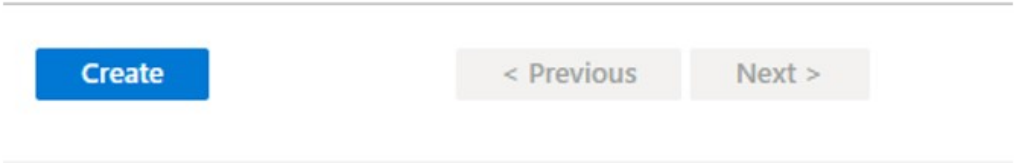


7) Configure the tenant as the following:

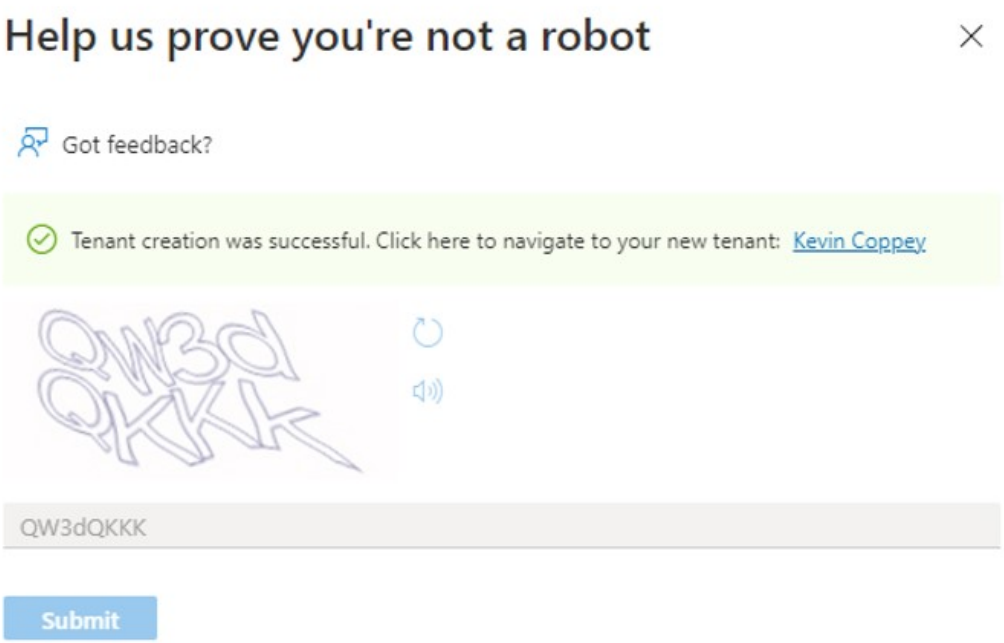
8) If everything went well, you should have the following screen:



9) Click on create at the bottom of the page:

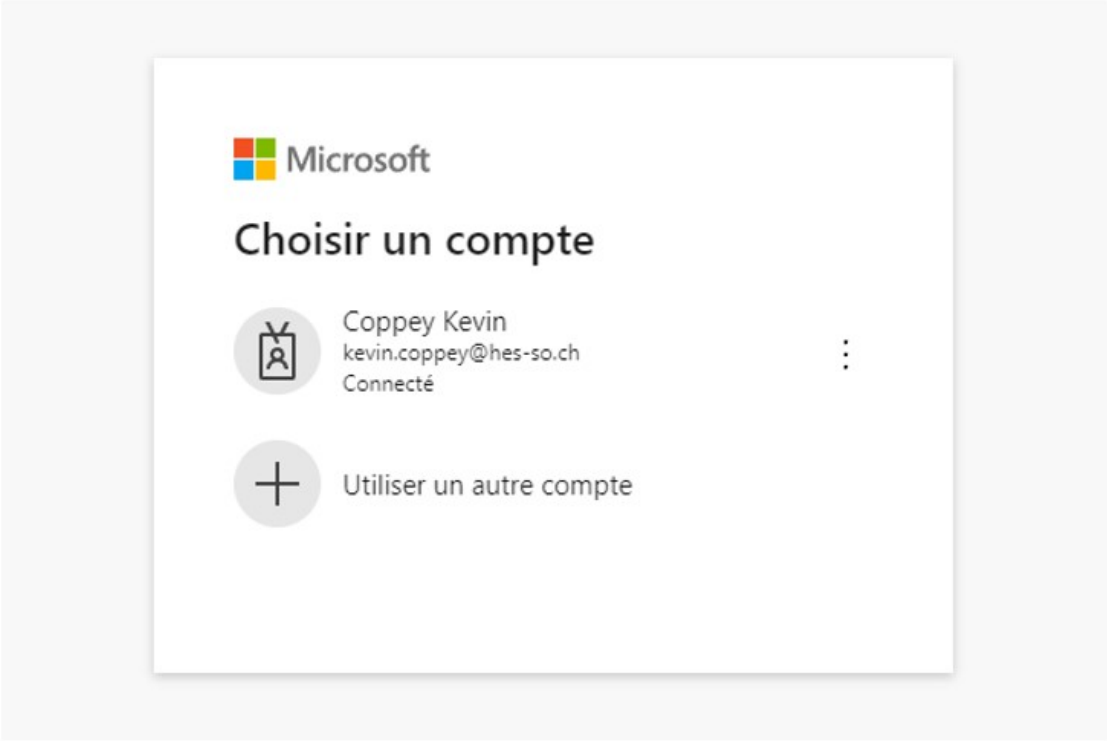


10) Wait a moment until you have a green message accepting the creation of the tenant. Then click on the name of your organization (underlined in blue):

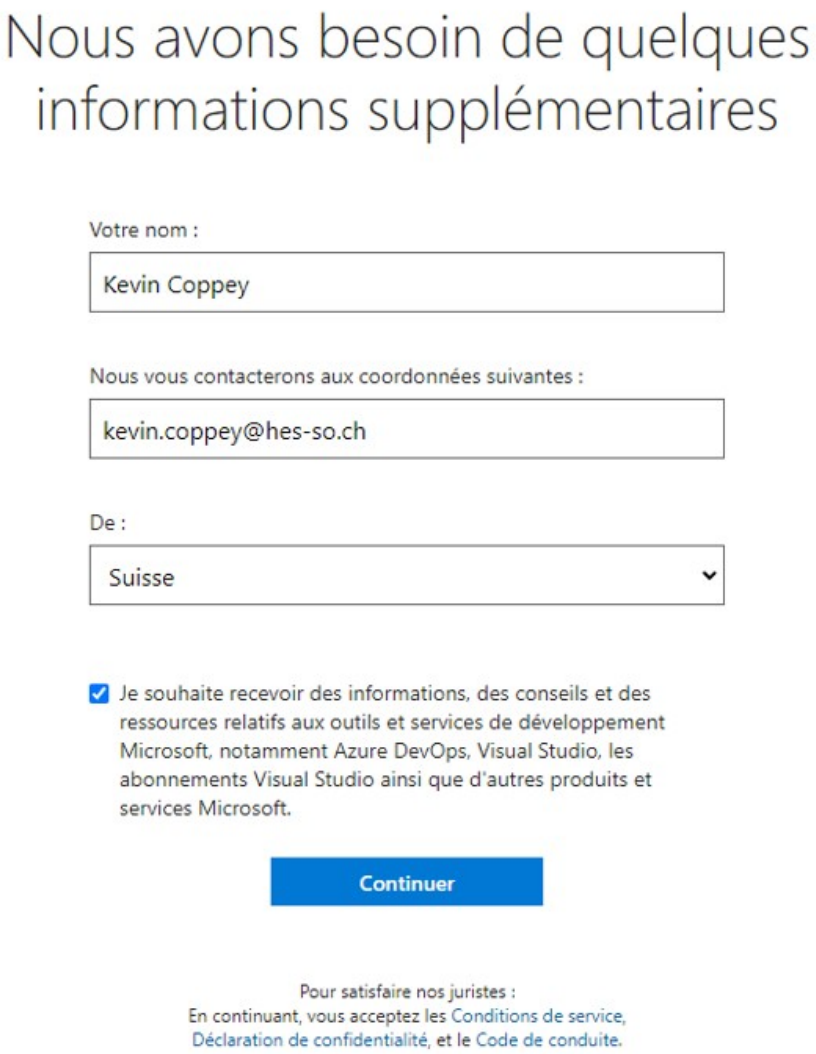


11) Go to my.visualstudio.com.

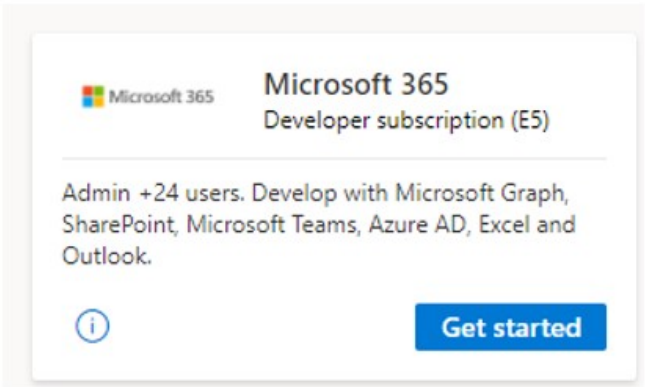
12) Sign in:



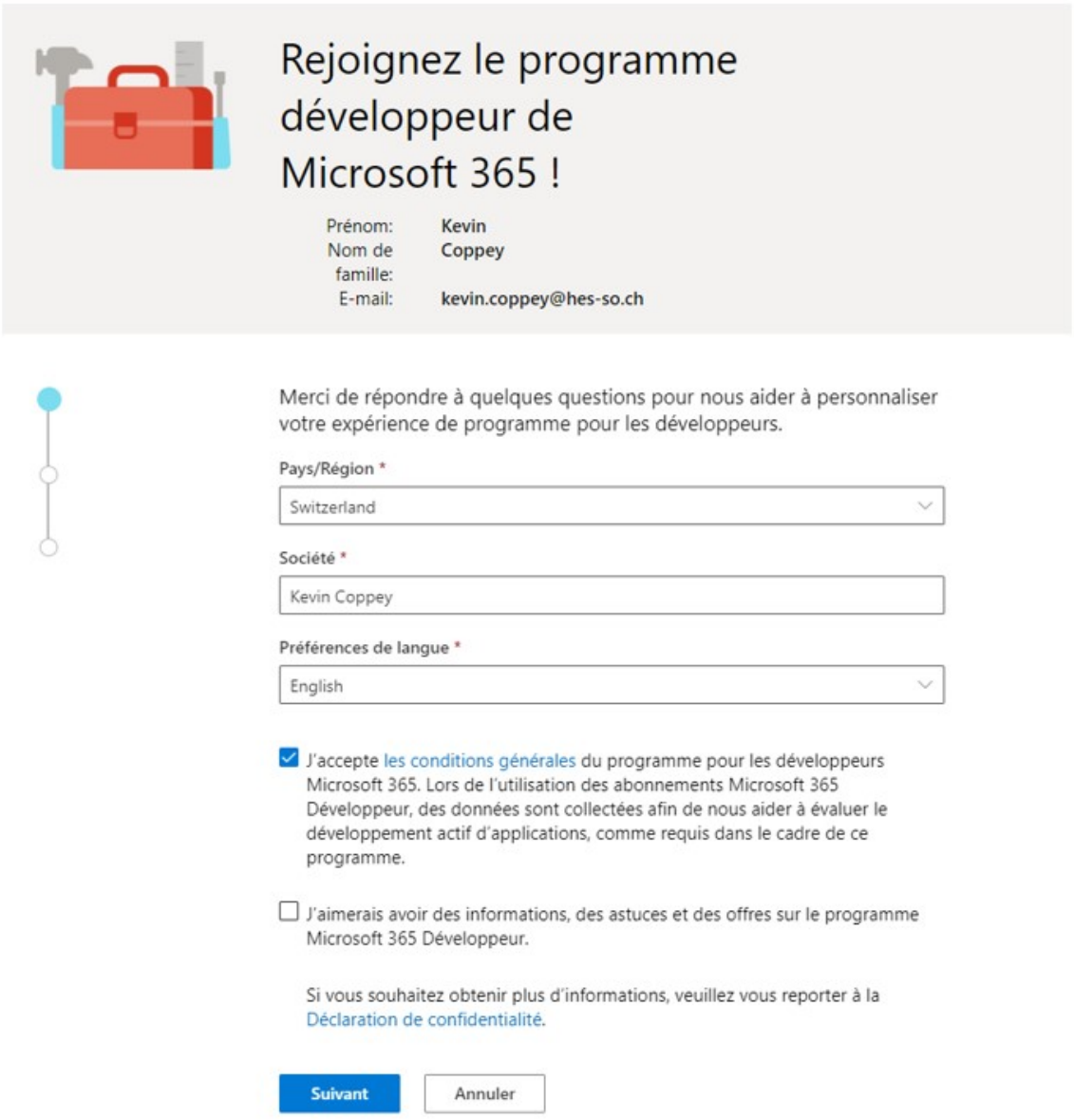
13) Fill in the form:



14) Click on “Get started” of the Microsoft 365 (E5) product:



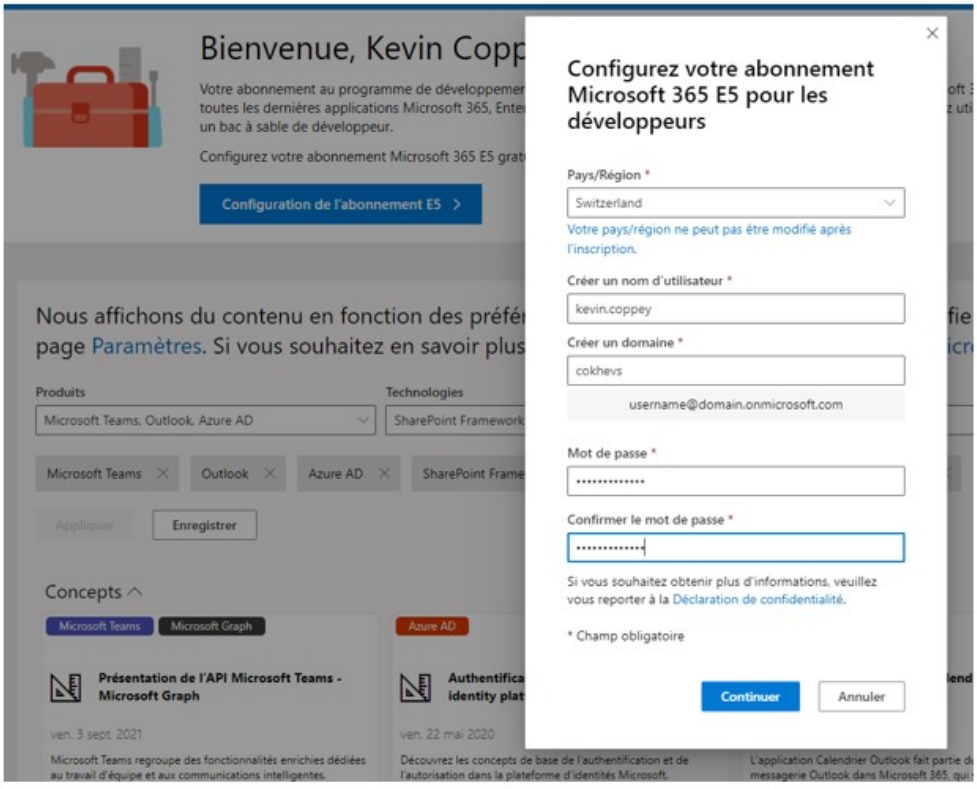
15) Fill in the following form:



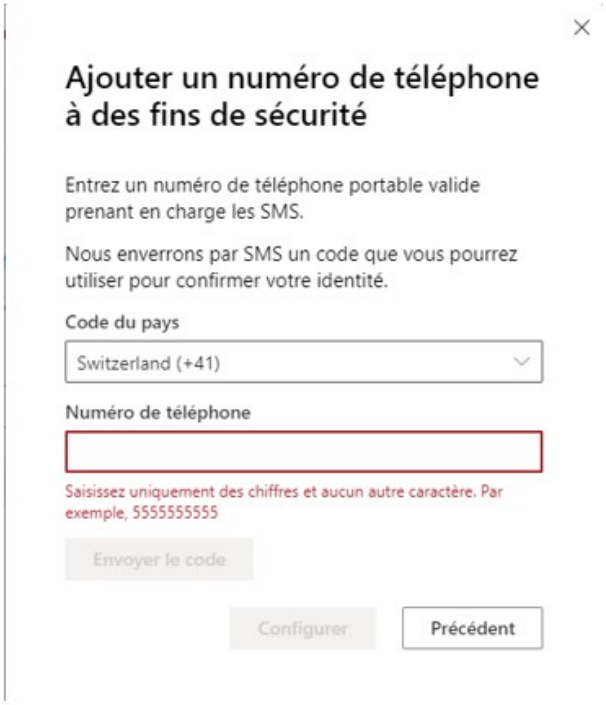
16) Answer as the following:

17) Choose every option of the list:

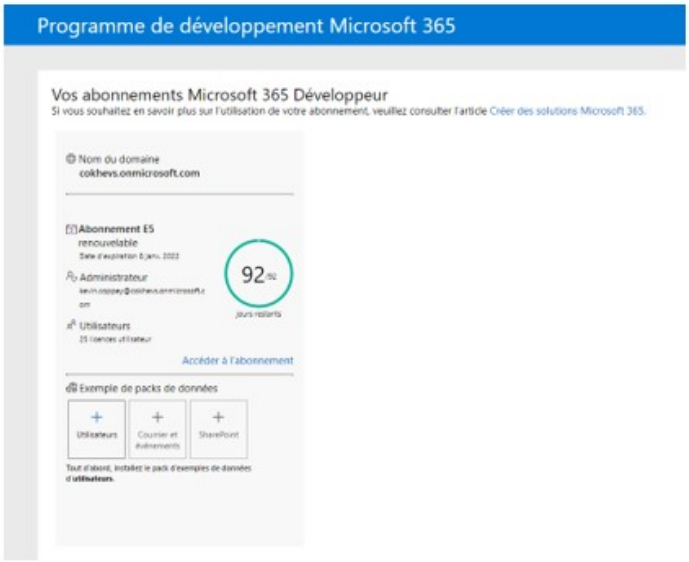
18) On this new page click on “Configuration de abonnement E5” and fill in the form :



19) Add your mobile phone for security purposes:



20) If everything went well, you will be on this page:



You should now be able to connect and use every Microsoft 365 Developer product with your tenant!

Annexe II : Guide de création d'un nouvel utilisateur et d'enrôlement d'une machine sur Intune (Source : Auteur)

Guide pour créer un compte utilisateur et enrôler sa machine sur Intune

Table des matières

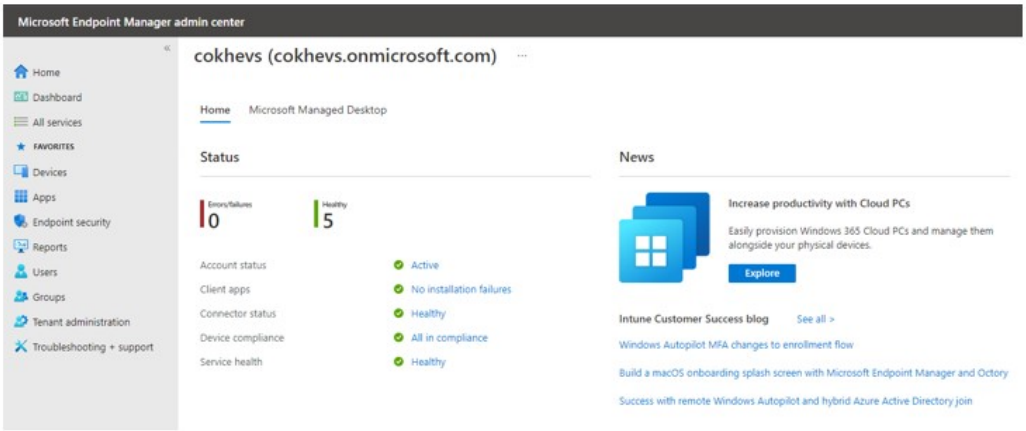
Introduction

Ce guide a été crée dans le but d'ajouter un utilisateur puis la machine sur laquelle il travaille afin de pouvoir la contrôler via le Cloud. Ce guide est réalisé dans le cadre du travail de Bachelor : « Microsoft Security ».

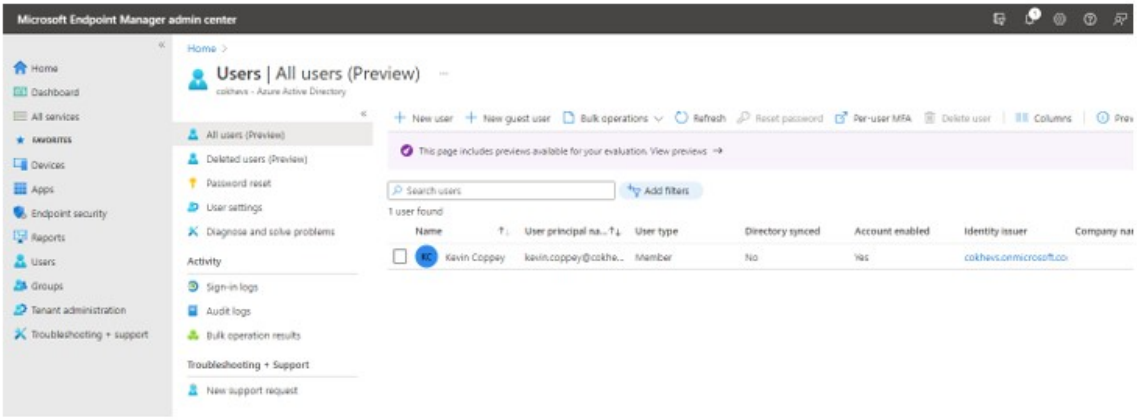
Configuration

La première étape est de créer un utilisateur qui correspond au compte d'un employé dans notre organisation fictive. Tout cela se fait via « Microsoft Azure Active Directory », cependant le service « Microsoft Endpoint Manager Admin Center » permet de le faire sans changer d'application.

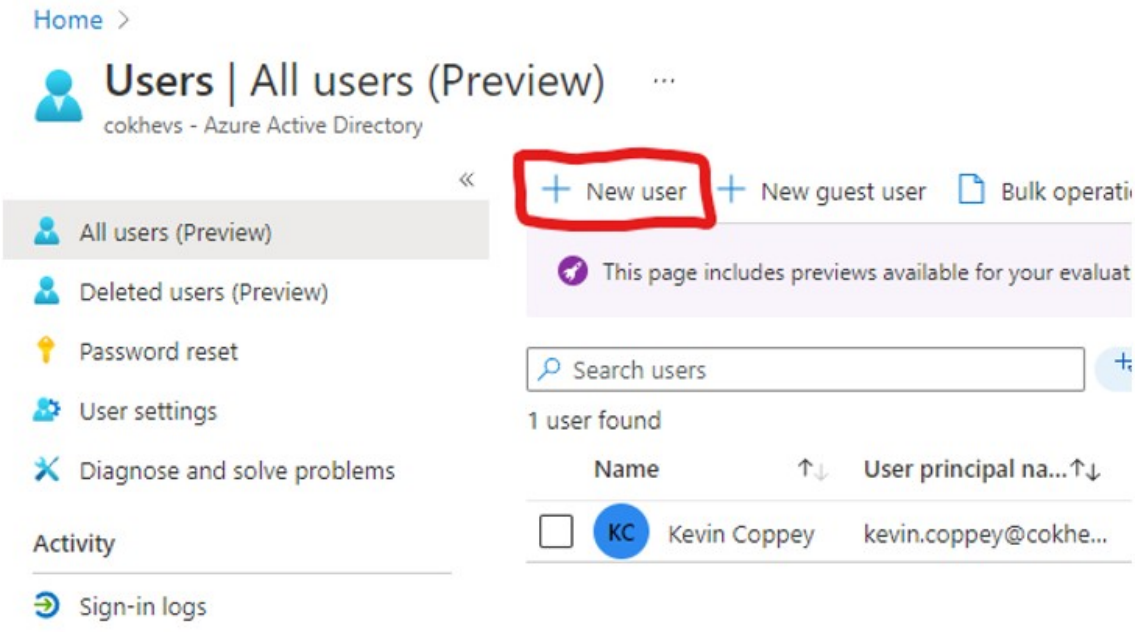
1) Se connecter sur Microsoft Endpoint Manager : https://devicemanagement.microsoft.com



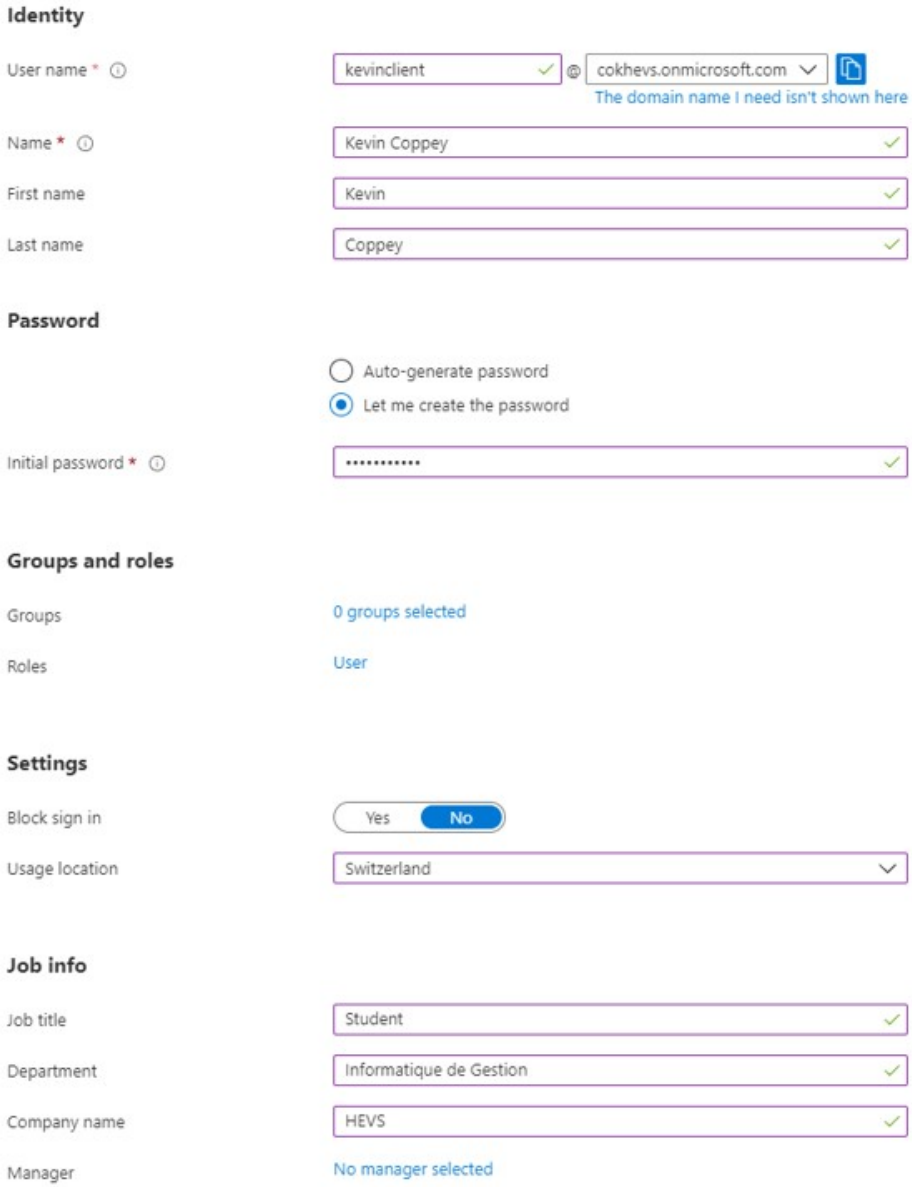
2) Se rendre sous « Users » dans le menu de droite :



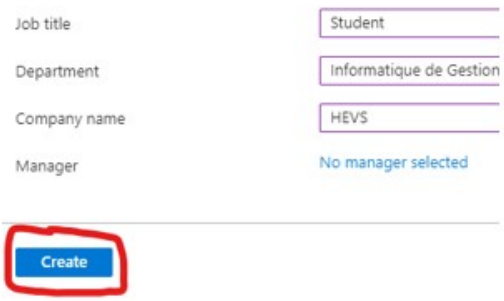
3) Ajouter un nouvel utilisateur en cliquer sur « New User » dans la barre d'outils du haut de l'application :



4) Remplir selon les informations suivantes :

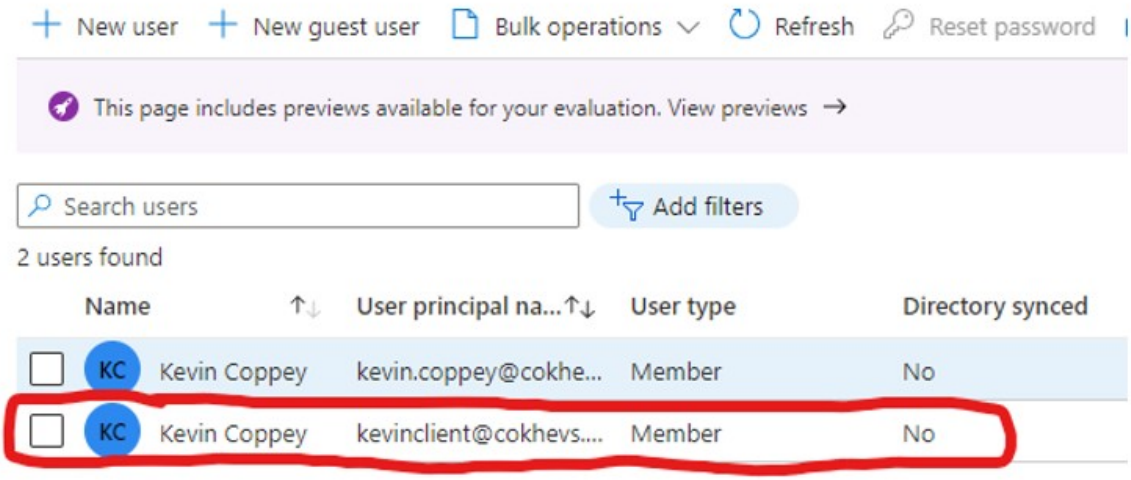


5) Cliquer sur le bouton « Create » situé en bas de la page :

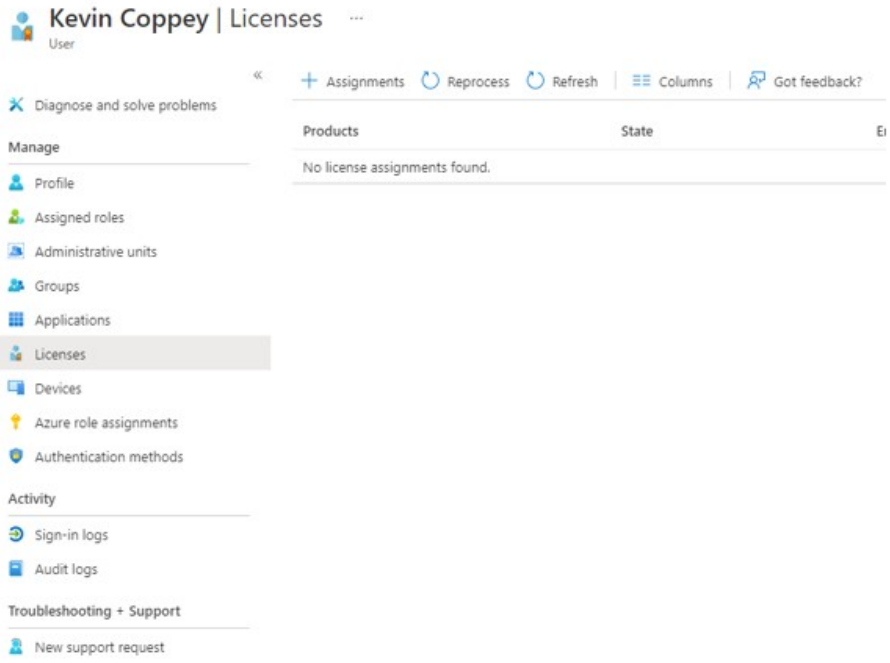


Nous possédons maintenant un nouvel employé dans notre organisation fictive. Nous devons lui accorder les permissions de licence lui permettant de se connecter au domaine via son point de terminaison.

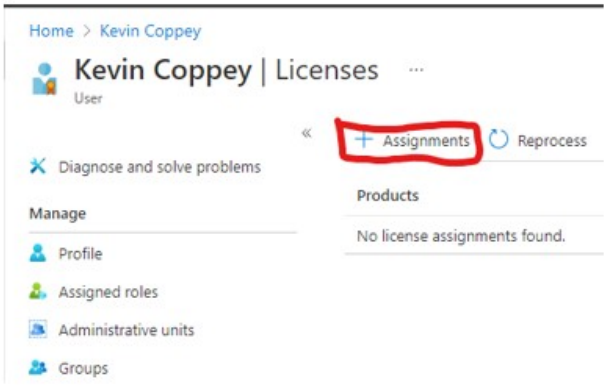
6) Cliquer sur le nouveau profil tout juste crée :



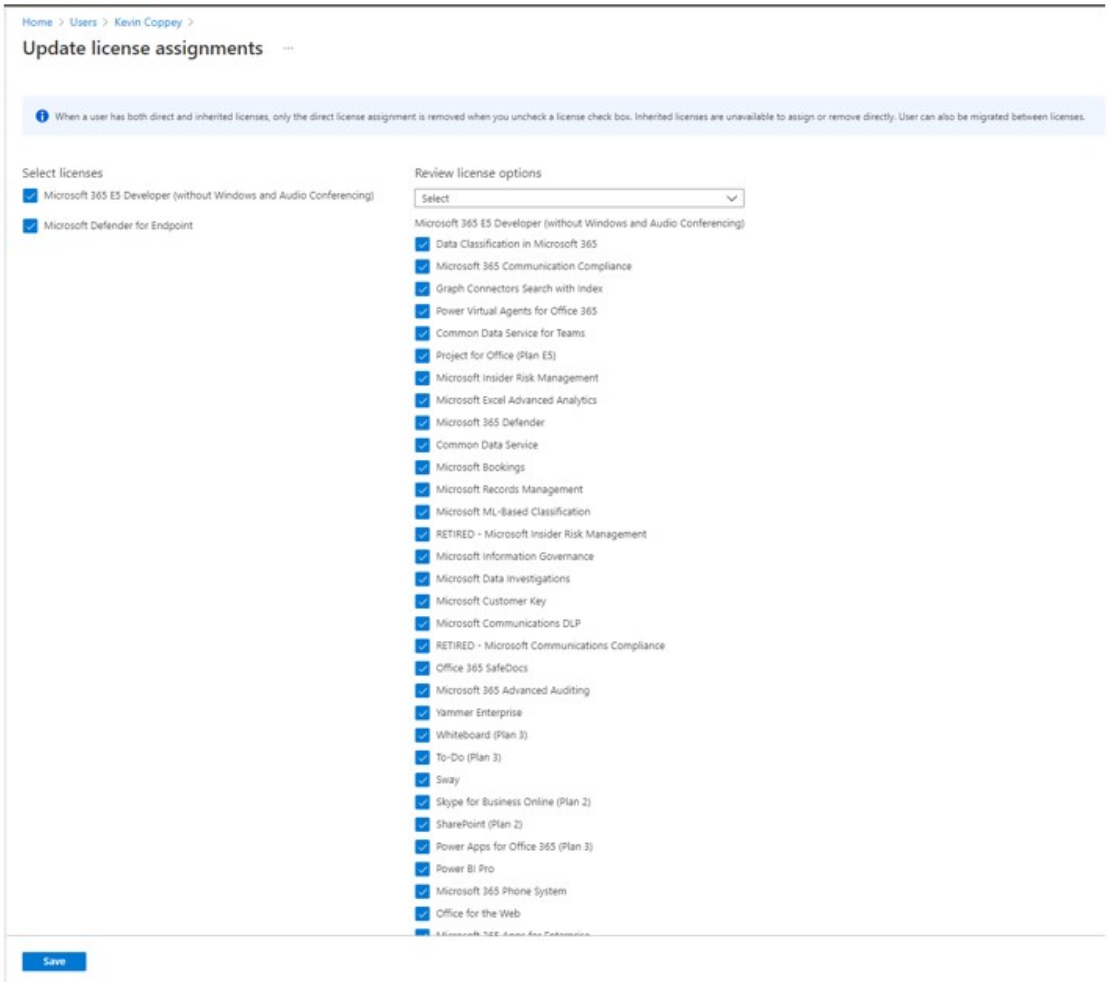
7) Sur la page d'accueil du profil, se rendre sous « Licenses » dans le menu de droite :



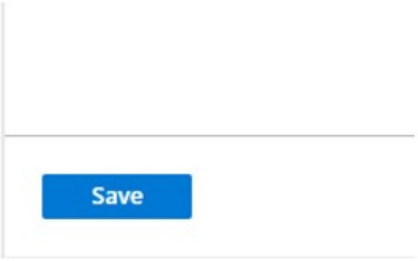
8) Cliquer sur le bouton « Assignments » dans la partie supérieur de la page :



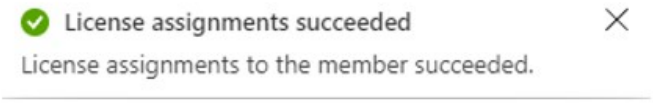
9) Sélectionner les deux licences « Microsoft 365 E5 Developer » et « Microsoft Defender for Endpoint » :



10) Cliquer sur le bouton « Save » tout en bas à gauche de la page :

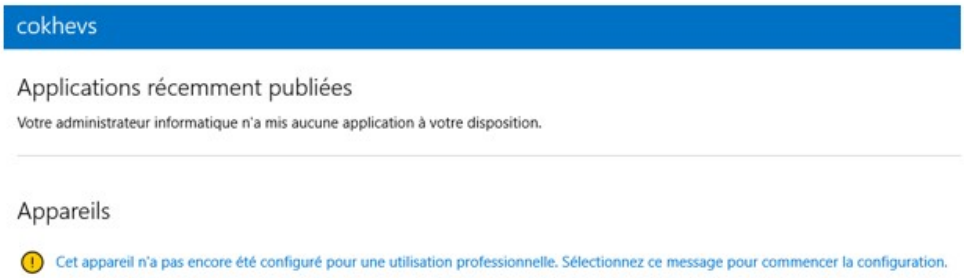


11) Une notification apparaît en tout en haut à droite de la page pour signaler le succès de la procédure :



12) Sur la machine virtuelle/le PC physique, télécharger l'application « Portail d'entreprise » sur le « Microsoft Store »

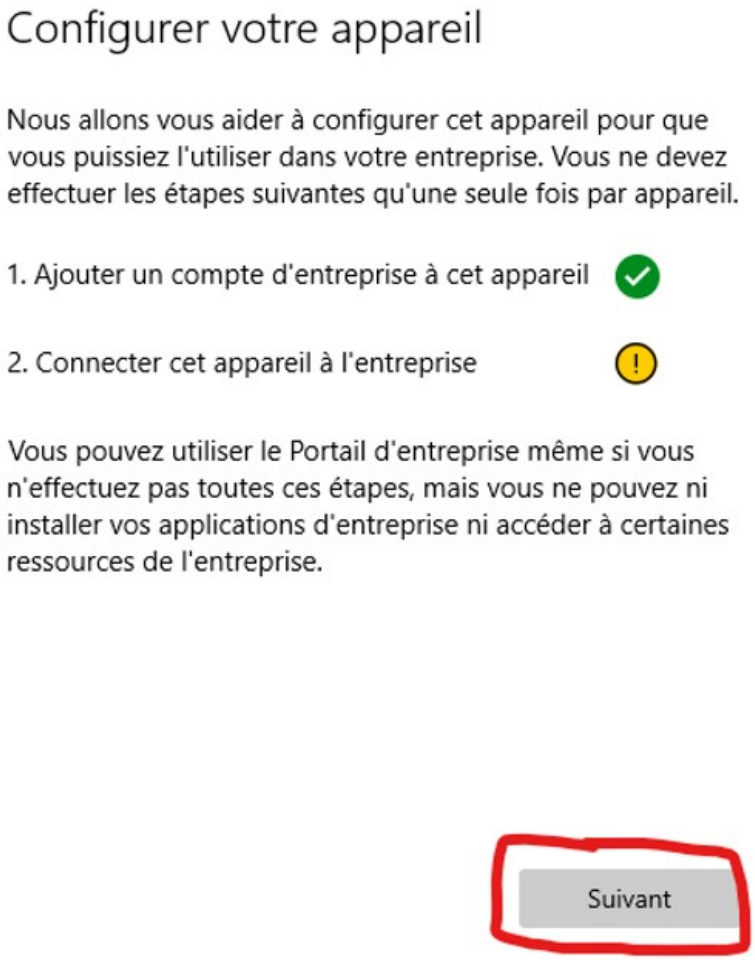
13) Une fois téléchargée, ouvrir l'application et constater le message suivant :



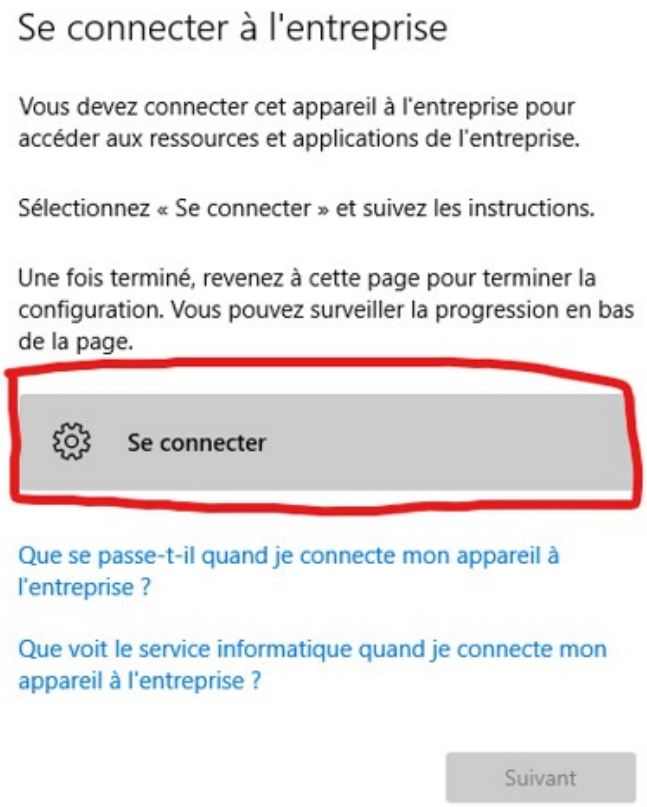
Ce message indique que l'appareil n'a pas encore été enrôlé pour qu'il puisse être géré par l'organisation. Il est donc nécessaire de procéder à la configuration pour que l'appareil de l'employé puisse apparaître sur « Microsoft Endpoint Manager ».

14) Cliquer sur le message au centre de l'écran :

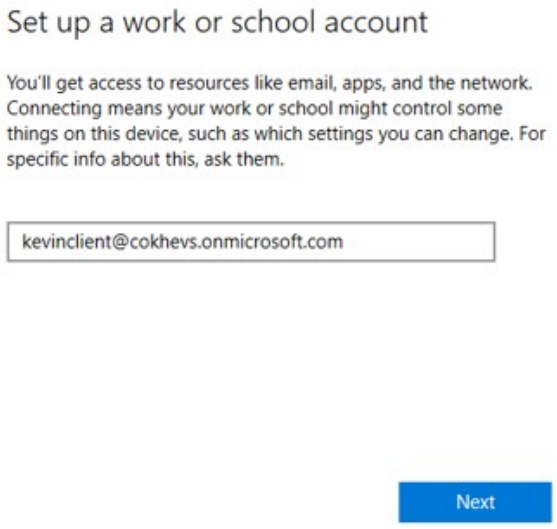
15) Sur la page « Configurer votre appareil », cliquer sur suivant tout en bas à droite.



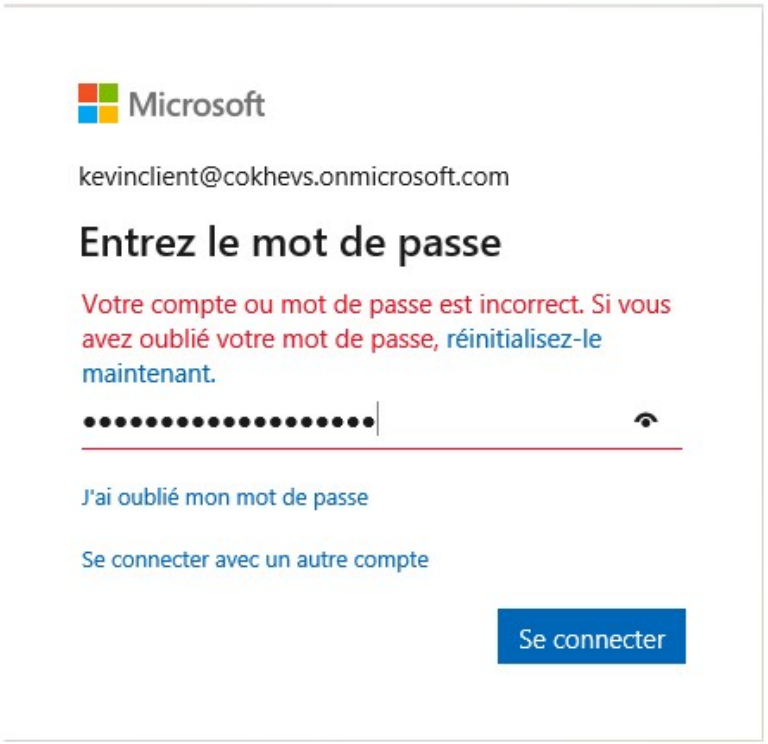
16) Sur la page « Se connecter à l'entreprise », cliquer sur le bouton « se connecter » au centre de l'écran :



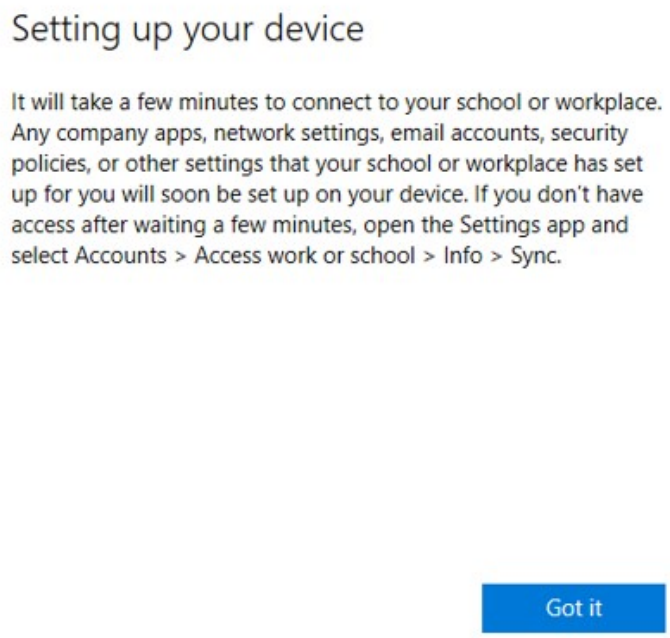
17) Entrer son adresse électronique de domaine et appuyer sur « Next » :



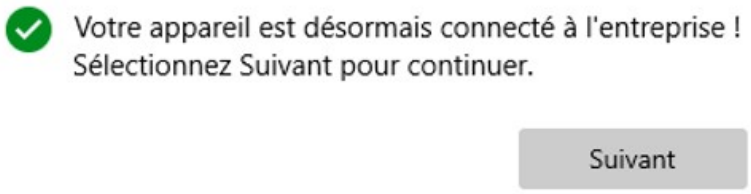
18) Entrer ses informations de connexion, puis cliquer sur « Se connecter » :



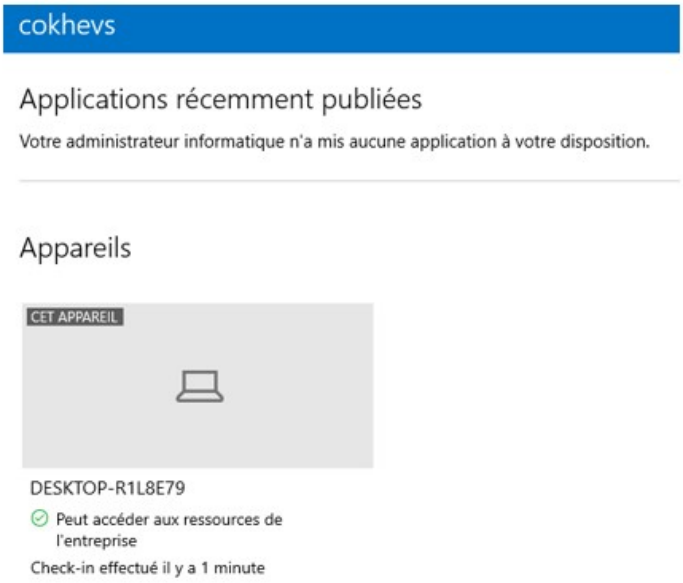
19) Prendre connaissance du message de la page « Setting up your device » et cliquer sur « Got it » :

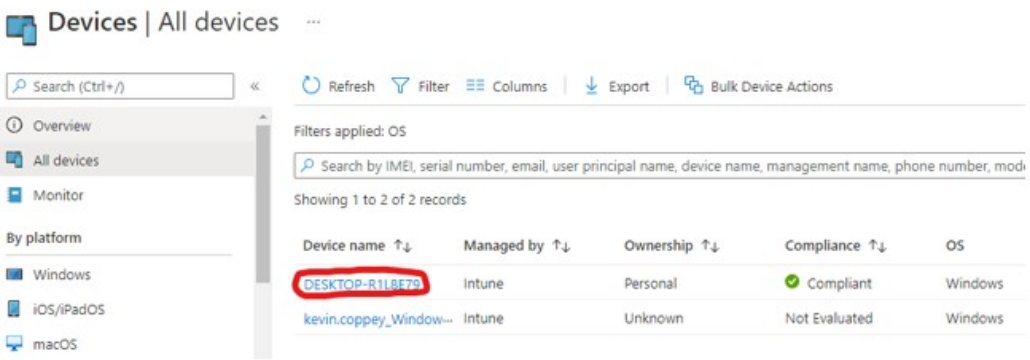


20) Le message suivant apparaît pour confirmer l'enrôlement, cliquer sur « Suivant »



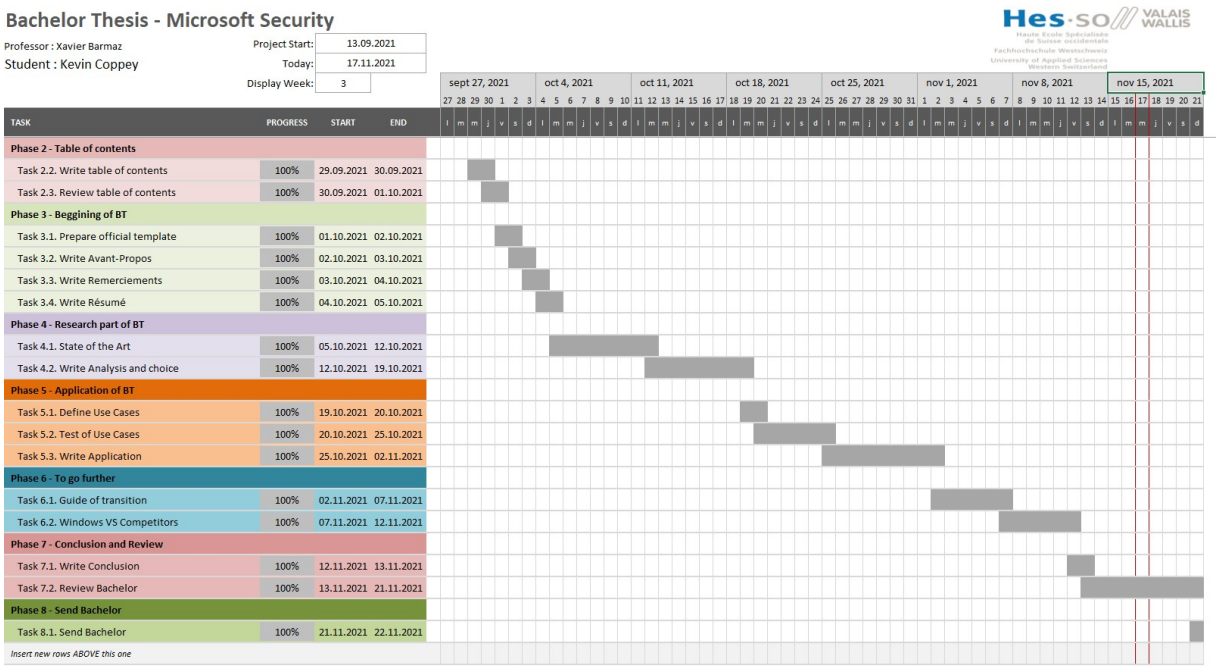
21) L'appareil est maintenant enrôlé sur « Azure Active Directory » et prêt pour être gérer par l'organisation :





Le compte du nouvel utilisateur est dorénavant créé et sa machine est enrôlée pour gestion auprès de l'organisation !

Annexe III : Diagramme de Gantt (Source : Auteur)



Bachelor Thesis - Microsoft Security

Professor : Xavier Barmaz
Student : Kevin Coppey

Project Start: 13.09.2021
Today: 17.11.2021
Display Week: 3

TASK	PROGRESS	START	END
Phase 2 - Table of contents			
Task 2.2. Write table of contents	100%	29.09.2021	30.09.2021
Task 2.3. Review table of contents	100%	30.09.2021	01.10.2021
Phase 3 - Beggining of BT			
Task 3.1. Prepare official template	100%	01.10.2021	02.10.2021
Task 3.2. Write Avant-Propos	100%	02.10.2021	03.10.2021
Task 3.3. Write Remerciements	100%	03.10.2021	04.10.2021
Task 3.4. Write Résumé	100%	04.10.2021	05.10.2021
Phase 4 - Research part of BT			
Task 4.1. State of the Art	100%	05.10.2021	12.10.2021
Task 4.2. Write Analysis and choice	100%	12.10.2021	19.10.2021
Phase 5 - Application of BT			
Task 5.1. Define Use Cases	100%	19.10.2021	20.10.2021
Task 5.2. Test of Use Cases	100%	20.10.2021	25.10.2021
Task 5.3. Write Application	100%	25.10.2021	02.11.2021
Phase 6 - To go further			
Task 6.1. Guide of transition	100%	02.11.2021	07.11.2021
Task 6.2. Windows VS Competitors	100%	07.11.2021	12.11.2021
Phase 7 - Conclusion and Review			
Task 7.1. Write Conclusion	100%	12.11.2021	13.11.2021
Task 7.2. Review Bachelor	100%	13.11.2021	21.11.2021
Phase 8 - Send Bachelor			
Task 8.1. Send Bachelor	100%	21.11.2021	22.11.2021
Insert new rows ABOVE this one			

ANNEXE IV – Cahier des charges (Source : Auteur)

Hes·so // VALAIS WALLIS
Haute Ecole de Gestion
Hochschule für Wirtschaft

FILIERE INFORMATIQUE DE GESTION

Microsoft Security Windows Client Security

Cahier des charges

Septembre 2021

Réalisé par Kevin Coppey.
Professeur responsable : Xavier Barmaz
Document déposé en septembre 2021

TABLE DES MATIÈRES

1. CHAPITRE 1 : INTRODUCTION

Le présent document est rédigé dans un but d'organisation afin de donner une ligne directrice à suivre lors de l'élaboration du travail de Bachelor.

Nous poursuivons les objectifs suivants :

- Définir le contexte du travail de Bachelor « Microsoft Security Windows Client »
- Définir les étapes et les objectifs de réalisation du travail de Bachelor
- Expliquer la stratégie d'organisation

1.1. CONTEXTE

Depuis l'apparition de la Covid-19, la plupart des entreprises ont dû proposer une alternative au travail traditionnel sur site. Nous avons donc vu l'essor du travail à distance et, par conséquent, de l'utilisation des outils à la maison.

Etant donné que la majorité des entreprises base leurs systèmes d'exploitation sur Windows, il est intéressant de se poser la question : « Comment faire pour protéger les appareils nomades en dehors et à l'intérieur de la structure de l'entreprise ? ».

Microsoft s'est penché sur la question et propose depuis plusieurs années une alternative à l'installation sur site de toute l'infrastructure. Cette alternative utilise la technologie du cloud pour proposer à ses clients un service simplifié et accessible.

Par conséquent, il est nécessaire pour tout responsable IT de choisir entre plusieurs possibilités :

- Sur site (On-Premise)
- L'informatique en Nuage (Cloud)
- La mixité (Mix)

Ce sont ces éléments que nous développons dans ce document.

1.2. APERÇU DES ÉTAPES

Afin de répondre à la question présente dans le contexte de ce document, il est nécessaire d'analyser les possibilités présentes sur le marché.

Ainsi, voici les différents axes d'état de l'art que nous proposons dans ce travail :

1) Etat de l'art des solutions natives à la sécurité Windows Client-Side (laptop).
2) Etat de l'art des solutions On-Premise.
3) Etat de l'art des solutions Cloud.

4) Etat de l'art des solutions Mix.

Les états de l'art, cités ci-dessus, permettent de passer au choix de l'alternative la plus à même d'être utilisée dans un contexte professionnel.

Pour ce faire, nous mettons en place un laboratoire de test suivant des cas d'utilisation spécifiques quant à la meilleure solution choisie.

1.3. INFORMATION SUR LE TRAVAIL

Type de travail : Recherche, analyse et test, établissement de guides.

Difficulté : Moyenne mais demande énormément de rigueur.

1.4. OBJECTIFS

- Etat de l'art des solutions natives dans la sécurité Windows Client-Side (laptop).
- Etat de l'art des solutions dites « On-Premise ».
- Etat de l'art des solutions dites « Cloud ».
- Etat de l'art des solutions dites « Mix ».
- Analyse et choix de la ou des meilleure(s) solution(s) pour soumission au laboratoire de test. De cette analyse va ressortir quelle stratégie est la meilleure (On-Premise, Cloud, Mix).
- Guide d'installation et de configuration des outils retenus après analyse.
- Création d'un laboratoire de test des outils selon le résultat de l'analyse (Use Case).

1.4.1. Bonus

- Comparaison des services proposés par Microsoft avec la concurrence afin d'assurer la légitimité de ses outils.
- Définition d'un guide de migration vers une solution Cloud ou Mix.

1.4.2. Risque

Dans l'hypothèse où une solution explorable ne permet pas de bénéficier de la gratuité d'un service offert par Microsoft, il sera nécessaire de prendre contact avec ces derniers pour obtenir une licence d'utilisation pour un tel module payant.

1.5. CONTRAINTES TECHNIQUES

- VirtualBox
- Windows 10 Server
- Windows 10 Professional
- Microsoft Azure
- Licences d'utilisation

2. CHAPITRE 2 : PLANIFICATION / OBJECTIFS

2.1. ETAT DE L'ART

Dans cette partie du document, nous nous intéressons à recenser les principales solutions natives de sécurité existantes sur Windows proposé par Microsoft afin de garantir sa légitimité face à la concurrence. (Cf. rubrique plus haut « bonus »)

Nous décomposons cet état de l'art en fonction de leur contexte d'utilisation : On-Premise, Cloud et Mix ainsi que les solutions déjà présentes sur un laptop Windows 10.

Chaque contexte d'utilisation implique la description claire de celui-ci et une liste des outils de sécurité en adéquation avec la thématique de ce TB.

Etant donné le vaste choix de solutions proposées par Microsoft dans le contexte de la sécurité des appareils « endpoints », ainsi que le temps accordé pour ce TB, nous développons pour chaque état de l'art un maximum de 5 outils.

2.1.1. ETAT DE L'ART DES SOLUTIONS NATIVES DANS LA SECURITE WINDOWS CLIENT-SIDE (LAPTOP)

La première étape est de recenser les solutions proposées nativement par Microsoft concernant la sécurité d'ores et déjà présentes sur les machines clientes utilisant Windows comme système d'exploitation.

2.1.2. ETAT DE L'ART DES SOLUTIONS ON PREMISE

Cette étape consiste en la recherche des solutions chez Microsoft présentes sur le marché dans un contexte d'utilisation « On-Premise ».

2.1.3. ETAT DE L'ART DES SOLUTIONS CLOUD

Cette étape concerne le recensement des solutions proposées par Microsoft pour une utilisation via le « Cloud ».

Il est possible que certaines de ces solutions soient payantes. Elles demandent donc une licence d'utilisation (Contacter Microsoft pour un trial)

2.1.4. ETAT DE L'ART DES SOLUTIONS MIX

Cette étape concerne le recensement des solutions proposées par Microsoft pour une utilisation hybride. Par conséquent, l'infrastructure est divisée par des outils installés sur site et d'autres sur le cloud.

Nous nous intéressons ici aux services de chez Azure qui sont directement lié à l'exploitation d'une infrastructure hybride.

Il est possible que certaines de ces solutions soient payantes. Elles demandent donc une licence d'utilisation nécessaire (Contacter Microsoft pour un trial)

2.2. COMPARAISON ET CHOIX

Après recensement des solutions proposées par Microsoft, il est temps de faire un choix.

Afin de procéder au choix de la meilleure solution, nous nous devons de détailler les différents outils analysés dans l'état de l'art à partir d'une liste de critères à déterminer. Par cette analyse, nous faisons notre choix entre les 3 types d'infrastructures :

- On-Premise
- Cloud
- Mix

2.3. INSTALLATION/TEST

Afin de réaliser ce laboratoire de test, nous pouvons d'ores et déjà présupposer l'installation des deux machines virtuelles suivantes :

- Windows Server 2019
- Windows 10

Il est très bien possible qu'une autre machine virtuelle vienne s'ajouter à cette liste si le besoin s'en ressent.

2.3.1. GUIDE D'INSTALLATION ET DE CONFIGURATION DE LA OU DES SOLUTION(S) RETENUE(S)

Cette partie est réalisée en fonction du choix fait dans la rubrique « COMPARAISON ET CHOIX ».

Un état de l'art des guides d'installation et de configuration sur les outils retenus est développé dans cette partie si toutefois ils existent.

Nous rédigeons, dans cette partie, toutes les étapes d'installation et de configuration des outils que nous avons retenus.

2.4. APPLICATION DE LA SOLUTION CHOISIE (LABO)

Un laboratoire de test est monté afin d'imaginer un ou plusieurs cas d'utilisation d'une solution On-Premise, Cloud ou Hybride.

Dans cette partie, nous imaginons un maximum de trois cas d'utilisation qui seraient envisageables dans une entreprise. Ces « Use Cases » permettent de prouver la légitimité de sécurité des machines « endpoints » de la ou des solution(s) retenue(s).

3. CHAPITRE 3 : Pour aller plus loin…

3.1. GUIDE DE MIGRATION

Nous imaginons, dans cette partie du TB, une stratégie de migration vers l'environnement choisi grâce à l'évaluation faites au-dessus.

Il est possible que cette partie n'apparaisse pas dans le TB final selon l'analyse faite des solutions. En effet, si les résultats montrent qu'un environnement On-Premise est retenu, il ne sera pas nécessaire d'expliquer la migration vers un environnement sur site.

Cependant, si les résultats de l'analyse montrent qu'une infrastructure cloud ou hybride est plus intéressante, nous établissons ici un guide pour passer d'une infrastructure On-Premise à Cloud ou hybride.

Dans cette optique, nous nous devons de réaliser un état de l'art sur les guides de migration déjà existants si toutefois ils existent.

3.2. COMPARAISON AVEC LA CONCURRENCE

Cette rubrique est utilisée pour confirmer ou infirmer le potentiel de Microsoft et de ses solutions par rapport à sa concurrence.

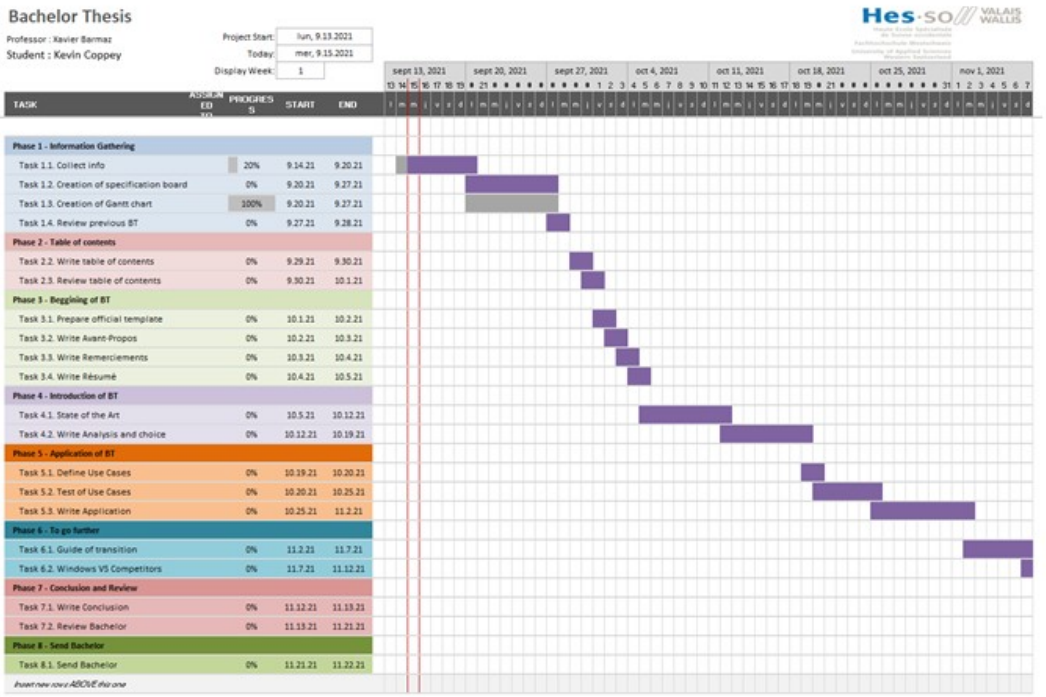
Les concurrents directs de Azure sont les suivants :

- Amazon Web Services (AWS)
- Google Cloud Platform
- IBM Cloud
- Alibaba Cloud

4. CHAPITRE 4 : ORGANISATION

4.1. DIAGRAMME DE GANTT

Afin de garantir une exécution des tâches relatives au Bachelor dans les temps, nous créons un diagramme de Gantt. Celui-ci contient les jalons principaux de ce Travail de Bachelor.



4.2. JOURNAL DE BORD

Un journal de bord est tenu afin de garder une trace de toutes les tâches effectuées dans le cadre de ce travail de Bachelor.

	A	B	C	D
1	**DATE**	**DURATION**	**WHAT**	**NOTES**
2	14.09.2021	01:30:00	Kick-off Bachelor meeting	This meeting had the purpose to handle all the administrative aspect of the thesis. We also discussed the core of the project to dive a little bit further into the concrete objectives of the work.
3	15.09.2021	10:00:00	Info gathering + organization + GANTT Chart	Information gathered about CLOUD VS ON-PREMISE solutions. Orgnization of notes taken during the Kick-off with Xavier. GANT Chart with deadlines created.
4	16.08.2021	05:00:00	Info gathering	Info gathering about difference AD + Azure AD.
5	17.08.2021	05:00:00	Info gathering	Info gathering about ON-PREMISE and CLOUD solutions.
6	19.09.2021	04:00:00	Info gathering	Info gathering about MIX solutions.
39	**TOTAL**	25:30		

ANNEXE V : Journal de bord (Source : Auteur)

DATE	DURATION	WHAT	NOTES
14.09.2021	01:30:00	Kick-off Bachelor meeting	This meeting had the purpose to handle all the administrative aspect of the thesis. We also discussed the core of the project to dive a little bit further into the concrete objectives of the work.
15.09.2021	10:00:00	Info gathering + organization + GANTT Chart	Information gathered about CLOUD VS ON-PREMISE solutions. Orgnization of notes taken during the Kick-off with Xavier. GANT Chart with deadlines created.
16.08.2021	05:00:00	Info gathering	Info gathering about difference AD + Azure AD.
17.08.2021	05:00:00	Info gathering	Info gathering about ON-PREMISE and CLOUD solutions.
19.09.2021	04:00:00	Info gathering	Info gathering about MIX solutions.
20.09.2021	08:00:00	Drafting of the specifications	Introduction + Planification/Objectives written.
21.09.2021	03:00:00	Drafting of the specifications	To go further + Organisation written -> End of specifications document.
27.09.2021	01:00:00	Specifications meeting	Meeting with Xavier to discuss the specifications.
28.09.2021	06:00:00	Rework of the Specifications	According to the meeting with Xavier, I corrected the mistakes and rework some parts of the doc.
30.09.2021	06:00:00	Drafting of the Table of Contents	Info gathering about State of the art. Kept only max. 5 solutions for every state of the art. All titles written.
01.10.2021	06:00:00	Review Table of Contents + Creation of template	Review everything by collecting information again. Official BT template created and organized.
03.10.2021	03:00:00	First sketch of "Résumé" and "Avant Propos"	80% of "Résumé" and "Avant Propos" parts have been created. --> Need to come back at the end to validate everything.
05.10.2021	08:00:00	State of the art	Windows native security -> Protection agains viruses and threats + beginning of Account protection
06.10.2021	08:00:00	Info gathering	Info gathering about ON-PREMISE.
07.10.2021	08:00:00	Info gathering + test	Info gathering about ON-PREMISE and test of solutions.
08.10.2021	06:00:00	Info gathering + test	Info gathering about ON-PREMISE and test of solutions.
09.10.2021	08:00:00	Info gathering + abandon ON-PREMISE	Problems with testing solutions with ON-PREMISE. I decided to keep going with Cloud solutions.
10.10.2021	12:00:00	Installation and configuration of lab + Guide for licenses+ Guide for enroll devices	I configured a windows 10 updated machine to test the Windows Update feature.
11.10.2021	13:00:00	State of the art CLOUD introduction + Windows update + BitLocker encryption part	Write the introduction and Windows update part, everything works fine !
12.10.2021	13:00:00	BitLocker + Antivirus + Windows Hello CLOUD	Those 3 guides are finished and work perfectly.
13.10.2021	13:00:00	Microsoft Defender SmartScreen for Cloud	Those guides are finished and works.
14.10.2021	13:00:00	SCCM for on-premise installation and test	SCCM is installed and works
15.10.2021	13:00:00	AD + GPO and SCCM State of the art	On-premise State of the art finished.
16.10.2021	12:00:00	MEM + MDE + MDO365 State of the art	Cloud State of the art finished.
17.10.2021	10:00:00	Gathering info for Hybrid Cloud and Co-management	Co-management part finished but there is not seem to be any other hybrid security service for Microsoft.
19.10.2021	08:00:00	Comparison between Microsoft and third	This part is finished.
22.10.2021	01:00:00	Meeting with Xavier to review the State of the Art	Structure is quite okay, I just need to correct some spelling mistakes, add print-screens and remove some parts.
23.10.2021	03:00:00	Correction according to Xavier's review of State of the Art	None.
24.10.2021	08:00:00	Research for Analysis	None.
25.10.2021	08:00:00	Research for Analysis	None.
26.10.2021	12:00:00	Research for Analysis	None.
27.10.2021	10:30:00	Selection of criteria	Criterion found.
28.10.2021	13:00:00	Analysis part finished	The analysis part is finished but I still need to come back later to check the structure. The Cloud is chosen.
29.10.2021	08:00:00	Restrucuration of the document	Clean not finished...
30.10.2021	13:00:00	Restrucuration of the document	Document cleant up.
01.11.2021	10:00:00	Research for Migration from On-Premis to Cloud + Active Directory and GPO to Cloud	The first part with AD + GPO to Cloud is written.
02.11.2021	12:00:00	Configuration Manager to Cloud + Clean up AD and GPO migration	Everything works perfectly.
03.11.2021	12:00:00	Clean up the document + Preparation Demo + Conclusion	The Bachelor is over, I need now to improve the quality of the texts, check if APA is okay and spelling mistakes.
04.11.2021	05:00:00	Clean up + Check spelling mistakes	None.
08.11.2021	06:00:00	Setup of the VM for the demo	None.
09.11.2021	08:00:00	Final clean up of the document	None.
10.11.2021	04:00:00	Check APA sources	None.
11.11.2021	10:00:00	Configuration of the VM for the demo	Uses cases ransomware.
12.11.2021	01:00:00	Meeting with Xavier to discuss the demo	Better to prove why Cloud is the best solution via some use cases.
14.11.2021	10:00:00	Powerpoint created + Poster created + Demo with Conditional Access Test	The first demo that I want to show on the 10th works perfectly and proves that Cloud is better than On-Premise.
15.11.2021	08:30:00	Demo wih video of installation of SCCM Test	The second demo that I want to show on the 10th works perfectly and proves that Cloud is better than Hybrid.
TOTAL	366:30		

Déclaration de l’auteur

Je déclare, par ce document, que j'ai effectué le travail de Bachelor ci-annexé seul, sans autre aide que celles dûment signalées dans les références, et que je n'ai utilisé que les sources expressément mentionnées. Je ne donnerai aucune copie de ce rapport à un tiers sans l'autorisation conjointe du RF et du professeur chargé du suivi du travail de Bachelor, y compris au partenaire de recherche appliquée avec lequel j'ai collaboré, à l'exception des personnes qui m'ont fourni les principales informations nécessaires à la rédaction de ce travail et que je cite ci-après : Le Professeur Xavier Barmaz.

Lieu et date :

Sierre, le 21.11.2021

Signature :

(Kevin Coppey, Étudiant HES-SO)