TECHNO 38

Publication périodique de Smals

Avril 2014

Mobile Device Management

Outils pour la gestion des smartphones et tablettes

Bert Vanhalst est licencié en informatique. Depuis novembre 2001, il est employé comme consultant dans la section Recherche de Smals. Il a contribué à l'introduction de services web et de l'architecture orientée service et est actuellement spécialisé dans les applications mobiles, en particulier concernant les aspects de gestion et de sécurité.

Contact : 02 787 48 02

bert.vanhalst@smals.be

1. Introduction

Depuis quelques années, les appareils mobiles connaissent une ascension fulgurante. En effet, les smartphones et les tablettes sont devenus extrêmement populaires. Cette nouvelle vague offre bien évidemment des opportunités pour permettre l'utilisation de ces appareils en entreprise, de manière à accéder avec plus de flexibilité aux applications et aux informations des entreprises.

En tant qu'organisation, nous ne souhaitons évidemment pas laisser nos informations business à la portée de tout un chacun. Nous sommes bien disposés à autoriser les utilisateurs d'appareils mobiles à accéder à certaines données, mais alors de façon sécurisée, contrôlée.

D'une part, une organisation peut elle-même mettre des appareils mobiles à la disposition de ses travailleurs. D'autre part, de nombreux collaborateurs possèdent déjà une tablette ou un smartphone récent, performant, qu'ils désirent également utiliser dans le contexte de l'organisation. On parle alors de Bring Your Own Device (BYOD[1]).

Dans les deux cas, il s'agit de disposer d'une solution permettant de définir et d'imposer un certain nombre de règles en vue de sécuriser cet accès. On peut aisément faire la comparaison avec les mesures de sécurité déjà appliquées pour les PC et autres ordinateurs portables. Cependant, les outils pouvant être utilisés à cette fin ne conviennent pas pour gérer des appareils mobiles. C'est la raison pour laquelle une catégorie particulière d'outils a vu le jour, à savoir les solutions de Mobile Device Management (MDM).

Le marché du MDM est occupé par divers *pure players* tels que Airwatch, MobileIron et Zenprise. Ce genre de technologie suscite clairement de l'intérêt, car les acteurs plus grands complètent leur gamme de produits avec une solution MDM. Airwatch a ainsi été repris par VMware, tandis que Zenprise a été racheté par Citrix.

Parallèlement, les fournisseurs de logiciels de protection (dont Symantec et McAfee) intègrent de plus en plus une fonctionnalité MDM dans leurs produits.

Dans le présent Techno, nous traiterons tout d'abord de l'architecture technique propre à une solution MDM. Nous expliquerons ensuite les fonctionnalités que nous pouvons en espérer, ainsi que la procédure à suivre pour enregistrer un nouvel utilisateur et un nouvel appareil dans un système MDM. Enfin, nous présenterons la solution que Smals offre dans ce contexte.

[1] *Voir les slides de la séance d'info, disponibles sur le site web de la section Recherche de Smals : http://www.smalsresearch.be/publications/document?docid=24*

2. Architecture

Avant de détailler les fonctionnalités, il est intéressant de voir à quoi ressemble l'architecture technique d'une solution MDM et d'explorer les options possibles en ce qui concerne le déploiement.

Une solution MDM comporte généralement trois éléments :

1. Une app cliente
2. Un serveur de contrôle des politiques (sécurité, …)
3. Une passerelle de politiques

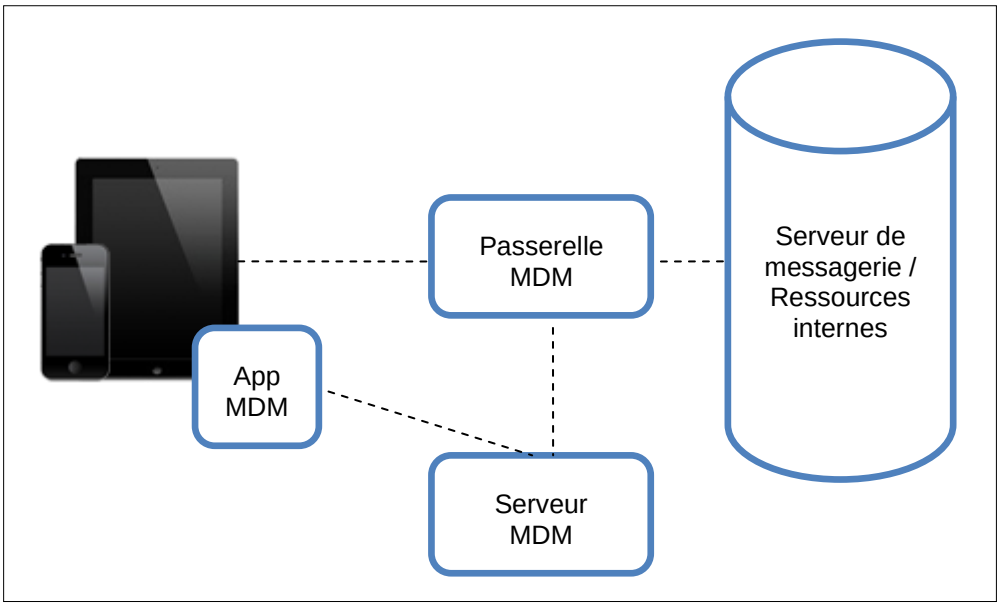


Illustration 1 : architecture MDM type

Les politiques de sécurité sont établies et gérées dans le serveur de politiques et d'administration (serveur MDM dans l'illustration). Les politiques sont communiquées aux appareils mobiles via une app MDM. Les appareils sont contrôlés de cette manière. L'accès aux ressources internes (serveur de messagerie par exemple) est contrôlé par une passerelle qui applique les règles d'accès définies (policy enforcement).

Globalement, il y a deux options pour le déploiement d'une solution MDM :

1. En mode SaaS : la solution MDM est hébergée chez le fournisseur de la solution MDM. L'administration et la configuration peuvent être assurées par les collaborateurs de l'entreprise, mais les données se trouvent dans un data center externe. Notez que cette méthode nécessite également une passerelle locale pour l'intégration avec les ressources internes (serveur de messagerie) ainsi qu'une intégration avec un répertoire d'utilisateurs.
2. Sur site : l'intégralité de la solution MDM est installée sur le réseau de l'entreprise. L'avantage de cette formule réside dans la confidentialité des données. Le software du serveur peut être livré sous forme de machine virtuelle ou éventuellement sous forme d'appliance hardware.

3. Fonctionnalités

Dans ce chapitre, nous aborderons les différentes fonctionnalités que possède généralement une solution de Mobile Device Management.

L'une des caractéristiques essentielles des solutions MDM est leur capacité à fonctionner sur différentes plateformes. En effet, elles supportent plusieurs systèmes d'exploitation mobiles. On retrouve généralement Android, iOS, Windows Phone et, dans une moindre mesure, BlackBerry. Certaines solutions MDM commencent également à supporter les systèmes d'exploitation desktop classiques, mais on n'en est qu'au tout début. Aujourd'hui, il n'existe donc pas de solution unique pour gérer tous les types d'appareil.

Le fait que les solutions MDM supportent plusieurs plateformes ne signifie toutefois pas que toutes les fonctionnalités sont disponibles sur chaque plateforme. La documentation de chaque produit contient une matrice de compatibilité indiquant quelle fonctionnalité est supportée sur quelle plateforme. Ci-après, nous verrons dans les grandes lignes quelle fonctionnalité est généralement livrée dans une solution MDM.

3.1. Politiques de sécurité

L'une des tâches-clés d'une solution MDM consiste à imposer des politiques de sécurité. Suivant la plateforme, des politiques peuvent être définies concernant les aspects suivants :

- **Mot de passe de l'appareil** - Il peut être demandé de définir un mot de passe pour déverrouiller l'appareil. Plusieurs règles peuvent être définies, comme le nombre maximal de tentatives infructueuses ainsi que la longueur minimale et la complexité du mot de passe.
- **Chiffrement** - Chiffrement des données présentes sur l'appareil et éventuellement de la carte SD.
- **Jailbreak / rooted devices** - Détection des appareils compromis.
- **Version minimale du système d'exploitation** - Si des problèmes de sécurité sont connus avec des versions antérieures du système d'exploitation, ces versions antérieures peuvent être exclues.
- **Apps** - Certaines apps peuvent être interdites (malware connu par exemple) ou imposées (app anti-malware par exemple).

Ci-dessous est proposé un exemple de configuration d'une politique de mot de passe. Notez que dans cet exemple, il n'est pas demandé à l'utilisateur de renouveler régulièrement le mot de passe de l'appareil (« Maximum Password Age » non paramétré). L'utilisateur dispose toutefois de six essais au maximum pour saisir le mot de passe correct, après quoi les données de l'appareil peuvent être entièrement effacées afin d'éviter un accès non autorisé. Il est aussi possible d'opter pour un système selon lequel l'utilisateur ne peut pas faire de nouvelle tentative durant un certain délai (par exemple 30 secondes). Ce délai s'allonge à chaque nouvelle tentative infructueuse.

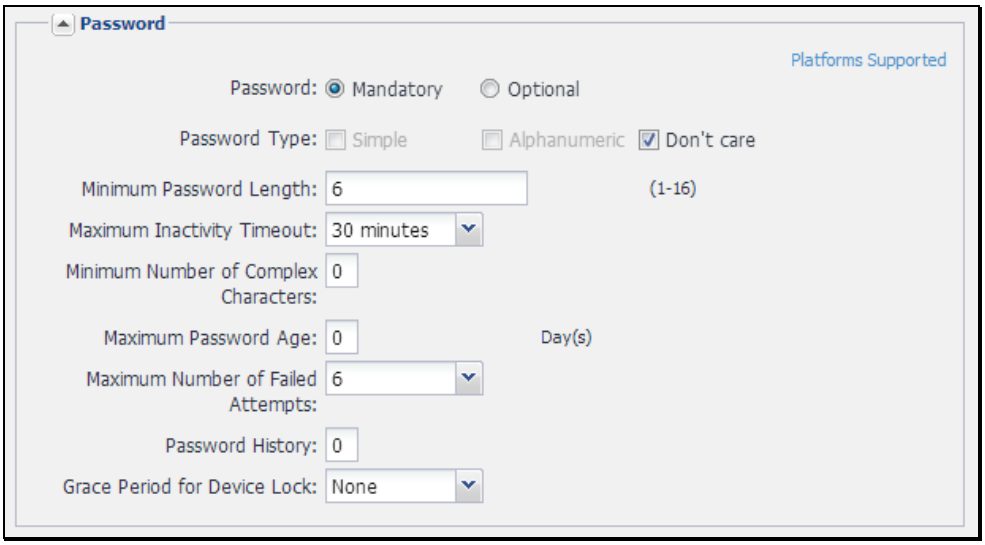


Illustration 2 : exemple de politique de mot de passe

3.2. Inventaire et monitoring

La console d'administration offre un aperçu de tous les appareils enregistrés. Pour chaque appareil, plusieurs données détaillées sont disponibles, comme le nom de l'utilisateur, le type d'appareil, la version du système d'exploitation… En outre, le statut de conformité par rapport aux politiques définies peut être suivi.

Illustration 3 : inventaire des appareils enregistrés

L'illustration suivante offre un exemple du statut d'un appareil concernant la politique de mot de passe. On voit que les règles sont respectées pour chacun des paramètres de l'appareil. Si « SD Card Encryption » n'est pas supporté, c'est tout simplement parce que l'appareil en question ne possède pas de slot pour carte SD.

Name	Setting Value	Device Value	Status
Password	Mandatory	Mandatory	✓
Password Type	Don't Care	Don't Care	✓
Maximum Inactivity Timeout	5 minutes	5 minutes	✓
Minimum Password Length	4	4	✓
Maximum Passcode Age	0 day	0 day	✓
Maximum number of Failed Attempts	6	6	✓
SD Card Encryption	Disabled	Unsupported	⚠
Device Encryption	Enabled	Enabled	✓

Illustration 4 : exemple de statut de conformité d'un appareil

3.3. Accès sécurisé aux ressources de l'entreprise

L'utilisateur d'un smartphone ou d'une tablette aura clairement plus d'utilité de son appareil s'il peut accéder aux ressources de l'entreprise comme la messagerie électronique, le calendrier, le répertoire des contacts et les documents.

Dans ce cadre, une solution MDM offre une fonction de passerelle : les appareils qui satisfont aux règles établies peuvent accéder à ces ressources d'entreprise. À l'inverse, si un appareil n'est pas conforme aux règles, l'accès sera bloqué et l'utilisateur pourra en être averti. Ce dernier sera alors invité à faire le nécessaire pour se mettre en règle et à nouveau avoir accès.

Ci-dessous est proposé un exemple d'appareil non conforme. Dans cet exemple, aucun mot de passe n'a été défini pour l'appareil. L'utilisateur peut maintenant être averti et être invité à rectifier la situation. Des alertes peuvent être envoyées par sms, par e-mail ou une notification push.

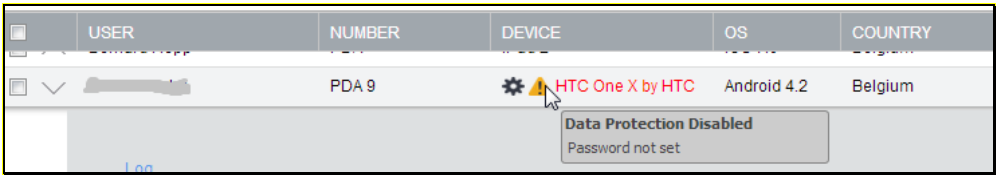


Illustration 5 : indication d'un appareil non conforme

Cette fonction de passerelle est tout d'abord axée sur la communication ActiveSync pour la synchronisation de la messagerie électronique, du calendrier et du répertoire des contacts : les appareils conformes sont autorisés à communiquer avec un serveur Microsoft Exchange ou Notes (via Notes Traveler).

Les fournisseurs de solutions MDM élargissent de plus en plus la fonction de la passerelle. Ainsi par exemple, une connexion sécurisée peut également être établie entre des apps et des serveurs back-end. Une app de synchronisation de fichiers (synchronisation et partage de fichiers) peut ainsi établir une connexion sécurisée avec un répertoire de documents internes.

3.4. Paramètres

La configuration de certains paramètres peut nettement faciliter la vie des utilisateurs. Des paramètres peuvent être configurés par un administrateur sur le serveur et être automatiquement forcés sur un appareil. Suivant la plateforme, il est possible de paramétrer entre autres les éléments suivants :

- Paramètres de la messagerie électronique (adresse du serveur, ...).
- Accès à un réseau Wi-Fi (SSID…).
- Paramètres VPN (type, adresse du serveur…).

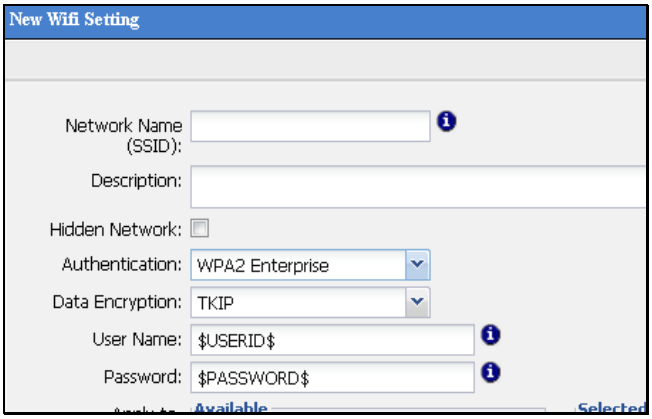


Illustration 6 : exemple de configuration Wi-Fi

3.5. Gestion des apps

Politiques

Un contrôle peut être effectué au niveau des apps installées sur un appareil. Il est ainsi possible de déterminer quelles apps sont autorisées, interdites ou obligatoires. Ces règles peuvent être imposées sur la base d'une politique. De même, la violation de la politique peut être soumise à des conséquences. Ainsi, l'accès aux ressources de l'entreprise (messagerie électronique, etc.) peut être refusé tant qu'une app interdite est installée ou qu'une app obligatoire n'est pas installée sur l'appareil.

À titre d'exemple, nous vous montrons ci-dessous comment une app non autorisée a été détectée sur un appareil.

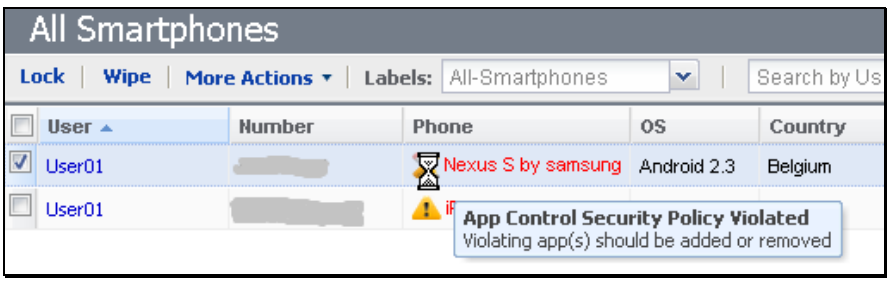


Illustration 7 : détection de la violation d'une politique en matière d'apps

L'aperçu détaillé de l'appareil indique l'application concernée (Beyond Tetris 1.1.2). L'utilisateur peut ensuite être invité à supprimer cette app.

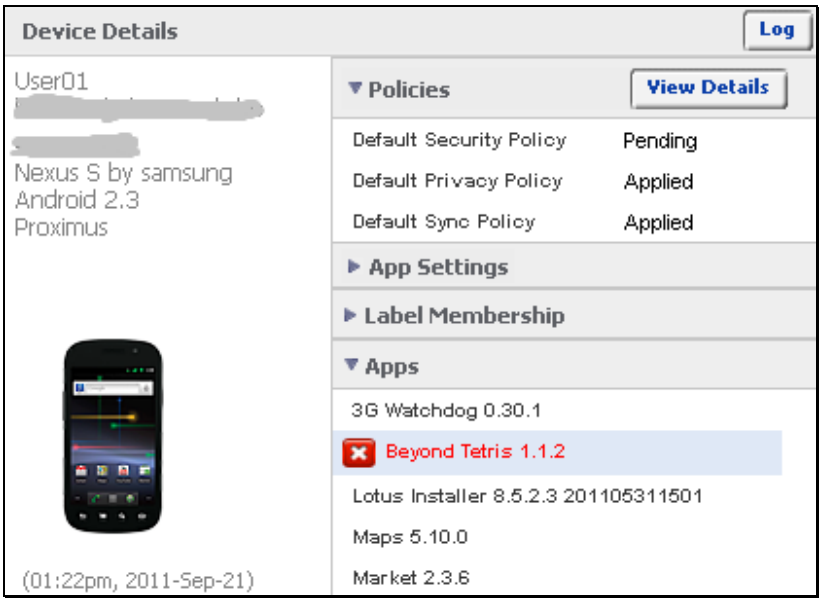


Illustration 8 : détection d'une app non autorisée

Inventaire

L'administrateur dispose d'un aperçu de toutes les apps actuellement installées sur les appareils gérés. Cet aperçu permet de voir quelles apps sont utilisées et lesquelles sont les plus populaires. En cas de malware connu, un administrateur peut vérifier si l'app porteuse de malware a été installée sur un appareil. Si tel est le cas, l'utilisateur peut être averti et sommé de supprimer l'app en question. Il peut éventuellement être recouru à un service de « App Reputation » comme Appthority[2] afin d'évaluer la fiabilité d'une app. Sur la base d'un rating, un tel service indique le degré de fiabilité d'une app.

Distribution

Une entreprise peut distribuer des apps via son propre *enterprise app store.*

- Des apps disponibles publiquement dans un app store officiel comme Google Play ou l'Apple App Store peuvent être recommandées via un enterprise app store. Si un utilisateur sélectionne une telle app, celle-ci est téléchargée depuis les app stores officiels.
- Des apps internes propres (in-house) peuvent également être distribuées via l'enterprise app store. Le téléchargement se fait alors directement sur le serveur MDM.

L'illustration ci-dessous montre une liste d'apps recommandées dans un enterprise app store.

[2] www.appthority.com

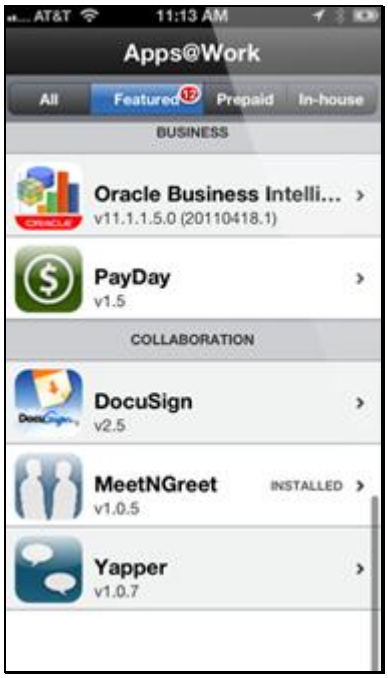


Illustration 9 : exemples d'apps recommandées dans un enterprise app store

3.6. Bloquer, effacer et localiser

Une solution MDM offre généralement plusieurs mesures concernant la perte ou le vol d'un appareil, qui consistent notamment à bloquer *(block)*, effacer *(wipe)* et localiser *(locate)* un appareil.

Bloquer

Il est tout d'abord possible de bloquer à distance l'écran d'un appareil. L'utilisateur doit alors réintroduire le mot de passe de son appareil. L'utilité d'un tel verrouillage est limitée, car il est peu probable qu'une personne malintentionnée s'empare d'un appareil dont l'écran n'est pas bloqué. Dans la pratique, cette mesure ne semble donc utile que lorsqu'un individu vole un appareil avec violence alors que l'écran est actif (non bloqué).

Effacer

S'il est possible de bloquer un appareil, il est aussi possible d'en effacer le contenu à distance. Une solution radicale consiste à effacer intégralement le contenu de l'appareil. Dans pareil cas, un *factory reset* est exécuté, c'est-à-dire que l'appareil est rétabli dans sa configuration d'usine.

Il est toutefois possible aussi d'effacer partiellement le contenu d'un appareil. Dans ce cas, seules les données d'entreprise sont supprimées de l'appareil, à savoir l'ensemble des données, des paramètres et des apps contrôlés par la solution MDM. Cette solution est bien plus intéressante pour les utilisateurs : si l'on retrouve l'appareil par la suite, on n'aura au moins pas perdu toutes les données personnelles comme les photos et la musique.

Localiser

Une dernière mesure dans le contexte du vol et de la perte d'appareils est la localisation. Le dernier emplacement connu d'un appareil peut être demandé via la console d'administration. Si l'appareil a été paramétré en ce sens par l'administrateur, l'utilisateur pourra également faire la manipulation lui-même sur un portail self-service.

Les données de localisation sont synchronisées à des moments réguliers entre le client MDM sur l'appareil et le serveur MDM. La localisation peut se faire de façon approximative à l'aide des mâts GSM ou avec plus de précision sur la base du GPS.

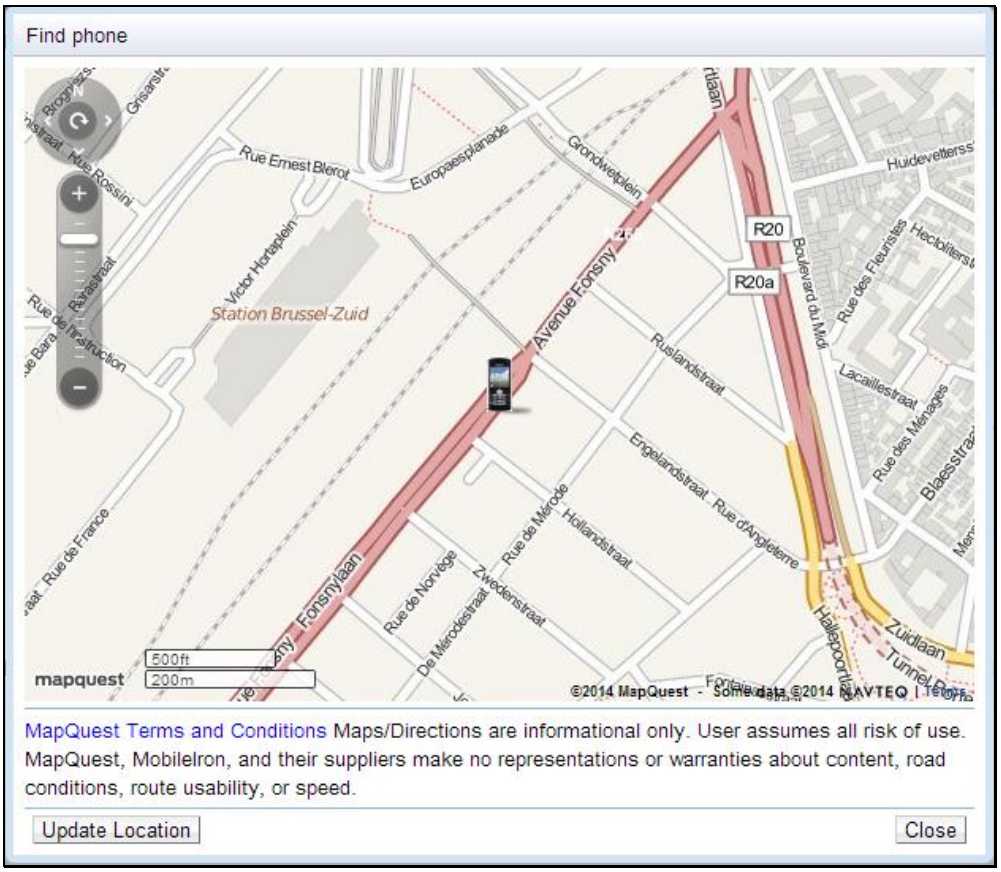


Illustration 10 : localisation d'un appareil

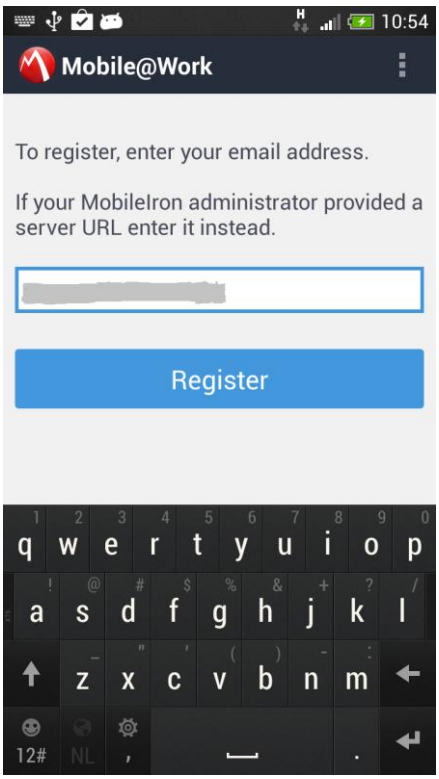
3.7. Portail self-service

Les utilisateurs ont parfois également la possibilité de gérer eux-mêmes en partie leur appareil via un portail self-service. Selon les droits dont ils disposent, ils peuvent alors par exemple localiser, bloquer ou effacer le contenu d'un appareil ou encore enregistrer un nouvel appareil.

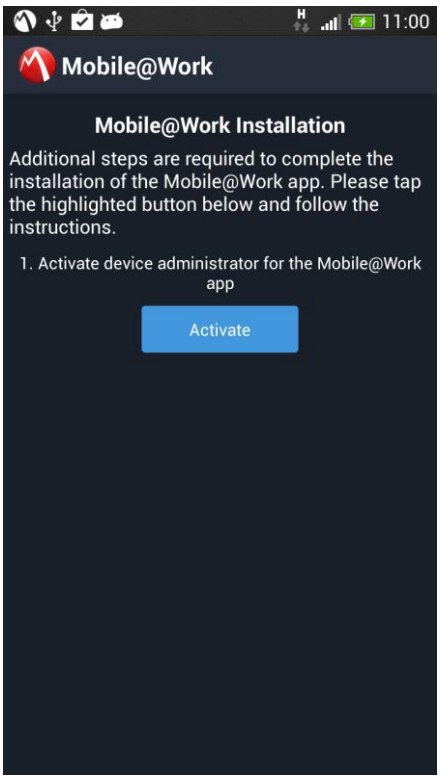
4. Processus d'enregistrement

Pour donner une idée de la façon dont s'effectue l'enregistrement d'un appareil dans une solution MDM, nous présentons ici dans les grandes lignes les démarches qu'un administrateur et un utilisateur final doivent entreprendre. C'est le support fourni par le helpdesk qui détermine qui exécute quelles tâches : configuration entière de l'appareil ou configuration au niveau du serveur seulement. Notez que cette procédure peut différer d'une plateforme à l'autre. À titre d'exemple, nous expliquons ci-après la procédure pour un appareil Android, illustrée par quelques captures d'écran.

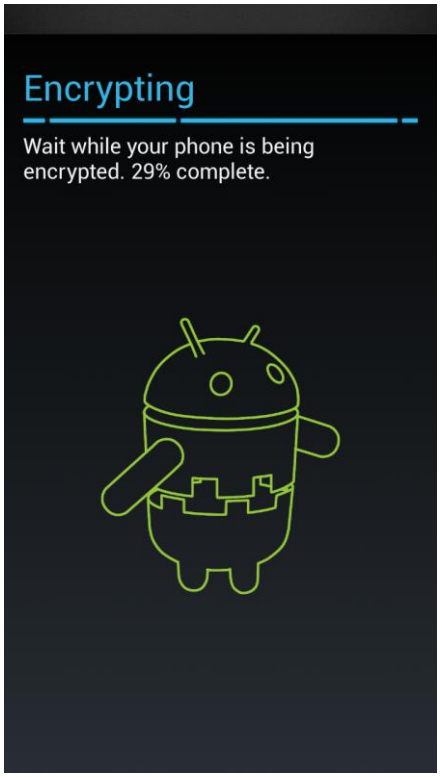
1. Création d'un utilisateur dans la solution MDM, éventuellement en relation avec un répertoire d'entreprise (LDAP).
2. Configuration du serveur de messagerie : octroi de droits d'accès à l'utilisateur.
3. Installation de l'app MDM sur l'appareil via les app stores officiels. L'installation requiert l'activation du *device administrator* pour l'app MDM. Cela signifie que l'app MDM reçoit des droits plus larges pour accomplir les tâches auxquelles elle est destinée.
4. Configuration de l'app MDM : saisie de l'adresse du serveur et des identifiants de l'utilisateur.
5. Configuration de l'appareil pour suivre les politiques, dont par exemple la définition d'un mot de passe et le chiffrement de l'appareil.
6. Configuration de la messagerie d'entreprise : un container sécurisé peut être utilisé sur l'appareil, comme Nitrodesk Touchdown ou un autre client de messagerie. Sa configuration peut se faire automatiquement. L'utilisateur doit uniquement saisir son mot de passe de messagerie.



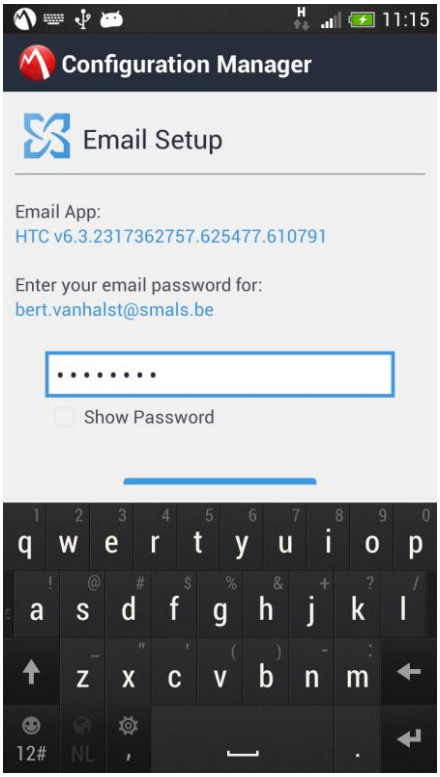
Configuration de l'app MDM



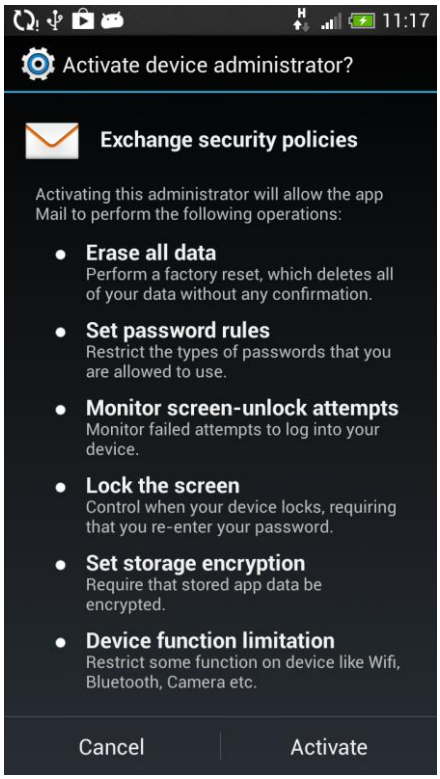
Activation de *device adminisrator*



Chiffrement de l'appareil



Configuration de la messagerie



Configuration des politiques de sécurité de la messagerie

5. Solution de Smals

Smals propose une solution pour la gestion des smartphones et tablettes et un accès sécurisé à la messagerie électronique, au calendrier et au répertoire des contacts via un serveur Exchange ou Notes.

En raison de la confidentialité des données, la solution est hébergée par Smals même et non chez un fournisseur de cloud externe.

La solution repose sur la technologie de MobileIron et offre un large éventail de fonctionnalités pour la gestion des appareils mobiles, comme un inventaire des appareils enregistrés, des politiques de sécurité (mot de passe de l'appareil, chiffrement des données présentes sur l'appareil) ainsi que le blocage, l'effacement du contenu et la localisation de l'appareil. Les politiques de sécurité sont ici en accord avec celles de l'extranet de la sécurité sociale.

6. Conclusion

Une solution de Mobile Device Management (MDM) nous permet d'imposer des règles de sécurité sur les smartphones et tablettes ainsi que d'offrir un accès sécurisé aux données d'entreprise comme la messagerie électronique, le calendrier et le répertoire des contacts.

Une solution MDM peut être mise en place non seulement pour les appareils qui sont la propriété de l'organisation, mais aussi pour les appareils privés des collaborateurs dans un contexte BYOD (Bring Your Own Device).

Les fournisseurs élargissent de plus en plus leur gamme de solutions MDM. Outre la simple et unique gestion des appareils, ils proposent désormais la gestion d'applications et de données. Il s'agit dans ce cadre de prêter attention à la distribution des apps et à la sécurisation toute particulière des données qui peuvent être consultées ou manipulées via certaines apps. On parle alors de Mobile Application Management (MAM) et de Mobile Content Management (MCM).

Cette technologie est donc encore en pleine évolution, de sorte qu'il convient de la suivre étroitement !