Chapitre 3
Configuration des périphériques

1. Introduction

Depuis toujours, les organisations qui mettent à disposition des appareils souhaitent offrir des configurations par défaut. Ces personnalisations ont pour objectif de personnaliser l'expérience, de faciliter la configuration de l'appareil, ou tout simplement d'améliorer la sécurité de l'organisation. Trop souvent, les menaces proviennent de l'intérieur de l'entreprise avec des configurations altérées par les utilisateurs. En plus de la sécurité, l'essor du télétravail a engendré la nécessité d'offrir des mécanismes d'accès à distance. Ceux-ci peuvent demander le déploiement de nombreux prérequis, dont des certificats, des profils de configuration pour l'accès aux réseaux internes (Wi-Fi, VPN, etc.). L'objectif est qu'après le provisionnement, l'enregistrement et la mise en service de l'appareil, celui-ci soit configuré sans demander d'actions particulières de l'utilisateur ou de l'administrateur. Outre cela, les appareils peuvent avoir des dérives de configuration, c'est particulièrement le cas pour les systèmes Windows ou macOS. Ces problèmes sont symptomatiques d'une gestion difficile des postes de travail, serveurs et périphériques de l'entreprise. L'analyse et la maîtrise de ces points critiques peuvent faire la différence entre un parc sain, et une infrastructure faible et vulnérable. Connaître son parc et suivre son évolution est la clé d'une infrastructure maîtrisée et d'un environnement de travail sûr et efficace.

Afin de vous donner tous les éléments permettant de réaliser des configurations adéquates sur les différentes plateformes, nous aborderons la mise en œuvre des prérequis nécessaires à la configuration de paramétrages, du déploiement de certificats, et de l'accès à distance. Vous pourrez ensuite obtenir un aperçu des profils de configuration disponibles incluant le **catalogue de paramétrages** (*settings catalog*) ou les **modèles prédéfinis**. Nous aborderons des configurations spécifiques aux appareils dans des scénarios Kiosk permettant de configurer le mode partagé de Microsoft Entra (*shared mode*). Pour toutes les configurations qui ne sont pas disponibles sur étagère, Microsoft Intune permet l'**exécution de scripts** pour les plateformes Windows, macOS, et Linux. Lorsque le système est soumis à des dérives de configuration ou tout simplement pour corriger des problèmes divers et variés, Microsoft offre un **mécanisme de remédiation** alliant un principe de découverte de la déviation et de correction. Parce que les entreprises ont entamé une transition du modèle traditionnel visant à gérer les systèmes Windows avec les stratégies de groupe (GPO), nous verrons quelle est la démarche et les méthodologies ainsi que les outils pour effectuer la transition vers des configurations proposées via Microsoft Intune. Enfin, nous verrons quels sont les rapports, outils et solutions permettant de suivre ces configurations dans le temps.

2. Concepts

Pour bien comprendre et maîtriser la configuration des appareils au sein de Microsoft Intune, il est primordial d'étudier et de comprendre les différents concepts proposés par les différentes plateformes qui en font un outil très puissant et utile dans l'entreprise. La maîtrise des concepts est essentielle pour pouvoir mettre en place le plus efficacement possible les éléments de configuration.

2.1 OMA-URI

OMA-URI pour *Open Mobile Alliance - Uniform Resource Identifier*, est un standard utilisé par les principales plateformes et systèmes d'exploitation pour gérer les paramètres sur les appareils. Ce mécanisme permet à Intune de définir ou d'obtenir des valeurs de configuration en communiquant directement avec les interfaces de configuration.

Le concept général repose sur l'utilisation d'identifiants uniformes pour accéder et modifier les paramètres de configuration de divers appareils tels que Windows, iOS/iPadOS, Android et macOS. Pour chaque plateforme, les OMA-URI suivent une certaine arborescence qui détermine comment les différentes configurations sont organisées et accessibles.

Voici quelques exemples d'OMA-URI selon les plateformes :

– Windows : ./Device/Vendor/MSFT/Policy/Config/DeviceLock/MinDevicePasswordLength
– iOS/iPadOS : com.apple.applicationaccess/allowAppInstallation
– Android : ./Device/Vendor/MSFT/Policy/Config/ApplicationManagement/AllowAppInstall
– macOS : com.apple.systempreferences/network

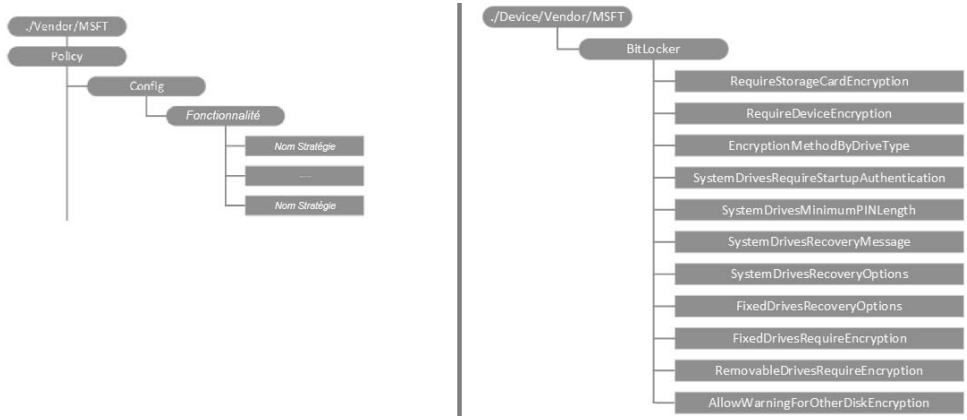
Lorsqu'un administrateur crée et applique une stratégie personnalisée via Intune, celui-ci devient le mécanisme de remise chargé d'envoyer les OMA-URI aux appareils clients concernés. Ce processus est rendu possible grâce à l'utilisation du protocole **OMA-DM** (***Open Mobile Alliance Device Management***), qui assure une communication efficace entre Intune et les appareils.

2.2 Configuration Service Providers

Le monde de la gestion des appareils mobiles et des systèmes d'exploitation a évolué de manière spectaculaire au cours des dernières décennies, en grande partie grâce aux progrès des technologies cloud et des solutions de gestion centralisée. Avec l'émergence de la mobilité et du télétravail, les interfaces de gestion traditionnelles comme les stratégies de groupe (GPO), *WMI*, etc., ont montré leurs limites. Ces mécanismes n'offraient une fiabilité que relative et ne permettaient pas de connaître l'état de la machine. C'est dans ce contexte que les ***Configuration Service Providers*** (**CSP**) ont vu le jour. Introduits avec Windows 10, les CSP ont été conçus pour tirer parti de la gestion moderne, également connue sous le nom de « modern management », qui utilise des services cloud pour fournir une configuration et une gestion cohérente sur tous les types d'appareils.

Les CSP permettent aux administrateurs de définir des politiques de configuration via des commandes standardisées, accessibles via des interfaces API. Ces commandes peuvent être exécutées à partir de solutions de gestion d'appareils mobiles (MDM) telles que Microsoft Intune.

Le concept d'un CSP repose sur l'encapsulation de paramètres de configuration spécifiques dans des « nœuds » de l'arborescence MDM. Chaque nœud représente un aspect particulier de la configuration de l'appareil, allant de la configuration du réseau Wi-Fi à la politique de sécurité des mots de passe, en passant par les mises à jour logicielles et les restrictions d'utilisation des applications. Cela permet une granularité fine et une gestion centralisée à un niveau jamais atteint auparavant.



Les CSP offrent également une grande flexibilité en permettant aux administrateurs de cibler des configurations spécifiques à des groupes ou à des utilisateurs particuliers, en fonction des besoins opérationnels et des politiques de sécurité de l'entreprise. L'implémentation de cette notion de CSP utilise le standard **OMA-URI** qui introduit cette notion d'arborescence de configuration.

L'approche moderne de Microsoft se repose sur la couverture de besoins essentiels afin de rendre le poste de travail efficace. Néanmoins, les dizaines d'années d'usages des stratégies de groupe ne peuvent effacer certains besoins historiques notamment quand il s'agit de configurer des applications tierces. Pour ce faire, Microsoft a implémenté une interface sur le CSP Policy permettant de gérer un ensemble sélectionné de stratégies ADMX.

Dans une stratégie ADMX, un modèle administratif contient les métadonnées d'une stratégie de groupe Windows et peut être modifié dans l'éditeur local de stratégie de groupe sur un PC. Chaque modèle administratif spécifie les clés de registre (et leurs valeurs) qui sont associées à une stratégie de groupe et définit les paramètres de la stratégie qui peuvent être gérés. Le CSP Policy vient donc configurer ces clés de registre et valeurs selon la définition du modèle et la configuration choisie par l'administrateur.

Microsoft utilise le protocole OMA-DM qui utilise le syncML xml pour l'échange de données entre les serveurs et les clients conformes. Ce protocole a été utilisé jusqu'alors, mais a lui-même montré plusieurs limites dont notamment le nombre d'échanges nécessaires pour obtenir et appliquer une configuration. Microsoft planifie notamment de basculer sur un protocole appelé ***Windows Declared Configuration*** (**WinDC**) qui a pour principaux avantages de réduire le nombre d'échanges, de réaliser la résolution des conflits de configuration localement et non par le service. Par conséquent, ceci minimise la propension à une dérive de configuration.

Ce nouveau protocole va peu à peu être généralisé sur les différentes configurations pour le système Windows. Il n'en est pas moins qu'il continuera d'utiliser le principe de CSP basé sur le standard OMA-URI.

La stratégie de Microsoft avec les CSP s'inscrit donc pleinement dans sa vision de l'*Unified Endpoint Management* (UEM), qui vise à unifier la gestion de tous les appareils - qu'ils soient sous Windows, macOS, iOS ou Android. Cette approche unifiée permet une gestion cohérente, une meilleure sécurité et une plus grande efficacité opérationnelle, tout en fournissant aux utilisateurs finaux des outils et des applications qui supportent leur productivité quotidienne sans les contraindre.

Remarque

Si vous souhaitez obtenir plus de détails sur les CSP et WinDC, vous pouvez lire les articles suivants : https://learn.microsoft.com/windows/client-management/declared-configuration?WT.mc_id=EM-MVP-4028970 ou https://learn.microsoft.com/windows/configuration/provisioning-packages/how-it-pros-can-use-configuration-service-providers?WT.mc_id=EM-MVP-4028970.

2.3 Config Refresh

Config Refresh est une fonctionnalité introduite en 2024 par Microsoft pour améliorer la gestion des politiques de configuration via Intune sur les **appareils Windows** à partir de Windows 11 avec la mise à jour de sécurité de juin 2024. Cette fonctionnalité permet aux administrateurs informatiques de contrôler plus efficacement la fréquence de mise à jour des configurations. Les administrateurs peuvent ainsi configurer le délai de rafraîchissement des stratégies, avec des intervalles pouvant varier de 30 minutes à 24 heures. Cette fonctionnalité vise à fournir le même niveau de contrôle que les administrateurs avaient auparavant avec les stratégies de groupe.

Tout comme avec les stratégies de groupe, Config Refresh permet de garantir que les appareils gérés restent conformes aux stratégies établies sans nécessiter de redémarrages fréquents ou des délais prolongés avant l'application des nouvelles configurations. Il permet de couvrir le cas des dérives de configuration qui peuvent arriver pour différentes raisons comme les changements réalisés par des administrateurs locaux ou des configurations qui ne se réappliqueraient pas nativement. Dans le cas d'un dépannage, les administrateurs ont la possibilité de suspendre temporairement ce processus de rafraîchissement pour une période déterminée. Après les actions de dépannage, le rafraîchissement peut être automatiquement réactivé ou manuellement remis en service à tout moment.

Config Refresh constitue donc un outil indispensable pour assurer un parc homogène et conforme aux exigences de l'entreprise.

2.4 Declarative Device Management

Le protocole de ***Declarative Device Management*** (**DDM**) d'Apple est la nouvelle mouture du protocole MDM utilisé pour la gestion des appareils iOS, iPadOS et macOS. L'ancien protocole MDM propriétaire d'Apple, basé sur OMA-DM avait les mêmes limitations que pour Windows. Le protocole générait de nombreux échanges entre l'appareil et le service de gestion. DDM repose sur un modèle où l'état souhaité des appareils est spécifié par les administrateurs IT, permettant aux appareils de s'autoconfigurer en fonction de déclarations simples et claires.

Le fonctionnement du protocole s'appuie sur des documents de configuration, souvent au format JSON ou XML, qui définissent les paramètres nécessaires pour optimiser la sécurité et les performances des appareils. Lorsqu'un appareil est enregistré dans Microsoft Intune, il reçoit ces déclarations qui contiennent les politiques de gestion, les exigences de sécurité, et d'autres configurations pertinentes. Cette connexion en temps réel permet une synchronisation instantanée des configurations et un contrôle centralisé, voire la capacité à définir des règles dynamiques qui s'ajustent en fonction des conditions d'utilisation. Par exemple, si un appareil change de réseau ou de configuration géographique, les politiques applicables peuvent être automatiquement ajustées pour assurer une conformité continue.

Le protocole de Declarative Device Management d'Apple permet aussi à Microsoft d'intégrer plus facilement et plus rapidement les nouveaux paramétrages proposés par les nouvelles versions d'iOS/iPadOS ou macOS. À date d'écriture de cet ouvrage, toutes les configurations de Microsoft Intune n'utilisent pas encore ce nouveau protocole mais Apple et Microsoft réalisent progressivement une transformation des configurations.

2.5 Concevoir ses stratégies de configuration

Quelles que soient la plateforme ou la solution de gestion, la conception des stratégies de configuration et les bonnes pratiques à adopter restent un enjeu crucial. Faut-il créer peu de stratégies qui regroupent de nombreux paramétrages ou de nombreuses stratégies qui regroupent peu de paramétrages ? Ces questions se posaient déjà à l'heure des stratégies de groupe (GPO) sous Windows. On retrouve donc les mêmes débats et la réponse n'est souvent pas si tranchée.

L'approche à adopter doit être hybride. Ainsi, il est recommandé de créer :

– **Quelques stratégies standards** avec les paramètres génériques qui s'appliquent à l'ensemble des appareils partageant la même typologie (Kiosk, poste standard, poste administrateur, etc.) d'une même plateforme.

– **Plusieurs stratégies avec peu de paramètres** pour des besoins liés à des populations ou à des configurations **spécifiques**. Ces stratégies plus ciblées sont plus faciles à comprendre et à dépanner. Si une configuration engendre un problème, il est plus simple d'identifier et de corriger l'origine du problème lorsqu'elle est isolée dans une stratégie dédiée.

Remarque

Vous devez éviter au maximum la création d'une stratégie pour configurer un seul paramétrage sous peine de très vite arriver à un nombre très important de stratégies et une difficulté de lecture ou de dépannage des stratégies.

Il faut donc que vous projetiez la conception de vos stratégies dès les premières créations afin de garder une cohérence dans le temps. Une structure de stratégies bien organisée permet d'adapter rapidement les configurations en fonction des évolutions des besoins de l'entreprise ou des politiques de conformité, sans avoir à réviser une stratégie complexe et surchargée.

2.6 Déploiement de certificats

Le déploiement de certificats permet de couvrir différents besoins sur les appareils comme l'authentification sur le réseau (802.1X, Wi-Fi, VPN), la signature et/ou le chiffrement d'e-mails, l'authentification sur des applications, etc.

Microsoft Intune propose différentes méthodes permettant de déployer et gérer des certificats :

– Les **certificats approuvés** (***trusted certificates***) permettent de déployer des certificats qui sont stockés dans les magasins de certificats approuvés comme les autorités racines ou intermédiaires.

– Les **certificats SCEP** utilisent le protocole standardisé du même nom. Il est utilisable par toutes les autorités et toutes les solutions qui le supportent. Dans ce cas de figure, c'est la machine qui procède à la demande via le protocole SCEP et au travers d'un rôle qui gère ces demandes. Ce mode de fonctionnement permet de garantir que la clé privée est générée sur les appareils et réduit ainsi son exposition. Parmi les inconvénients, on retrouve :
  – La complexité de mise en œuvre de l'infrastructure supportant le protocole SCEP.

  - La sécurisation de l'infrastructure puisque le rôle NDES doit être accessible par les appareils. Ceci requiert de soit mettre ce rôle en frontal sur Internet, soit de le publier via des solutions de publication telles que Microsoft Entra Application Proxy ou Microsoft Entra Private Access.
- Les certificats PKCS utilisent le **connecteur PKCS** qui se charge de faire les demandes pour l'appareil ou l'utilisateur. Cette méthode peut être utilisée avec les autorités de certification : *Active Directory Certificate Services* (AD CS) et Digicert PKI. Elle est la plus simple à mettre en œuvre et à maintenir mais comporte quelques inconvénients dont :
  - La génération étant réalisée par le connecteur PKCS pour l'appareil, cela signifie que la clé privée peut transiter par plusieurs briques pouvant être compromises.
  - La gestion des certificats n'est pas automatisée et requiert donc des actions manuelles (révocation du certificat, etc.).
- Les **certificats PKCS importés manuellement** dans le service Microsoft Intune. Ce scénario cible principalement le chiffrement S/MIME et les profils e-mail. Cette méthode revient à utiliser le connecteur de certificat qui se chargera de gérer l'import des fichiers PFX dans le service. Cette méthode requiert la construction de code permettant la gestion des demandes et l'import manuel des certificats.

Remarque

Nous ne détaillerons pas ce scénario peu commun mais nous vous renvoyons vers la documentation associée : https://learn.microsoft.com/mem/intune/protect/certificates-imported-pfx-configure?WT.mc_id=EM-MVP-4028970

3. Prérequis

Cette section aborde les prérequis à mettre en œuvre pour permettre différents aspects de la configuration des appareils dont notamment le déploiement de certificat ou l'accès à distance.