TRUST IN GERMAN SICHERHEIT

Document de présentation technique 0273

G DATA

Gestion des périphériques mobiles

TechPaper_#0273_2015_04_21

Développement d'applications G DATA

Table des matières

1. Introduction

Les administrateurs de systèmes et réseaux d'entreprise ont toujours géré des groupes homogènes de périphériques clients. Le processus de planification et de dimensionnement des clients réseau est géré quasiment exclusivement avec des ordinateurs de bureau. Cette prévisibilité a permis de simplifier le déploiement de l'infrastructure réseau, du matériel client et des applications en garantissant l'uniformité au niveau de l'ensemble des périphériques réseau. Cependant, depuis que les smartphones et les tablettes ont bouleversé l'univers de l'électronique grand public, le paysage technologique est bien plus complexe. Des tendances telles que la personnalisation des technologies de l'information et la tendance AVEC (apportez votre équipement personnel de communication) ont entraîné la diversification des périphériques utilisés en entreprise. Les administrateurs ont désormais pour tâche de fournir un large accès aux ressources tout en garantissant la sécurité. Ce document de présentation technique a pour objectif de décrire les tendances d'utilisation des smartphones et des tablettes dans les réseaux d'entreprise (chapitre 2), ainsi que les stratégies de gestion pratiques pour les administrateurs qui doivent faire face à une utilisation croissante des périphériques mobiles (chapitre 3). Le chapitre 4 traite de l'utilisation de l'application G Data Mobile Device Management.

2. Les périphériques mobiles dans l'entreprise

La vitesse d'adoption des technologies dans les environnements d'entreprise est bien inférieure à celle à laquelle les consommateurs adoptent les nouveaux périphériques. Même les produits qui peuvent facilement être intégrés aux procédures de travail doivent être soumis à des tests de compatibilité avec l'infrastructure de l'entreprise, un processus qui peut nécessiter beaucoup de temps et d'argent. Depuis qu'Apple a popularisé les périphériques mobiles avec le lancement de l'iPhone et de l'iPad, des centaines de millions d'utilisateurs, particuliers et professionnels, ne peuvent plus se passer de cette association d'une technologie moderne et d'une grande facilité d'utilisation. De nombreuses entreprises cherchent cependant toujours comment intégrer correctement ces périphériques à leur environnement. Ce retard dans l'adoption des technologies entraîne souvent des tensions entre les attentes des utilisateurs finaux et les fonctionnalités proposées par les solutions déployées au sein de l'entreprise. Deux grandes tendances de l'informatique d'entreprise illustrent ce problème : la personnalisation des technologies de l'information et la tendance AVEC (apportez votre équipement personnel de communication).

La personnalisation des technologies de l'information (en d'autres termes, l'influence des périphériques personnels des clients sur les solutions informatiques d'entreprise) s'est développée de manière importante. Les utilisateurs finaux sont habitués à bénéficier d'un réseau Internet mobile disponible en permanence, d'une messagerie électronique dans le nuage et de très nombreuses applications leur permettant de personnaliser leur expérience mobile. Aucun administrateur ne peut nier que ces services peuvent être très pratiques, certains de leurs avantages sont cependant en contradiction inhérente avec les structures informatiques d'entreprise. La vitesse à laquelle de nouvelles applications sont proposées pour les plates-formes mobiles dépasse de loin les capacités des administrateurs à tester la compatibilité et la sécurité de chaque application. L'utilisation de services dans le nuage implique souvent le stockage de données sur des serveurs gérés par des tiers. Les utilisateurs finaux s'attendent à ce que leurs périphériques leur proposent de tels services, toutes les entreprises ne sont cependant pas prêtes sur le plan technique à les offrir d'une manière conforme aux politiques informatiques.

Même si les services et périphériques mobiles ne sont pas activement déployés dans un environnement d'entreprise, cela ne signifie pas pour autant que les administrateurs ne les rencontrent pas du tout. Il s'agit de la tendance AVEC (apportez votre équipement personnel de communication) : les utilisateurs finaux apportent leurs périphériques au travail et s'attendent à pouvoir utiliser l'infrastructure de l'entreprise, comme l'accès Wi-Fi et les partages réseau. De même, de nombreuses configurations de serveurs de messagerie électronique permettent l'accès à distance à l'aide de périphériques mobiles, que le périphérique en question soit géré ou non. Cela entraîne souvent des réactions automatiques : pour éviter toute fuite de données sensibles ou toute infiltration de logiciels malveillants au niveau du réseau, les périphériques mobiles sont tous bloqués de l'infrastructure d'entreprise ou les fonctionnalités des périphériques sont limitées par des politiques particulièrement restrictives.

Cela peut sembler paralysant, il faut cependant comprendre que l'utilisation des périphériques mobiles au sein de l'entreprise n'est pas un phénomène tout noir ou tout blanc. La tendance AVEC et la personnalisation des technologies de l'information peuvent sembler déstabiliser un environnement parfaitement organisé, le déploiement de périphériques d'entreprise ou la gestion de périphériques personnels peut cependant présenter plusieurs avantages. L'utilisation d'une solution de gestion des périphériques peut permettre de tirer profit des aspects positifs de l'utilisation des périphériques mobiles tout en limitant ses effets au niveau du reste de l'infrastructure d'entreprise.

2.1. Avantages

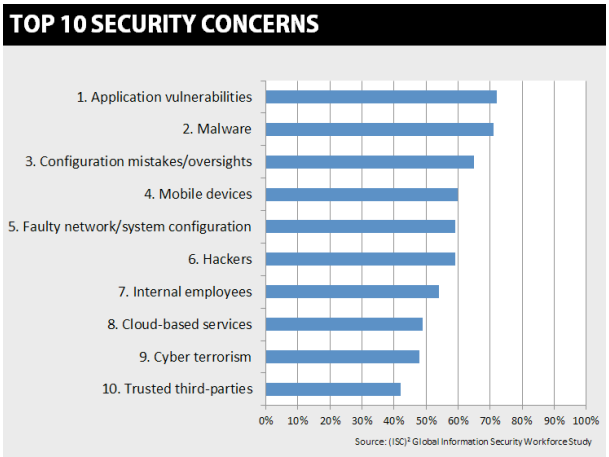
L'intégration des smartphones et des tablettes dans les procédures de travail de l'entreprise présente des avantages évidents, que le déploiement soit assuré de manière centralisée ou que les périphériques soient apportés par les employés. Proposer un accès mobile aux ressources de l'entreprise peut améliorer de manière importante la productivité des travailleurs à distance et des sous-traitants. L'association des contrôles d'accès et de la gestion des périphériques leur permet d'utiliser leurs périphériques de manière sûre et efficace pour accéder aux ressources de l'entreprise lorsqu'ils ne sont pas au bureau. Il est désormais possible de rester joignable en déplacement : les employés peuvent consulter leur messagerie électronique, leur calendrier et leurs notifications à distance.

Les applications et périphériques d'entreprise sont souvent plus complexes à utiliser alors que l'électronique grand public est conçue pour permettre aux utilisateurs finaux de se familiariser rapidement avec son utilisation. Cela réduit la courbe d'apprentissage pour les employés, qui peuvent vite s'habituer aux périphériques utilisés par l'entreprise.

Pour terminer, dans un environnement AVEC, les entreprises n'ont pas à investir des sommes importantes dans le déploiement de périphériques, cela leur permet de réaliser des économies. Plutôt que d'acheter et de déployer de nouveaux smartphones et de nouvelles tablettes, les périphériques des employés peuvent être dimensionnés avec le logiciel de gestion des périphériques et directement utilisés à des fins professionnelles. Les entreprises n'ont plus à assurer le remplacement des périphériques en cas de perte ou de casse d'un smartphone ou d'une tablette par un employé.

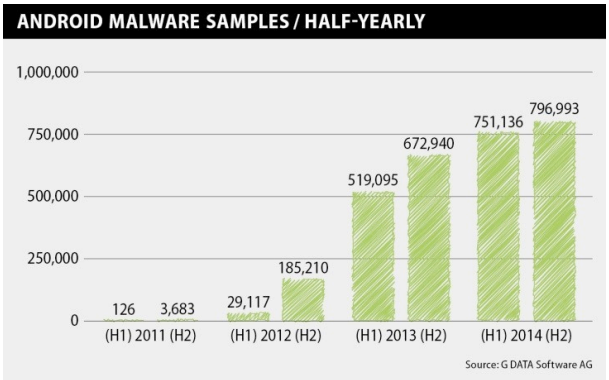
2.2. Risques

L'adoption des périphériques mobiles peut avoir de nombreux effets positifs sur la productivité de l'entreprise, elle présente cependant des défis. Les périphériques mobiles sont classés au quatrième rang des principaux problèmes de sécurité dans l'étude 2015 Global Information Security Workforce Study de la (ISC)2 Foundation[1]. Les périphériques mobiles sont, tout comme les PC, exposés aux logiciels malveillants. Les systèmes Android et iOS sont notamment les plus visés : avec une part de marché combinée de 96,3 %[2], ils sont une cible de choix pour les criminels. En 2014, les experts de la sécurité G Data ont étudié plus de 1,5 million de nouveaux logiciels malveillants Android, soit 30 % de plus qu'en 2013[3]. Les logiciels malveillants Android sont utilisés à une multitude de fins néfastes, dont :



- le vol de données, telles que des courriers électroniques, des données de connexion et des documents sensibles,
- l'envoi de SMS à des numéros de téléphone payants (à l'étranger), ce qui génère des coûts importants,
- l'espionnage d'applications bancaires mobiles,
- le verrouillage de périphériques dans le but d'obtenir une rançon (rançongiciel).

Les logiciels malveillants ne sont cependant pas la seule menace qui pèse sur les périphériques mobiles. Sur Internet, des sites d'hameçonnage peuvent pousser l'utilisateur à saisir des données personnelles de manière anodine en apparence. Et si le périphérique est sûr, cela ne signifie pas pour autant qu'il peut être utilisé en toute sécurité dans un contexte professionnel. Lorsque les employés accèdent à des documents d'entreprise via des périphériques mobiles, il faut veiller à ce que des informations sensibles ne puissent pas être divulguées, que ce soit par accident (lors du téléchargement vers un service de partage de fichiers, par exemple) ou de manière délibérée (menace interne).



Les périphériques mobiles peuvent présenter des risques au niveau de la sécurité mais également entraîner une baisse de productivité. L'utilisation des applications doit être limitée afin que les employés ne consacrent pas un temps excessif aux jeux et autres passe-temps. La gestion des contacts peut permettre de limiter l'utilisation des fonctionnalités du téléphone au strict nécessaire et de gagner ainsi du temps et de l'argent.

Les avantages de l'utilisation des périphériques mobiles dans l'entreprise l'emportent sur les risques. Ces

[1] Source : (ISC)2 Foundation, https://www.isc2cares.org/IndustryResearch/GISWS/

[2] CY14. Source : IDC, https://www.idc.com/getdoc.jsp?containerId=prUS25450615

[3] Source : rapport G DATA sur les logiciels malveillants mobiles, H2/2014

derniers doivent cependant être limités. Une politique de gestion des périphériques mobiles intégrée peut permettre de gérer les risques au niveau de la sécurité et les problèmes de productivité et de garantir un usage sûr et efficace des smartphones et des tablettes.

3. Gestion des périphériques mobiles

En tant qu'administrateur, il est quasiment impossible de ne pas prendre en compte des tendances telles que la personnalisation des technologies de l'information et la tendance AVEC. Les utilisateurs finaux continueront à demander des tablettes et des smartphones d'entreprise conformes au paradigme d'utilisation auquel ils sont habitués. En l'absence de déploiement actif de tels périphériques, ils apporteront les leurs. Si l'on considère les avantages que les périphériques mobiles peuvent présenter pour la productivité, l'objectif de la gestion des périphériques mobiles doit être d'augmenter la productivité tout en garantissant la sécurité et en réduisant les coûts.

3.1. Déploiement et administration

Les smartphones et les tablettes doivent être déployés avant d'être gérés par une solution de gestion des périphériques mobiles. Le déploiement implique une connexion initiale entre le périphérique et le serveur, le périphérique envoie ensuite régulièrement des rapports au serveur et peut être géré à distance. La communication entre le serveur et le périphérique a lieu sous la forme de trafic Internet (lorsqu'une connexion directe avec le serveur peut être établie), de messages poussés (souvent basés sur des solutions de messagerie dans le nuage propres au fournisseur) ou de SMS (en l'absence de connexion Internet mobile). Il n'est pas nécessaire de maintenir une connexion permanente entre le périphérique et le serveur : le périphérique peut exécuter les politiques du serveur même en l'absence de contact avec le serveur. Les périphériques sont alors protégés en permanence, même à l'extérieur de l'environnement de l'entreprise.

Le déploiement doit être rationalisé autant que possible. Les nouveaux périphériques gérés par l'entreprise doivent toujours être équipés de fonctionnalités de gestion des périphériques mobiles avant d'être remis aux employés. Les périphériques AVEC ne doivent pas pouvoir accéder au réseau de l'entreprise et à ses ressources avant d'être équipés d'un système de gestion des périphériques mobiles. Il est possible d'utiliser un réseau hôte pour les périphériques non conformes aux exigences ou pour les périphériques utilisés par des visiteurs.

Pour éviter une augmentation de leur charge de travail, les administrateurs doivent choisir une solution de gestion des périphériques qui s'intègre aux structures de gestion existantes. L'utilisation de plusieurs applications dorsales doit être évitée. Dans l'idéal, les périphériques mobiles peuvent être gérés à l'aide du même type d'interface et de fonctionnalités de rapport que celles disponibles pour d'autres types de périphériques du réseau pour permettre une procédure de travail intégrée et une configuration cohérente.

L'aspect juridique de la gestion des périphériques doit être pris en compte pour les périphériques AVEC. Ces périphériques n'appartiennent pas à l'entreprise, les administrateurs ne sont donc pas automatiquement autorisés à les gérer.

Des autorisations telles que l'effacement à distance, par exemple, peuvent poser problème. Selon la situation juridique, il est possible que les entreprises doivent demander l'autorisation de l'utilisateur final avant d'intégrer un périphérique à la solution de gestion des périphériques mobiles. Il est recommandé de définir un contrat de licence pour les utilisateurs finaux expliquant les actions que l'entreprise doit

pouvoir effectuer sur le périphérique. L'utilisateur final peut accepter ou refuser le contrat de licence pour les utilisateurs finaux mais il ne pourra accéder aux ressources de l'entreprise en cas de refus du contrat. Un contrat de licence pour les utilisateurs finaux peut être utile, même pour les périphériques non AVEC.

3.2. Antivol

Les périphériques mobiles augmentent les risques pour l'infrastructure physique et les procédures de travail basées sur des informations. Entre les employés qui emportent des fichiers sensibles avec eux en déplacement et les périphériques mobiles perdus ou volés, il est plus facile que jamais de divulguer accidentellement des informations confidentielles. Plusieurs mesures peuvent être définies pour empêcher l'accès aux courriers électroniques, documents et autres communications de l'entreprise lors de la perte ou du vol d'un périphérique. Pour commencer, il peut être utile de tenter de récupérer le périphérique. La localisation à l'aide de la technologie GPS ou par le biais du déclenchement d'une alerte peut être utile. Si la localisation du périphérique n'est pas une option ou ne fournit pas de résultats exploitables, vous pouvez le verrouiller de manière à ce qu'il ne puisse pas être utilisé. En dernier ressort, les périphériques peuvent être réinitialisés, toutes les données présentes sur le périphérique sont alors effacées.

3.3. Applications

Une partie du charme des périphériques mobiles réside dans le fait qu'il est possible de compléter leurs fonctionnalités par défaut en installant des applications. Cela peut être extrêmement utile, même dans le cadre d'une entreprise : des outils de productivité ou des applications de configuration peuvent augmenter de manière importante les utilisations possibles pour les périphériques mobiles. Les périphériques d'entreprise doivent également proposer un environnement contrôlé, les applications ne doivent pas causer de problèmes de compatibilité, divulguer des informations sensibles ou diffuser des logiciels malveillants. La gestion des applications est un moyen puissant de contrôler les fonctionnalités d'un périphérique mobile et d'assurer à la fois la sécurité et la facilité d'utilisation.

Il peut être difficile d'établir une distinction entre les bonnes et les mauvaises applications. Certaines applications, telles que les jeux, sont clairement inadaptées à des environnements d'entreprise. D'autres, telles que les services de stockage de fichiers en ligne, peuvent être utiles mais peuvent également présenter des risques pour la confidentialité. Même des applications qui semblent ne présenter aucun risque peuvent s'avérer nuisibles, parce qu'elles incluent des failles de sécurité, parce que leurs services dorsaux sont corrompus ou parce qu'elles transmettent des informations de manière non sécurisée. La productivité est également un facteur : les employés qui ont seulement besoin d'un smartphone pour passer des appels et prendre des rendez-vous doivent uniquement avoir accès au téléphone et au calendrier tandis que les employés qui travaillent sur des documents en déplacement doivent pouvoir accéder au navigateur, aux applications de bureau et autres composants nécessaires.

3.4. Protection en temps réel et protection à la demande

Les clients mobiles sont, comme les ordinateurs de bureau et les ordinateurs portables, exposés aux attaques en ligne. Les périphériques Android enracinés ne disposent pas de mécanismes de protection suffisants contre les applications malveillantes de sources inconnues. Cependant, même les applications

malveillantes qui parviennent à s'infiltrer dans les boutiques d'applications officielles peuvent avoir des conséquences graves. De même, certains sites Web peuvent tenter de diffuser des logiciels malveillants en tirant profit de failles dans le système d'exploitation ou en trompant l'utilisateur final. Sur les ordinateurs de bureau, des sites Web d'hameçonnage peuvent tenter de pousser les utilisateurs à communiquer leurs mots de passe ou autres données sensibles. Pour contrer ces menaces, il faut configurer des mesures de protection pour tous les périphériques mobiles gérés.

La protection en temps réel assure la protection permanente des périphériques sans nécessiter d'interaction de l'utilisateur. Elle inclut des technologies telles que la protection contre l'hameçonnage et des vérifications antivirus automatiques. La protection à la demande est au contraire uniquement activée lorsque l'utilisateur final ou l'administrateur la déclenche. Par exemple, il est possible de lancer manuellement une vérification antivirus pour s'assurer qu'aucune application malveillante n'a été précédemment installée sur le périphérique.

Les solutions de protection en temps réel et de la protection à la demande varient beaucoup en fonction de la plate-forme cliente. Les clients Android sont particulièrement sensibles aux applications malveillantes, les périphériques iOS sont, quant à eux, plus exposés à la perte de données et aux tentatives d'hameçonnage. Les solutions de gestion des périphériques mobiles doivent proposer des mesures adaptées de manière optimale à chaque plate-forme mobile : l'utilisation d'un même module pour tous les périphériques ne permet pas de contrer les nombreuses menaces auxquelles les périphériques doivent faire face.

3.5. Filtrage et gestion des contacts

Le contrôle des flux de communication peut être essentiel pour les périphériques utilisés dans un contexte professionnel. Le blocage d'applications peut être utile si la communication doit être totalement bloquée. Certains scénarios exigent cependant un filtre plus élaboré. Plutôt que de bloquer complètement l'application téléphonique si un périphérique doit uniquement être utilisé pour la communication professionnelle, les appels entrants et sortants peuvent être filtrés s'ils ne répondent pas aux critères de l'entreprise. Une entreprise qui fournit à ses employés des téléphones pour communiquer avec le siège lorsqu'ils sont en déplacement peut ainsi bloquer tous les appels téléphoniques à l'exception de ceux avec des contacts de l'entreprise préalablement approuvés.

La gestion du répertoire se trouve au centre de la gestion des contacts. Les contacts stockés sur le périphérique peuvent être synchronisés vers le serveur central et les administrateurs peuvent envoyer les derniers numéros de téléphone aux périphériques. La gestion des contacts peut, tout comme la gestion des applications, être utilisée pour des périphériques individuels, le mieux est cependant de l'associer à une gestion basée sur des groupes. Il est possible d'autoriser ou de bloquer des numéros de téléphone pour des groupes de périphériques ou d'envoyer un répertoire d'entreprise complet à tous les périphériques.

4. Utilisation de l'application G Data Mobile Device Management

G Data propose un module pour la gestion des périphériques mobiles dans le cadre de ses solutions professionnelles. Les solutions G Data AntiVirus Business, G Data Client Security Business, G Data Endpoint Protection Business et G Data Managed Endpoint Security incluent toutes le module Mobile Device Management avec prise en charge des systèmes iOS et Android. Ce module est totalement intégré aux autres composants des solutions professionnelles et peut être géré à partir de la même application (G Data Administrator). Cela présente un avantage évident par rapport aux solutions indépendantes, qui nécessitent une administration distincte et dont la courbe d'apprentissage est souvent prononcée.

4.1. Android

Le module G DATA Mobile Device Management pour Android est disponible avec la solution G Data Internet Security pour Android. Les fonctionnalités de l'application sont gérées de manière centralisée via la solution G Data Administrator et incluent toute une série de fonctions de sécurité et de productivité pour tous les périphériques équipés du système d'exploitation Android version 2.3 ou une version plus récente.

4.1.1. Déploiement et administration

La première étape consiste à déployer le module G Data Internet Security pour Android sur tous les périphériques Android. Pour veiller à ce que seuls les clients réseau autorisés puissent se connecter au serveur, un mot de passe doit être défini du côté du serveur avant le déploiement des clients. Le même mot de passe devra ensuite être saisi dans l'application pour permettre son authentification au niveau de l'application G Data ManagementServer. Les installations de clients sont initiées à l'aide de l'application G Data Administrator. Le processus de déploiement est effectué par courrier électronique. Un courrier électronique d'activation contenant un lien vers le fichier d'installation peut être envoyé à une ou plusieurs adresses électroniques. Une fois le fichier téléchargé sur le client Android et les autorisations demandées confirmées, l'application G Data Internet Security pour Android est installée et peut être lancée à partir du menu des applications Android. Pour terminer le déploiement, l'application Android doit être connectée au ManagementServer ; elle se connecte ensuite au serveur et télécharge immédiatement la configuration de gestion des périphériques mobiles par défaut.

Une fois le périphérique connecté au ManagementServer, il s'affiche automatiquement dans l'application G Data Administrator. Les périphériques Android étant répertoriés en tant que clients dans la liste des clients normaux, ils peuvent être placés dans des groupes. La création d'un groupe dédié est recommandée, avec des sous-groupes pour les différents types d'accès aux périphériques (entreprise, privé ou mixte), pour les différents services utilisant des périphériques Android ou pour tout autre service. Cela permet une administration efficace et le périphérique peut ainsi automatiquement récupérer les paramètres corrects.

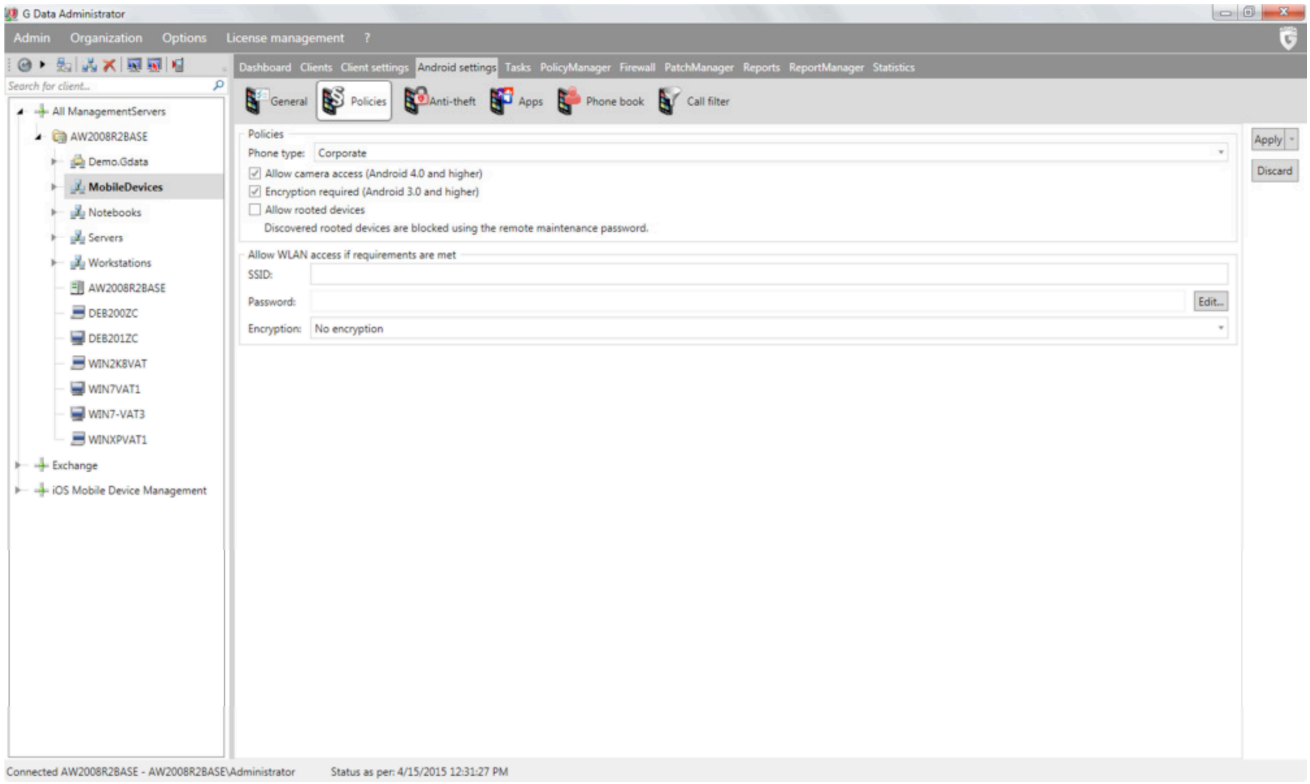


Image 1 : G Data Administrator, paramètres Android, politiques

Pour chaque périphérique ou groupe, un type de téléphone peut être défini sous PARAMÈTRES ANDROID > POLITIQUES. Pour les périphériques fournis par l'entreprise et uniquement destinés à l'usage de l'entreprise, le type de téléphone ENTREPRISE est recommandé. Les menus de paramétrage de l'application Internet Security pour Android sont alors verrouillés du côté client, les utilisateurs ne peuvent donc pas modifier par accident les paramètres gérés lors de la connexion au réseau de l'entreprise. Le type de téléphone PRIVÉ peut être utilisé pour les périphériques non fournis par l'entreprise. Cela permet à l'utilisateur final d'accéder pleinement aux paramètres de l'application Internet Security pour Android. Le type de téléphone MIXTE est utilisé pour les périphériques fournis par l'entreprise qui sont utilisés pour des communications aussi bien professionnelles que privées.

Certains paramètres de base doivent être configurés juste après le déploiement d'un nouveau périphérique. Une synchronisation et un planning de mise à jour doivent toujours être définis. Les deux paramètres dépendent de l'usage du périphérique. Les périphériques souvent connectés à un réseau sans fil (réseau local sans fil) peuvent être configurés pour mettre automatiquement les signatures antivirus à jour et synchroniser les données avec l'application ManagementServer plusieurs fois par jour. Les périphériques principalement utilisés à l'extérieur du réseau de l'entreprise ou qui se connectent à Internet à l'aide d'un plan de données mobiles peuvent être configurés de manière à ce que les mises à jour soient effectuées moins souvent, manuellement ou uniquement lors de la connexion via Wi-Fi. La même chose s'applique à la synchronisation : il est possible de configurer des paramètres différents pour les plans de données mobiles et Wi-Fi. Si nécessaire, il est possible d'affecter un contrat de licence pour les utilisateurs finaux aux périphériques. Les entreprises peuvent avoir l'obligation légale d'informer les utilisateurs finaux que leur périphérique peut être géré à distance.

4.1.2. Antivol

Les mesures antivol peuvent être déclenchées automatiquement ou manuellement. Certaines peuvent être configurées de manière à être exécutées en cas d'événement au niveau du périphérique (changement de carte SIM, par exemple). D'autres peuvent être déclenchées à l'aide de l'application G Data Administrator pour envoyer une commande via Google Cloud Messaging. Pour terminer, des commandes peuvent être envoyées par SMS.

Pour activer toutes les mesures, plusieurs paramètres doivent être configurés sous PARAMÈTRES ANDROID > ANTIVOL. Pour utiliser des commandes SMS, un mot de passe de maintenance à distance (un code PIN numérique) doit être saisi. Il servira également de mot de passe de l'écran de verrouillage si aucun mot de passe n'a été défini de manière explicite. Un numéro de téléphone certifié doit être défini pour veiller à ce que la commande de réinitialisation du mot de passe de maintenance à distance ne puisse être envoyée à n'importe qui, la réinitialisation du téléphone n'aura lieu que si la commande est envoyée depuis le numéro de téléphone certifié. Pour terminer, une adresse électronique doit être saisie pour recevoir un retour des actions en fournissant un.

En cas de perte ou de vol d'un périphérique, le moyen le plus rapide d'exécuter une action sur le périphérique est de lui envoyer un SMS. Les administrateurs peuvent sélectionner les commandes individuelles qui peuvent être envoyées au périphérique. Les mesures suivantes sont disponibles :

- Envoi à l'administrateur d'un courrier électronique avec les données de localisation.
- Réinitialisation du périphérique. Toutes les données personnelles seront effacées.
- Déclenchement d'une alarme sonore.
- Mise en sourdine de toutes les sonneries, à l'exception de celle déclenchée par l'option d'alarme sonore.
- Activation de l'écran de verrouillage à l'aide du mot de passe de l'écran de verrouillage.
- Définition du mot de passe de l'écran de verrouillage.

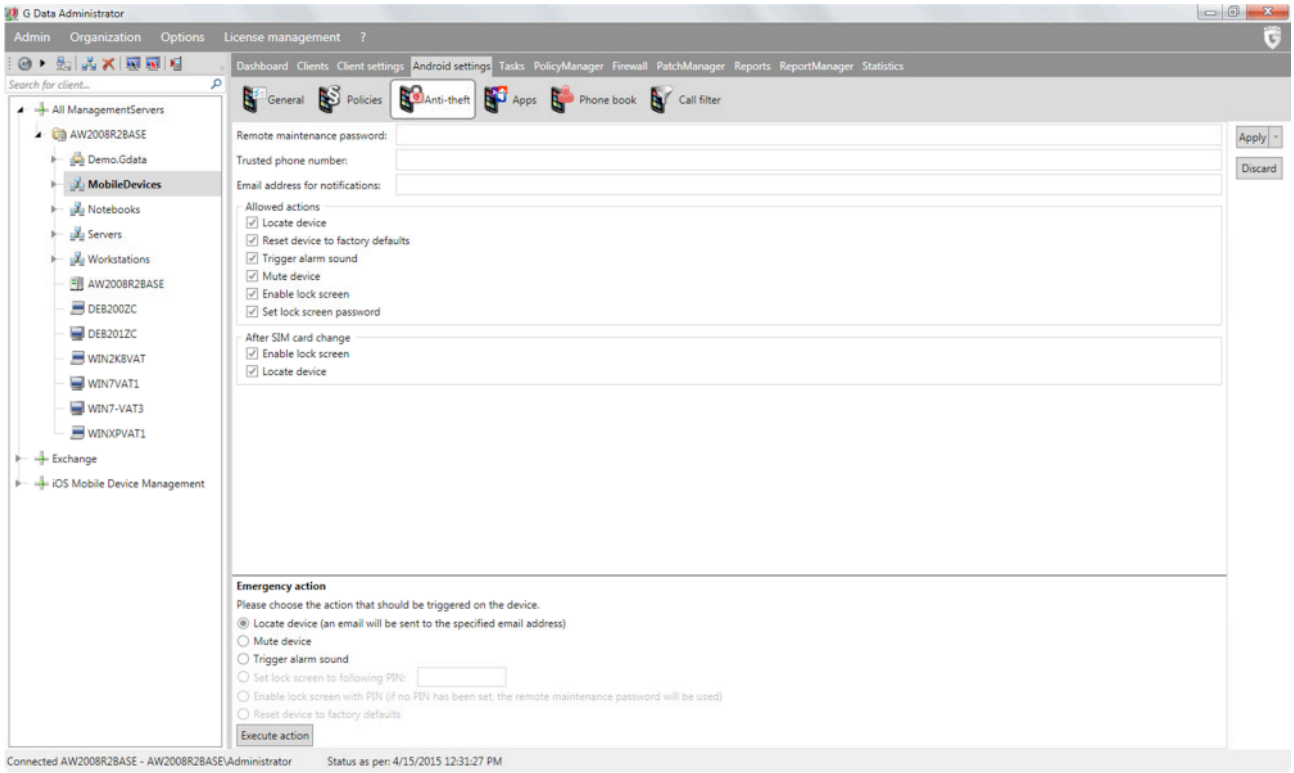


Image 2 : G Data Administrator, paramètres Android, antivol

Lorsqu'un périphérique est volé, sa carte SIM est souvent retirée pour empêcher le propriétaire d'origine de contacter le périphérique via son numéro de téléphone. Les SMS ne sont donc pas remis au périphérique. Pour résoudre ce problème, vous pouvez définir des actions qui doivent automatiquement être effectuées en cas de changement de carte SIM. L'écran de verrouillage du téléphone peut être activé, le périphérique est alors inaccessible et peut être localisé. Parallèlement aux mesures basées sur la carte SIM et les SMS, plusieurs actions peuvent également être lancées via l'application G Data Administrator. Il n'est pas nécessaire que le périphérique soit connecté au réseau ManagementServer pour que cela fonctionne : il s'appuie sur Google Cloud Messaging, un service en ligne de Google qui vous permet d'envoyer des commandes aux périphériques Android[4].

Les actions antivol peuvent affecter de manière importante la capacité à utiliser le téléphone (en supprimant les données du téléphone, par exemple), il est recommandé d'informer l'utilisateur par le biais d'un contrat de licence pour les utilisateurs finaux.

4.1.3. Applications

G Data Mobile Device Management pour Android offre des possibilités de gestion des applications complexes. L'application peut être utilisée pour répertorier les applications utilisées par les périphériques mobiles du réseau. Chaque application installée est répertoriée avec son nom, sa version et sa taille. Pour chaque application, les administrateurs doivent obtenir des informations au sujet du fournisseur, des fonctions et de l'historique des versions dans la mesure où des sources d'informations sont disponibles. La ou les boutiques officielles de nombreuses applications fournissent suffisamment de détails. Pour

[4] Vous devez disposer d'un compte Google Cloud Messaging, que vous pouvez ouvrir gratuitement sous https://code.google.com/apis/console/.

d'autres applications, il peut être nécessaire de faire des recherches sur la page d'accueil du fournisseur. Les applications peuvent être ajoutées à la liste blanche ou à la liste noire en fonction de ces informations et de l'utilisation prévue du périphérique (en fonction du type et du groupe de périphériques et de la zone du réseau). Cela permet d'autoriser ou de bloquer les applications répertoriées. L'exécution des applications est bloquée à l'aide du mode de passe défini.

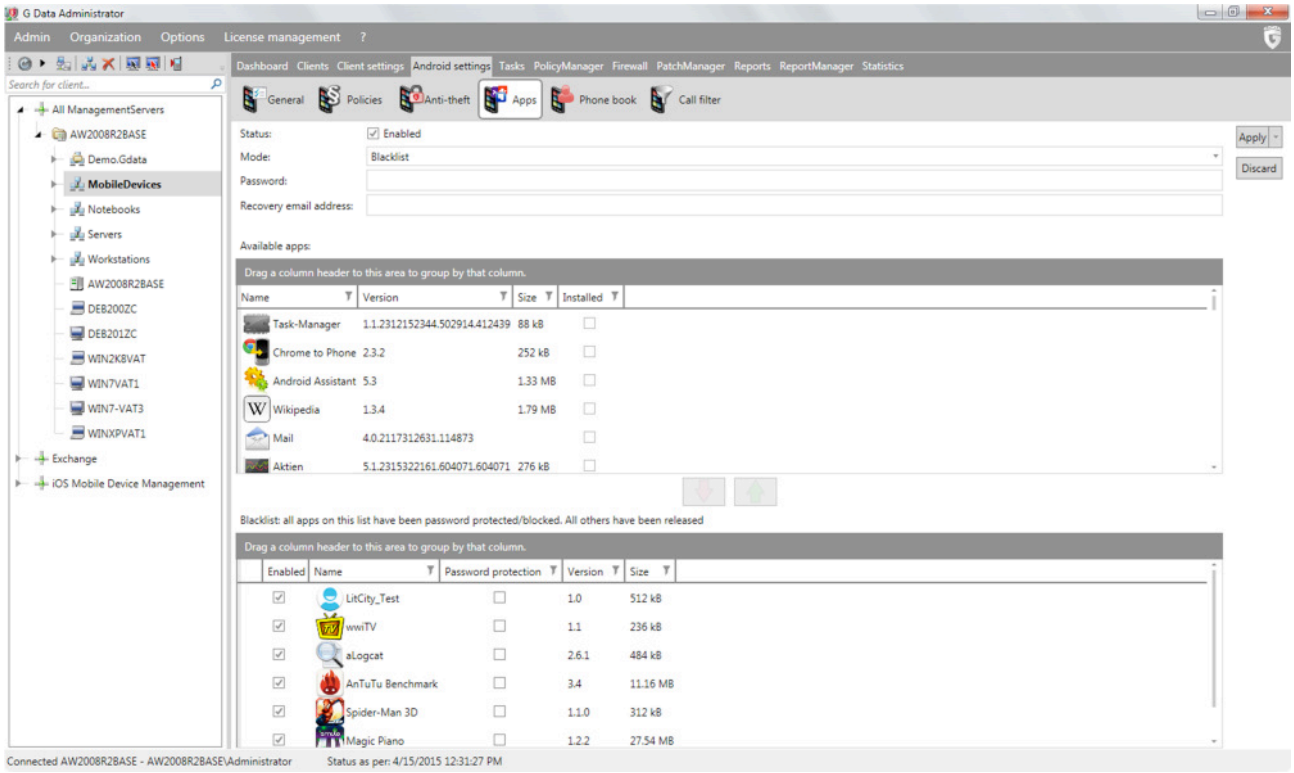


Image 3 : G Data Administrator, paramètres Android, applications

Pour décider si vous devez utiliser une approche basée sur une liste noire ou une liste blanche, vous devez vous baser sur la mesure dans laquelle le périphérique doit être bloqué. Si la gestion des applications est utilisée en mode liste noire, elle peut facilement être configurée pour des périphériques multi-usages sur lesquels l'utilisateur final doit pouvoir installer de nouvelles applications sans disposer d'une autorisation préalable. Le risque réside dans le fait que toutes les applications peuvent être installées et exécutées. Les utilisateurs ne peuvent plus accéder aux applications qu'une fois celles-ci bloquées manuellement par un administrateur. Les listes blanches sont une méthode plus sûre mais plus restrictive : les applications ne peuvent être utilisées que si elles ont été ajoutées à la liste blanche. Cela est particulièrement utile lorsqu'un périphérique est configuré pour un seul usage. Les administrateurs peuvent alors préinstaller les applications requises, les ajouter à la liste blanche et refuser l'accès à toutes les autres applications.

Si l'objectif est uniquement de bloquer quelques applications connues tout en laissant à l'utilisateur une relative liberté, l'approche basée sur une liste noire suffira. Le minimum est cependant de protéger les paramètres Android et la sécurité Internet avec un mot de passe. Cela permet d'éviter que les utilisateurs finaux ne modifient les paramètres. L'ajout de la boutique d'applications officielle à la liste noire permet de s'assurer qu'aucune autre application ne puisse être installée. Pour contrôler totalement les applications d'un périphérique, l'approche basée sur une liste blanche est l'option la plus fiable. Les applications de la liste blanche peuvent être utilisées sans aucune limitation, les autres applications sont

cependant bloquées. Cette option est très utile pour les périphériques configurés pour une sécurité maximale ou pour une seule procédure de travail. Par exemple, un périphérique qui doit uniquement être utilisé par des représentants commerciaux peut fonctionner en mode liste blanche, seuls le composant téléphonique et l'ordinateur frontal de la base de données commerciale peuvent alors être utilisés.

4.1.4. Protection en temps réel et protection à la demande

La protection en temps réel contre les logiciels malveillants est disponible via les modules PROTECTION WEB et VÉRIFICATION ANTIVIRUS. Il est également possible de limiter les fonctionnalités via l'onglet POLITIQUES de l'application G Data Administrator.

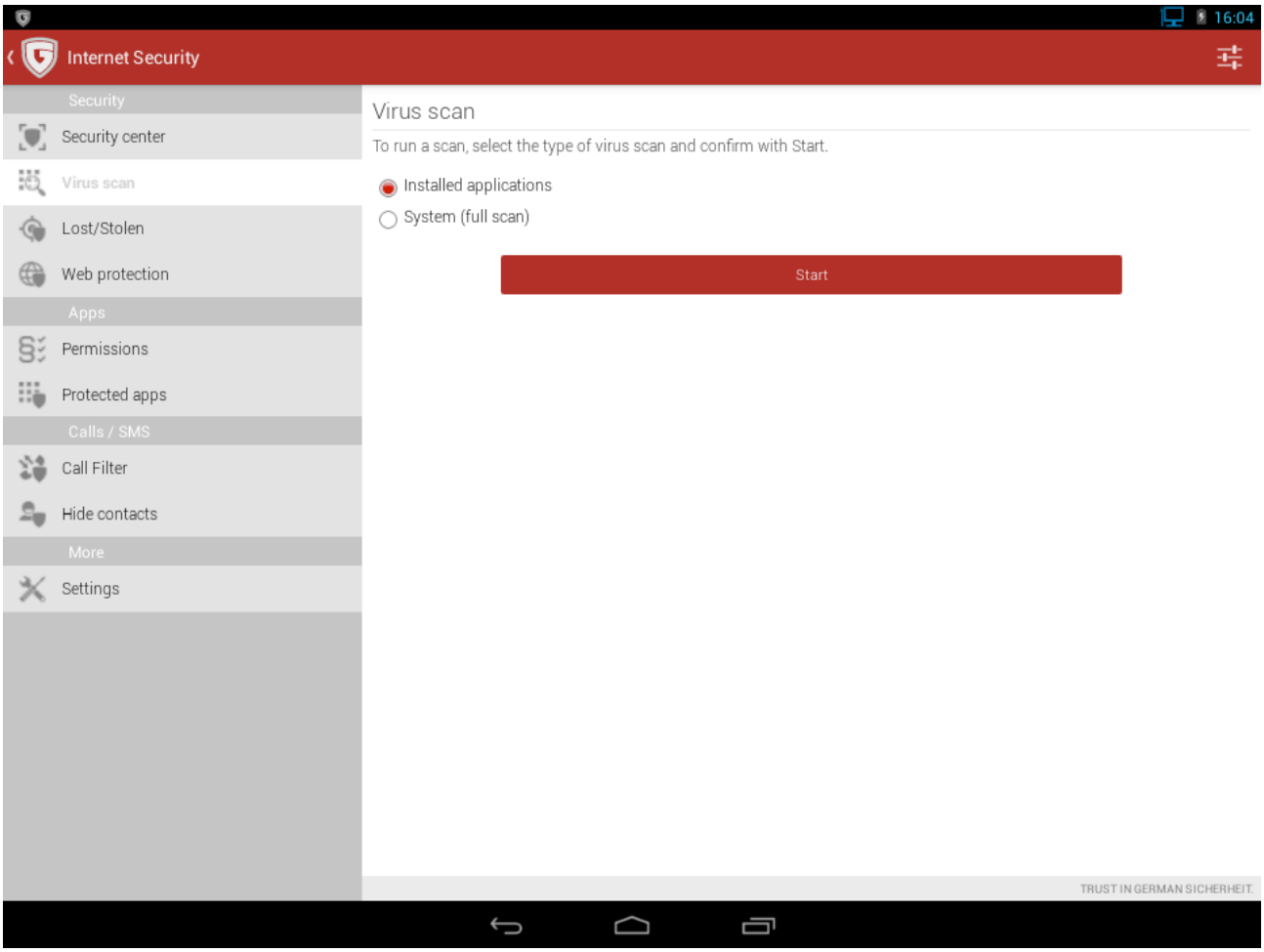


Image 4 : G Data Internet Security pour Android, sécurité, analyse antivirus

La protection Web assure la protection en temps réel lors de l'utilisation du navigateur Android. La protection Web peut produire une faible quantité de trafic de données, elle peut donc être configurée pour fonctionner uniquement lorsque le périphérique est connecté via Wi-Fi. La vérification antivirus s'assure de manière transparente de l'absence de logiciels malveillants dans les applications téléchargées et bloque l'installation si des logiciels malveillants sont détectés.

La protection à la demande contre les logiciels malveillants est disponible sous la forme d'une vérification antivirus complète pour l'intégralité du périphérique. Une vérification régulière de toutes les applications

est recommandée pour s'assurer de l'absence de logiciels malveillants sur les supports de stockage (cartes SD, par exemple). Selon la fréquence d'utilisation du périphérique et la fréquence d'installation et d'enregistrement de nouveaux logiciels, l'intervalle peut être défini sur un jour, trois jours, sept jours, quatorze jours ou trente jours. Il est généralement recommandé de procéder à une vérification quotidienne : l'analyse n'entraîne pas de ralentissements notables et assure une sécurité maximale. Pour vous assurer que la vérification antivirus n'épuise pas la batterie du périphérique, vous pouvez la configurer de manière à ce qu'elle ait uniquement lieu lors du rechargement du périphérique.

Sur les périphériques Android, la principale menace provient des périphériques enracinés. Si l'utilisateur final dispose d'un accès racine au périphérique, il est facile de contourner la sécurité au niveau du système d'exploitation et des applications et si un logiciel malveillant parvient à infecter le périphérique, il pourra accéder de manière quasiment illimitée aux fonctions du système d'exploitation. Pour conserver le contrôle des périphériques mobiles gérés, nous vous recommandons donc de refuser l'accès réseau aux périphériques enracinés via l'onglet POLITIQUES. De plus, l'administrateur peut activer ou désactiver l'accès aux appareils photo (pour les périphériques utilisant le système d'exploitation Android version 4.0 ou supérieure) et/ou le chiffrement des mandats pour protéger les données stockées sur le périphérique.

4.1.5. Filtrage et gestion des contacts

Le répertoire de l'entreprise peut être utilisé pour gérer les contacts sur les périphériques Android. Il est possible, sans utiliser les possibilités de filtrage, de garantir efficacement le contrôle des contacts en bloquant le répertoire intégré au périphérique et en renseignant le répertoire d'entreprise de l'application Internet Security pour Android. Avec le module de filtrage des appels, cela offre des possibilités de filtrage et de gestion des contacts complètes.

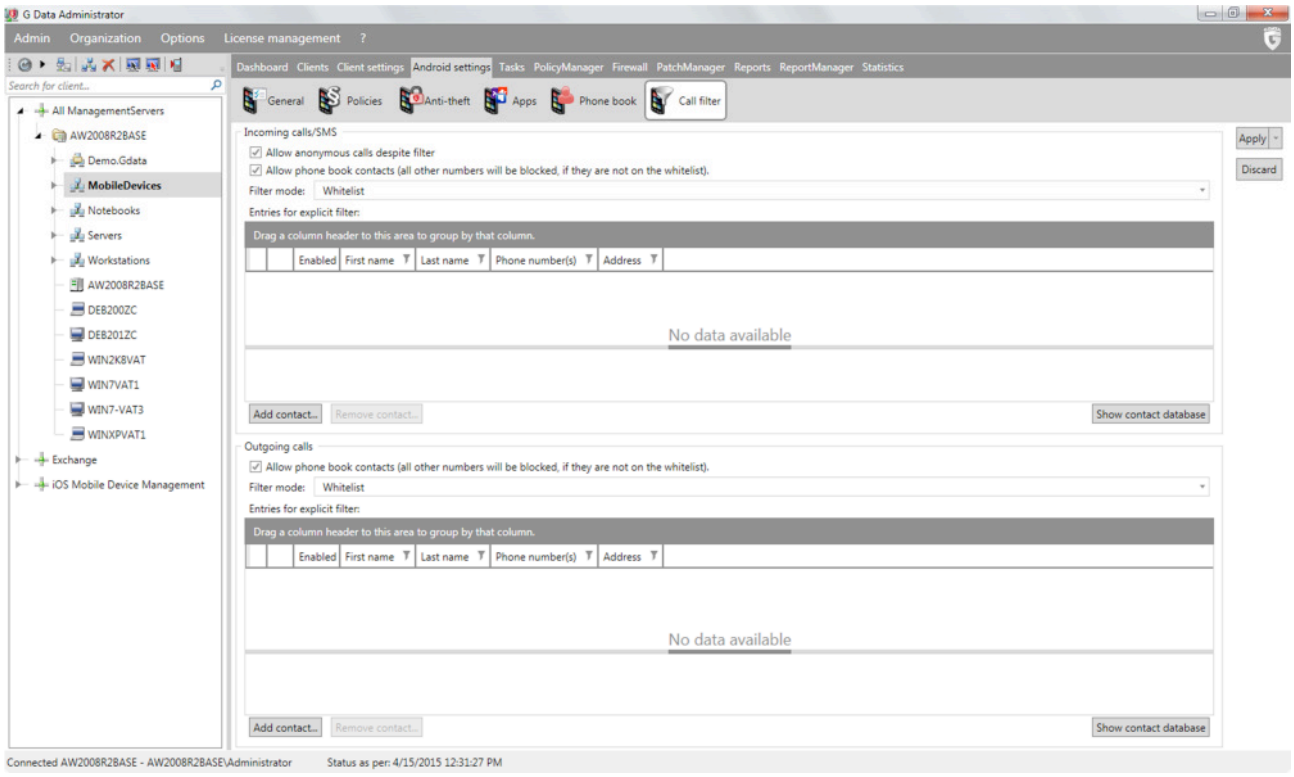


Image 5 : G Data Administrator, paramètres Android, filtrage des appels

La base de données des contacts constitue la base de toutes les fonctionnalités. Elle fait office de concentrateur central pour tous les contacts d'entreprise, en fonction desquels des répertoires pour différents périphériques, ainsi que des filtres de SMS et d'appels ciblés peuvent être créés. Pour les organisations avec un nombre de contacts limité ou pour les petits répertoires gérés, la saisie manuelle de contacts est un moyen pratique de renseigner rapidement la base de données de contacts. Les contacts peuvent être importés si le réseau utilise Active Directory. Une fois tous les contacts définis, ils peuvent être distribués aux périphériques adaptés. Il est ainsi possible de fournir à tous les périphériques une liste complète des numéros directs des collègues. Il est également possible d'autoriser uniquement l'accès de groupes de périphériques à certains numéros de téléphone explicitement déployés dans le répertoire, en association avec le blocage du répertoire standard et l'utilisation du filtre d'appels.

Le filtre d'appels peut également être utilisé pour le filtrage complet des communications entrantes et sortantes. Il fait office de filtre du répertoire intégré au périphérique. Plutôt que de bloquer complètement le répertoire Android, le filtre permet un contrôle granulaire des flux de communication. Par exemple, lorsque le mode basé sur une liste blanche est activé, les appels entrants et sortants ne sont pas autorisés, sauf ceux dont les numéros ont été ajoutés à la liste blanche. En mode basé sur une liste noire, la communication est généralement autorisée, des numéros spécifiques peuvent cependant être bloqués. Un filtre supplémentaire permet la communication avec les contacts des répertoires Android et Internet Security tout en bloquant tous les autres (les contacts de la liste blanche étant la seule exception).

4.2. iOS

L'application G Data Mobile Device Management pour les périphériques iOS a été conçue comme solution sans agent pour le système d'exploitation iOS version 7.0 ou supérieure. G Data Administrator permet de déployer des profils de politiques au niveau d'un ou plusieurs périphériques iOS. Cela permet aux administrateurs de gérer les périphériques de manière flexible tout en conservant un contrôle maximal sur leur utilisation.

4.2.1. Déploiement et administration

Les déploiements de clients iOS peuvent être initiés à partir de l'application G Data Administrator. Le processus de déploiement est effectué par courrier électronique. Dans la zone de gestion des clients, sélectionnez n'importe quel nœud sous GESTION DES PÉRIPHÉRIQUES MOBILES IOS, cliquez sur le bouton de la barre d'outils ENVOYER LE LIEN D'INSTALLATION AUX CLIENTS MOBILES et saisissez une liste d'adresses électroniques. Il est possible de saisir certains paramètres pour personnaliser l'aspect de la demande MDM sur le périphérique. Le NOM, la DESCRIPTION et l'ORGANISATION sont affichés dans la demande MDM et également par la suite, au niveau de l'onglet GÉNÉRAL des PARAMÈTRES IOS. Le CONTRAT DE LICENCE POUR LES UTILISATEURS FINAUX peut être utilisé pour informer l'utilisateur final du fait que le périphérique sera géré à distance.

Lorsque l'utilisateur final ouvre le lien du courrier électronique d'installation sur un périphérique iOS, le périphérique s'affiche immédiatement dans l'application G Data Administrator (avec le STATUT DE SÉCURITÉ de l'onglet CLIENTS détaillant son statut en attente). Dès que l'utilisateur final accepte la demande MDM, le périphérique iOS peut être pleinement géré via G Data Administrator.

Lorsqu'un périphérique iOS est sélectionné dans G Data Administrator, un ensemble de modules MDM

iOS devient disponible. L'onglet CLIENTS (IOS) affiche une vue d'ensemble des périphériques iOS gérés. Pour chaque client, plusieurs propriétés spécifiques du périphérique sont affichées, telles que le numéro IMEI, la version du système d'exploitation iOS et le nom du produit. La colonne STATUT DE SÉCURITÉ affiche des avertissements pour les périphériques sans profil de politique, ainsi que les alertes relatives au statut d'installation MDM. Le module PARAMÈTRES IOS permet aux administrateurs de configurer des mesures antivol (reportez-vous au chapitre 4.2.2), ainsi que des profils de politiques (reportez-vous au chapitre 4.2.3). Le module RAPPORTS (IOS) peut être utilisé pour suivre le statut de différents messages poussés, le principal mode de communication entre G Data ActionCenter et les périphériques iOS. Les rapports incluent le statut de déploiement des profils et les confirmations des fonctions antivol.

4.2.2. Antivol

Lors de la perte ou du vol d'un périphérique, la première mesure à prendre est de veiller à ce que personne ne puisse accéder aux données du périphérique. Le périphérique peut ensuite être localisé à l'aide du GPS (pour trouver et récupérer le périphérique) ou une mesure plus drastique, qui consiste à effacer le périphérique, peut être prise (s'il n'y a aucune chance de trouver et de récupérer le périphérique). Apple propose aux utilisateurs iCloud enregistrés une fonctionnalité leur permettant de trouver leur iPhone. Les utilisateurs peuvent se connecter à un site Web dédié pour verrouiller, suivre ou effacer un périphérique.

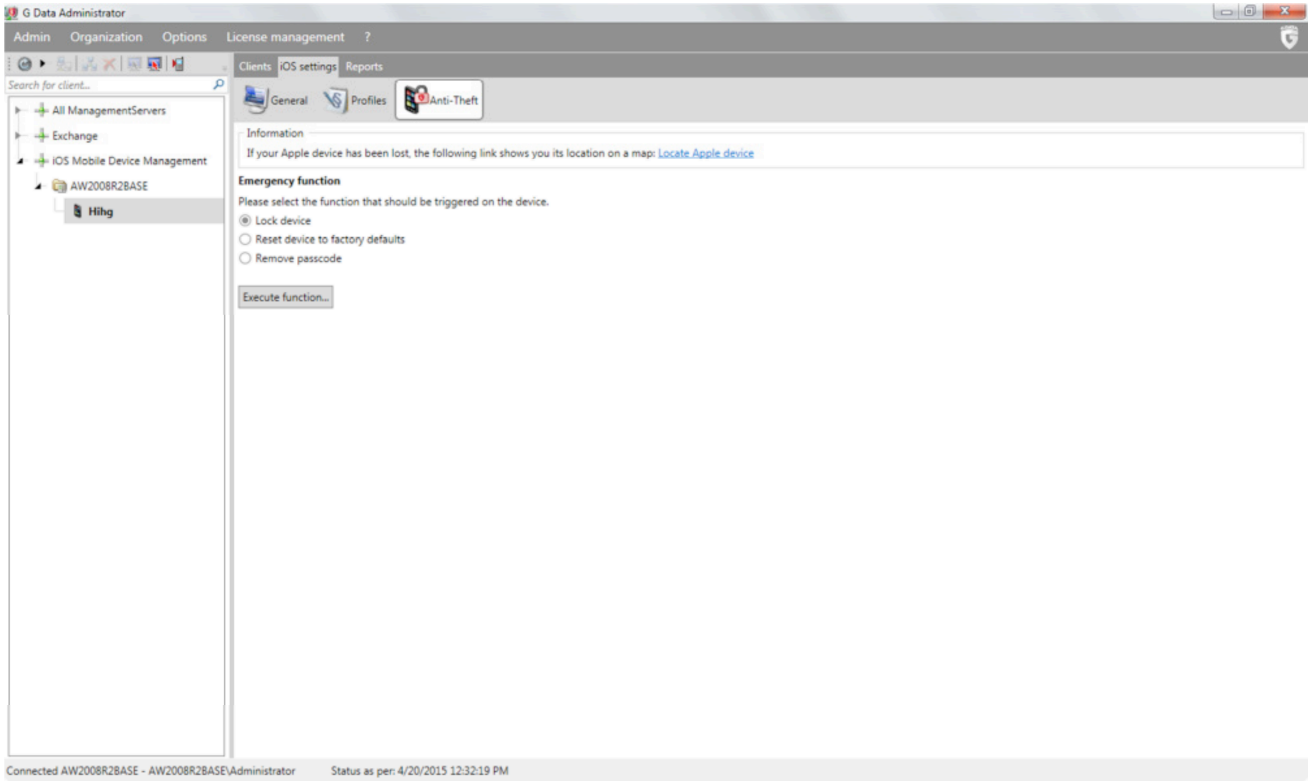


Image 6 : G Data Administrator, paramètres iOS, antivol

En guise d'alternative à cette fonctionnalité, le module PARAMÈTRES IOS permet aux administrateurs de déclencher des fonctions antivol sur l'onglet ANTIVOL sans qu'ils aient besoin de se connecter à un site Web externe. Les fonctions de réinitialisation et de verrouillage du périphérique peuvent être déclenchées en sélectionnant l'option correspondante et en cliquant sur EXÉCUTER LA FONCTION. Pour les périphériques verrouillés à l'aide d'un code de passe inconnu, utilisez l'option SUPPRIMER LE CODE DE PASSE.

4.2.3. Applications, protection et gestion des contacts

Contrairement aux périphériques Android, iOS dispose d'un concept de gestion de la sécurité unifié, qui permet aux administrateurs de consolider les paramètres de sécurité couvrant une large plage de modules dans un même profil. Ces profils peuvent ensuite être appliqués à plusieurs périphériques, ce qui réduit le temps nécessaire pour sécuriser tous les périphériques iOS du réseau. L'onglet PROFILS de l'application G Data Administrator peut être utilisé pour créer et modifier des profils.

Chaque profil peut inclure un maximum de cinq politiques, chacune étant axée sur un type spécifique de paramètres de sécurité :

- RESTRICTION DES FONCTIONNALITÉS : permet de limiter l'utilisation de l'iCloud, de veiller à une utilisation sûre de l'écran de verrouillage et de contrôler plusieurs autres fonctions.
- PARAMÈTRES DU CODE DE PASSE : permet d'appliquer des normes pour l'utilisation du code de passe, telles que le nombre minimal de caractères complexes, la longueur minimale et la période de grâce après le verrouillage du périphérique.
- RESTRICTION DES APPLICATIONS : permet de bloquer ou d'autoriser Safari (dont des fonctions telles que les témoins, les fenêtres contextuelles et JavaScript) et iTunes Store.
- RESTRICTION DU CONTENU MULTIMÉDIA : permet de contrôler les types de contenu multimédia autorisés (applications, films, émissions de télé).
- WI-FI : saisissez les informations relatives au réseau Wi-Fi, de manière à permettre aux périphériques iOS de se connecter automatiquement à un réseau Wi-Fi spécifique.

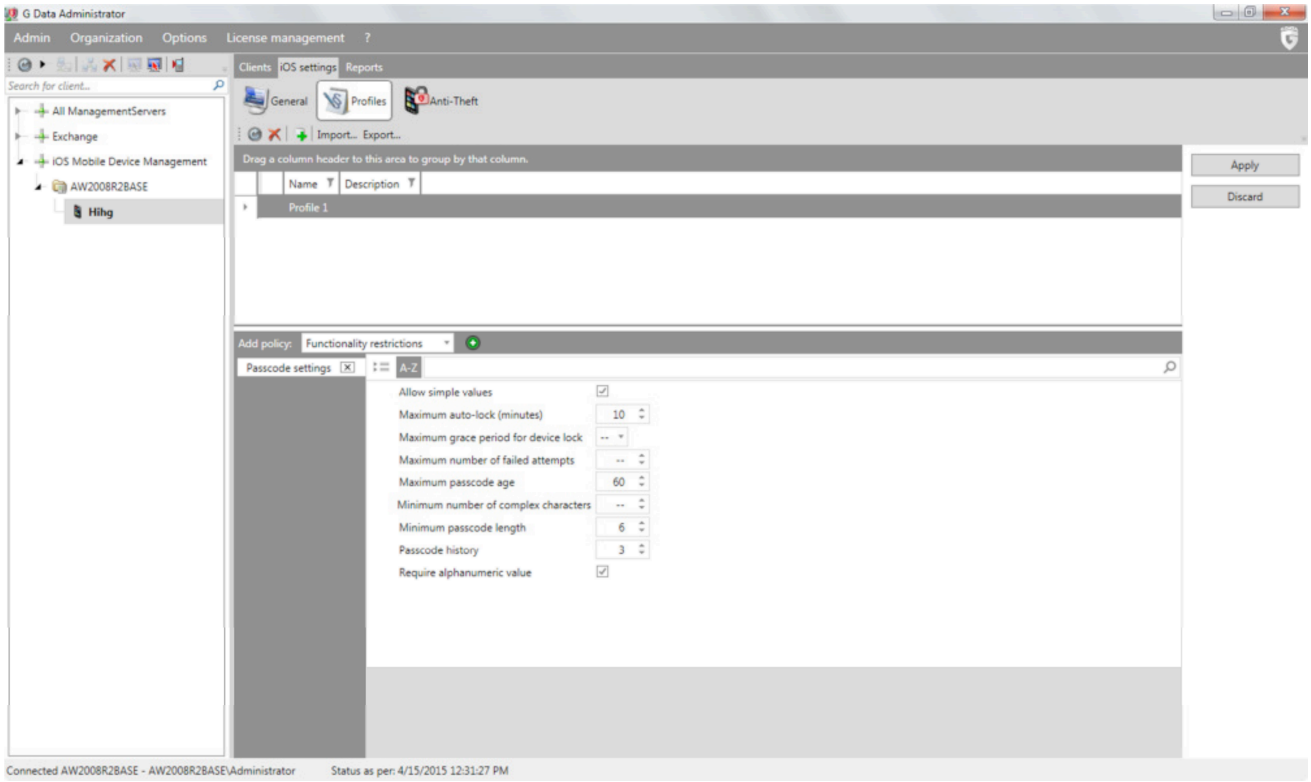


Image 7 : G Data Administrator, paramètres iOS, profils

Apple autorise les utilisateurs à supprimer à tout moment des profils MDM de leur périphérique, les administrateurs doivent donc veiller à ce que leurs profils de sécurité présentent une raison pour les utilisateurs de ne pas les supprimer. Nous vous recommandons d'ajouter la politique Wi-Fi à chaque

profil. Le périphérique peut ainsi se connecter au réseau Wi-Fi (protégé) indiqué. Si un utilisateur final tente de contourner une partie de la politique de sécurité en supprimant le profil MDM d'un périphérique iOS, l'accès Wi-Fi est automatiquement supprimé, ce qui limite de manière importante l'accès du périphérique aux ressources de l'entreprise. Les périphériques qui présentent des risques n'ont ainsi pas accès aux partages réseau sensibles ou autres données confidentielles.