TREND MICRO™

9.0 TREND MICRO™ Mobile Security™

Manuel de l'administrateur

Sécurité complète pour portables d'entreprise

Endpoint Security

Référence document TSFM96394/140410

Date de publication : Mars 2014

La documentation utilisateur de Trend Micro™ Mobile Security 9.0 SP1 for Enterprise présente les fonctions principales du produit et fournit les instructions d'installation pour votre environnement de production. Lisez entièrement la documentation avant d'installer ou d'utiliser le produit.

Vous trouverez des informations détaillées sur l'utilisation des fonctions spécifiques du produit dans le fichier d'Aide en ligne et dans la Base de connaissances en ligne sur le site Web de Trend Micro.

Trend Micro cherche toujours à améliorer sa documentation. Si vous avez des questions, des commentaires ou des suggestions à propos de ce document ou de tout autre document de Trend Micro, veuillez nous contacter à l'adresse docs@trendmicro.com.

Vous pouvez évaluer cette documentation sur le site Web suivant :

http://www.trendmicro.com/download/documentation/rating.asp

Table des matières

Préface

Chapitre 1: Introduction

Chapitre 2: Mise en route avec Mobile Security

Chapitre 3: Gestion des dispositifs mobiles

Chapitre 4: Protection des dispositifs à l'aide de stratégies

Chapitre 5: Gestion de la Banque d'applications d'entreprise

Chapitre 6: Mise à jour des composants

Chapitre 7: Affichage et maintenance des journaux

Chapitre 8: Utilisation des notifications et rapports

Chapitre 9: Dépannage et contact de l'assistance technique

Index

Préface

Bienvenue dans le Manuel de l'administrateur de Trend Micro™ Mobile Security for Enterprise version 9.0 SP1. Ce guide fournit des informations détaillées sur les options de configuration de Mobile Security. Parmi les sujets abordés : mise à jour de votre logiciel pour assurer la protection contre les risques de sécurité les plus récents, configuration et utilisation des stratégies pour la prise en charge de vos objectifs de sécurité, configuration des scans, synchronisation des stratégies sur les dispositifs mobiles et utilisation des journaux et des rapports.

Cette préface aborde les sujets suivants :

Public ciblé

La documentation de Mobile Security s'adresse à la fois aux utilisateurs de dispositif mobile et aux administrateurs qui sont responsables de la gestion des agents de dispositif mobile dans les environnements d'entreprise.

Les administrateurs doivent avoir une connaissance de moyenne à avancée de l'administration système Windows et des stratégies des dispositifs mobiles, comme :

- L'installation et la configuration des serveurs Windows
- L'installation de logiciels sur les serveurs Windows
- La configuration et la gestion des dispositifs mobiles (tels que les smartphones et Pocket PC/Pocket PC Phone)
- Les concepts du réseau (comme l'adresse IP, le masque réseau, la topologie, les paramètres LAN)
- Les diverses topologies de réseau
- Les dispositifs réseau et leur administration
- Les configurations réseau (telles que l'utilisation de VLAN, HTTP et HTTPS)

Documentation de Mobile Security

La documentation de Mobile Security contient les éléments suivants :

- *Manuel d'installation et de déploiement*—ce manuel vous aide à faire fonctionner Mobile Security et vous assiste dans la planification et l'installation réseau.
- *Manuel de l'administrateur*—ce manuel décrit en détail les stratégies et les technologies de configuration de Mobile Security.
- *Aide en ligne*—l'objectif de l'aide en ligne est de fournir des descriptions des principales tâches du produit, des conseils d'utilisation et des informations spécifiques aux champs, telles que les plages de paramètres valides et les valeurs optimales.

- *Fichier Lisez-moi*—il contient des informations de dernière minute sur le produit qui ne se trouvent pas dans la documentation en ligne ou imprimée. Les rubriques contiennent une description des nouvelles fonctionnalités, des conseils d'installation, les problèmes connus et l'historique des versions.
- *Base de connaissances*—la base de connaissances est une base de données en ligne contenant des informations sur la résolution des problèmes et le dépannage. Elle contient les dernières informations sur les problèmes connus identifiés pour les produits. Pour accéder à la base de connaissances, ouvrez :

  http://esupport.trendmicro.com/

Conseil

Trend Micro recommande de consulter le lien adéquat du centre de téléchargement (http://downloadcenter.trendmicro.com/?regs=FR) pour obtenir des mises à jour sur la documentation du produit.

Conventions typographiques du document

La documentation utilise les conventions suivantes.

TABLEAU 1. Conventions typographiques du document

CONVENTION	DESCRIPTION
MAJUSCULES	Acronymes, abréviations, noms de certaines commandes et touches du clavier
Gras	Menus et commandes de menu, boutons de commande, onglets et options
Italique	Références à des documents annexes
`Monospace`	Exemples de lignes de commande, de code de programme, adresses Internet, noms de fichier et sortie de programme

CONVENTION	DESCRIPTION
Navigation > **Chemin**	Le chemin de navigation pour atteindre un écran particulier Par exemple, **Fichier** > **Sauvegarder** signifie, cliquez sur **Fichier** puis cliquez sur **Sauvegarder** sur l'interface
Remarque	Remarques de configuration
Conseil	Recommandations ou suggestions
Important	Informations relatives aux paramètres de configuration requis ou par défaut et aux limites des produits
AVERTISSEMENT!	Actions stratégiques et options de configuration

Chapitre 1

Introduction

Trend Micro™ Mobile Security for Enterprise v9.0 SP1 est une solution de sécurité intégrée pour vos dispositifs mobiles. Ce chapitre décrit les composants et les fonctionnalités de Mobile Security et vous explique comment Mobile Security protège vos dispositifs mobiles.

Ce chapitre contient les sections suivantes :

Comprendre les menaces mobiles

Avec la standardisation des plates-formes et leur connectivité croissante, les dispositifs mobiles sont exposés à des menaces de plus en plus nombreuses. Le nombre de programmes malveillants s'exécutant sur les plates-formes mobiles est en augmentation constante, et de plus en plus de spams sont envoyés par SMS. De nouvelles sources de contenu, comme le WAP et le WAP-Push, sont également utilisées pour diffuser des contenus non sollicités.

En plus des menaces que génèrent les programmes malveillants, les spams et les autres contenus indésirables, les dispositifs mobiles doivent aujourd'hui faire face au piratage et aux attaques de déni de service (DoS). Les dispositifs mobiles, dont la plupart disposent désormais de la même connectivité réseau que celle traditionnellement associée aux dispositifs informatiques plus importants comme les ordinateurs portables et les ordinateurs de bureau, sont désormais les cibles d'attaques de ce type.

En outre, le vol de dispositifs mobiles peut conduire à la mise en danger de données personnelles ou sensibles.

À propos de Trend Micro Mobile Security v9.0 SP1

Trend Micro™ Mobile Security for Enterprise est une solution de sécurité complète pour vos dispositifs mobiles. Mobile Security intègre les technologies anti-programmes malveillants de Trend Micro pour lutter efficacement contre les menaces récentes ciblant les dispositifs mobiles.

Ses fonctions de pare-feu et de filtrage intégrées permettent à Mobile Security de bloquer toute communication réseau indésirable vers des dispositifs mobiles. Ces communications réseau indésirables comprennent : des messages SMS et WAP Push, ainsi que des données reçues via des connexions 3G/GPRS.

Cette version de Mobile Security est indépendante d'OfficeScan™ et peut être installée séparément, en tant qu'application autonome, sur un ordinateur Windows.

De plus, Mobile Security comprend un module de chiffrement universel qui offre des fonctionnalités de protection par mot de passe de connexion et de chiffrement des

données pour les dispositifs mobiles Symbian et Windows. Ce module de chiffrement empêche tout risque pour les données en cas de perte ou de vol d'un dispositif mobile.

AVERTISSEMENT!

Trend Micro ne peut pas garantir la compatibilité entre Mobile Security et le logiciel de chiffrement du système de fichiers. Des logiciels offrant des fonctionnalités similaires, telles que le scan anti-programmes malveillants, la gestion SMS et la protection par pare-feu, risquent d'être incompatibles avec Mobile Security.

Architecture du système Mobile Security

Selon les besoins de votre entreprise, vous pouvez mettre en œuvre Mobile Security avec différentes méthodes de communication client-serveur. Vous pouvez également choisir de configurer une ou plusieurs combinaisons de méthodes de communication client-serveur sur votre réseau.

Trend Micro Mobile Security prend en charge trois différents modèles de déploiement :

- Modèle de sécurité renforcée (Installation de deux serveurs) avec le serveur de communication du nuage
- Modèle de sécurité renforcée (installation de deux serveurs) avec le Serveur de communication local
- Modèle de sécurité de base Installation sur un serveur)

Consultez le *Manuel d'installation et de déploiement* pour la procédure détaillée.

Composants du système Mobile Security

Le tableau suivant fournit les descriptions des composants de Mobile Security.

TABLEAU 1-1. Composants du système Mobile Security

COMPOSANT	DESCRIPTION	REQUIS OU FACULTATIF
Serveur d'administration	Le serveur d'administration vous permet de gérer les agents de dispositif mobile à partir de la console Web d'administration. Une fois les dispositifs mobiles inscrits sur le serveur, vous pouvez configurer les stratégies des agents de dispositif mobile et effectuer des mises à jour.	Requis
Serveur de communication	Le serveur de communication gère les communications entre le serveur d'administration et les agents de dispositif mobile. Trend Micro Mobile Security fournit deux types de serveurs de communication : • Serveur de communication local (LCS)—il s'agit d'un serveur de communication déployé localement sur votre réseau. • Serveur de communication du nuage (CCS)—il s'agit d'un serveur de communication déployé sur le nuage et vous n'aurez pas besoin d'installer ce serveur. Trend Micro gère le serveur de communication du nuage et il vous suffit de vous-y connecter à partir du serveur d'administration. Voir la section *Comparaison entre le Serveur de communication local et le serveur du nuage à la page 1-6*.	Requis
Expéditeur de SMS	Vous pouvez utiliser l'expéditeur de SMS pour envoyer des messages SMS aux utilisateurs.	Facultatif
Connecteur Exchange	Trend Micro Mobile Security utilise le connecteur Exchange pour communiquer avec Microsoft Exchange Server, et détecte les dispositifs qui utilisent le service Exchange ActiveSync.	Facultatif

Composant	Description	Requis ou facultatif
Agent de dispositif mobile (MDA)	L'agent de dispositif mobile est installé sur les dispositifs mobiles administrés. L'agent communique avec le serveur de Mobile Security et exécute les paramètres de commandes et de stratégies sur le dispositif mobile.	Requis
Microsoft SQL Server	Le Microsoft SQL Server héberge les bases de données du serveur de Mobile Security.	Requis
Active Directory	Le serveur Mobile Security importe les utilisateurs et les groupes de l'Active Directory.	Facultatif
Autorité de certification	L'autorité de certification gère les informations d'identification et pour une communication sécurisée.	Facultatif
SCEP	L'extension du protocole d'inscription du certificat simple (SCEP) opère avec l'autorité de certification pour émettre des certificats dans les grandes entreprises. Il gère la délivrance et la révocation des certificats numériques. SCEP et l'autorité de certification de peuvent être installées sur le même serveur.	Facultatif
Certificat APNs (Apple Push Notification service)	Le serveur Mobile Security communique à travers le service Apple Push Notification (APNs) pour les dispositifs iOS	Requis pour gérer les dispositifs mobiles iOS
Certificat SSL	Trend Micro Mobile Security exige un certificat de serveur SSL (Secure Socket Layer) privé émis par une autorité de certification publique reconnue afin de garantir une communication sécurisée entre les dispositifs mobiles et le serveur de communication à l'aide de HTTPS.	Requis afin de gérer les dispositifs mobiles iOS 5 et versions supérieures de dispositifs mobiles

Composant	Description	Requis ou facultatif
Outil d'administration des utilisateurs BES	L'outil d'administration des utilisateurs BES est nécessaire pour assister la gestion des dispositifs BlackBerry enregistrés sur le serveur BES.	Requis afin de gérer les dispositifs mobiles BlackBerry
Serveur SMTP	Connectez le serveur SMTP pour vous assurer que les administrateurs peuvent obtenir des rapports du serveur Mobile Security, et envoyer des invitations aux utilisateurs.	Facultatif

Comparaison entre le Serveur de communication local et le serveur du nuage

Le tableau suivant compare le Serveur de communication local (LCS) et le serveur de communication du nuage (CCS).

Tableau 1-2. Comparaison entre le Serveur de communication local et le serveur du nuage

Fonctions	Serveur de communication du nuage	Serveur de communication local
Installation requise	Non	Oui
Méthode d'authentification utilisateur prise en charge	Clé d'inscription	Active Directory ou clé d'inscription
Personnalisation d'agent pour Android	Non pris en charge	Pris en charge
Gérer les dispositifs mobiles Symbian	Non pris en charge	Pris en charge
Gérer les dispositifs mobiles Windows	Non pris en charge	Pris en charge

Nouveautés de cette version (v9.0 SP1)

Le tableau suivant décrit les nouvelles fonctionnalités incluses dans Trend Micro™ Mobile Security for Enterprise v9.0 SP1.

Nom des fonctionnalités	Description
Serveur d'administration autonome	Cette version de Trend Micro Mobile Security est indépendante d'OfficeScan et peut être installée directement sur un ordinateur Windows.
Serveur de communication du nuage facultatif	Outre le serveur de communication installé localement (serveur de communication local), cette version offre également la possibilité d'utiliser le serveur de communication déployé dans le nuage (serveur de communication du nuage). Les administrateurs n'ont pas besoin d'installer le serveur de communication du nuage. Celui-ci est géré par Trend Micro.
Intégration de serveur Exchange	Fournit l'intégration de Microsoft Exchange Server et prend en charge des dispositifs mobiles iOS, Android et Windows Phone qui utilisent le service Exchange ActiveSync.
Stratégies basées sur des modèles	Vous permet de créer, copier ou supprimer des stratégies de sécurité et de les affecter à un groupe de dispositifs mobiles.
Prise en charge de comptes administrateurs multiples	Vous permet de créer plusieurs comptes administrateurs avec des rôles différents, qui peuvent être personnalisés en fonction des besoins et au moment opportun.
États des dispositifs mis à jour	Affiche l'état actuel des dispositifs mobiles de façon plus appropriée, avec la liste des états des dispositifs mise à jour.
Mise en service des dispositifs iOS	Vous permet de pousser le profil de configuration vers des dispositifs mobiles iOS pour configurer les paramètres VPN, Wi-Fi et Exchange ActiveSync.
Gestion des dispositifs mobiles iOS en mode surveillé	Cette version prend également en charge les dispositifs mobiles iOS en mode surveillé.

NOM DES FONCTIONNALITÉS	DESCRIPTION
Gestion de l'écran du Tableau de bord	Vous permet de gérer les informations affichées sur l'écran du **Tableau de bord** sous forme de widgets. Vous pouvez ajouter ou supprimer les widgets selon vos besoins.
Confirmation de commande du serveur	Fournit l'interface de **Gestion de la file de commandes** qui affiche l'état actuel de chaque commande exécutée à partir du serveur.
Contrôle des applications à l'aide de catégories	Vous permet d'autoriser ou de bloquer l'installation de certaines applications qui appartiennent à des catégories sur des dispositifs mobiles iOS et Android à l'aide de listes d'applications bloquées ou approuvées.
Inscription d'un dispositif mobile à l'aide d'un code QR	Introduit l'inscription d'un dispositif mobile à l'aide d'un code QR envoyé par e-mail à l'utilisateur.
Stratégie de verrouillage des fonctionnalités améliorée	Ajoute davantage de fonctionnalités et de composants de système d'exploitation à la liste de verrouillage des fonctionnalités dont l'administrateur contrôle la disponibilité sur les dispositifs mobiles.
Prise en charge du programme d'achats en grande quantité d'iOS	Vous permet d'importer dans la console Web d'administration de Mobile Security les applications iOS achetées par le biais du programme d'achats en grande quantité d'Apple.
Interface de l'agent de dispositif mobile mise à jour	Introduit la nouvelle interface utilisateur des agents de dispositifs mobiles Android et iOS.
Intégration de MARS	Fournit l'intégration de l'agent de serveur et de dispositif mobile Android avec Trend Micro Mobile Application Reputation Service (MARS) pour les risques de sécurité des applications et pour l'utilisation des ressources.
Téléchargement de rapports administrateur	Vous permet de télécharger les rapports administrateur depuis la console Web d'administration de Mobile Security.
Journaux de violation de la stratégie	Fournit des journaux de violation de la stratégie pour les dispositifs mobiles Android.

Nom des fonctionnalités	Description
Intégration de Trend Micro Control Manager	Trend Micro Mobile Security assure l'intégration avec Trend MicroControl Manager. Cette intégration permet aux administrateurs de Control Manager de remettre des stratégies d'entreprise à des dispositifs mobiles et de visualiser l'écran du **Tableau de bord** de Mobile Security dans Control Manager.

Nouveautés de la version 8.0 SP1

Le tableau suivant décrit les fonctions supplémentaires qui ont été introduites dans Trend Micro™ Mobile Security for Enterprise v8.0 Service Pack 1 (SP1).

Nom des fonctions	Description
Authentification basée sur l'identité du dispositif	Permet d'authentifier un lot de dispositifs mobiles en utilisant leurs numéros IMEI et/ou leurs adresses MAC Wi-Fi.
Groupe non administré pour Android et iOS	Introduit un groupe "non administré" pour les dispositifs mobiles Android sur lesquels 'l'administrateur du dispositif' est désactivé, et pour les dispositifs mobiles iOS sur lesquels les profils d'inscription sont supprimés.
Journaux d'événements améliorés	Fournit des journaux d'événements améliorés pour enregistrer les événements liés à la réinitialisation du mot de passe, à la localisation à distance, au verrouillage à distance et à la suppression à distance du dispositif mobile.
URL d'inscription personnalisable	Fournit une URL plus courte et personnalisable pour l'inscription des dispositifs mobiles.
client iOS simple	Introduit un client iOS pour une authentification client et une inscription simples en utilisant l'e-mail de l'utilisateur. Le client iOS permet également d'accéder à la Banque d'applications d'entreprise sur le dispositif mobile.

Nouveautés de la version 8.0

Le tableau suivant décrit les fonctions supplémentaires qui ont été introduites dans Trend Micro™ Mobile Security for Enterprise v8.0.

Nom des fonctions	Description
Personnalisation d'agent	Vous permet de prédéfinir l'adresse IP du serveur et le numéro de port dans le package d'installation Android.
prise en charge du proxy Web pour Android	Vous permet de configurer un proxy Web pour les dispositifs mobiles Android.
Paramètres des notifications push HTTP(S) pour Android	Fournit les paramètres permettant d'activer ou de désactiver les notifications push HTTP(S) pour dispositifs mobiles Android.
Mise en service simplifiée	Vous permet de configurer à l'avance l'adresse IP du serveur, le nom de domaine et le numéro de port du serveur pour les dispositifs mobiles Android, facilitant le déploiement et l'inscription des dispositifs mobiles.
Analyse après mise à jour des signatures	Lance automatiquement une recherche de menaces de sécurité sur le dispositif mobile après avoir effectué la mise à jour des signatures, et affiche la progression dans la barre de notification.
Stratégie de protection contre les menaces Internet	Vous permet de gérer la stratégie de protection contre les menaces Internet depuis le serveur Mobile Security et la déploie sur les dispositifs mobiles Android. Cela permet également aux dispositifs mobiles de renvoyer au serveur le journal de protection contre les menaces Internet.
Ajout de restriction de carte SD pour Android	Vous permet de contrôler la disponibilité de la carte SD pour les dispositifs mobiles Android.
Inventaire d'applications	Maintient la liste des applications installées sur les dispositifs mobiles et l'affiche sur l'écran d'état du dispositif.
Contrôle d'applications	Vous permet d'autoriser ou de bloquer l'installation de certaines applications sur les dispositifs mobiles disposant de listes bloquées ou approuvées.

Nom des fonctions	Description
Application push	Vous permet de pousser le package d'installation de l'application ou le lien Web de l'application vers les dispositifs mobiles en vue d'une installation.
Suppression sélective	Vous permet de supprimer toutes les données d'entreprise du serveur, sans effacer les données personnelles de l'utilisateur.
Vérification de la compatibilité	Vous permet de définir les critères de compatibilité sur le serveur et vérifie la compatibilité des dispositifs mobiles.
Authentification facultative à l'aide d'Active Directory	Vous permet de configurer l'authentification de l'utilisateur à l'aide d'Active Directory (AD) ou de la base de données Mobile Security pour les dispositifs mobiles Symbian, Windows Mobile, iOS lors de leur enregistrement.
Écran Tableau de bord	Introduit l'écran du **Tableau de bord** pour remplacer l'ancien écran **résumé** de la console Web afin de fournir le récapitulatif de l'état des composants du serveur et des dispositifs mobiles.
Rapports programmés	Vous permet de paramétrer Mobile Security pour qu'il envoie les rapports programmés à des intervalles prédéfinis.
Écran de vérification de configuration rapide	Introduit l'écran de **Configuration et vérification de la configuration de Mobile Security** qui vous permet de vérifier rapidement la configuration de Mobile Security et qui identifie les problèmes, le cas échéant. Si l'écran de vérification de la configuration détecte des paramètres de configuration incorrects, il fournit des suggestions pour y remédier.
Réinitialisation du mot de passe à distance et à la demande pour iOS et Android	Vous permet de réinitialiser le mot de passe à distance pour les dispositifs mobiles iOS et Android, à partir de la console Web.
Banque d'applications d'entreprise	Vous permet de créer une liste de webclips et d'applications que les utilisateurs peuvent télécharger et installer sur leurs dispositifs mobiles.

Nouveautés de la version v7.1

Le tableau suivant décrit les fonctions supplémentaires qui ont été introduites dans Trend Micro™ Mobile Security for Enterprise v7.1.

Nom des fonctions	Description
Prise en charge des dispositifs mobiles iOS et Blackberry	Ajout de la prise en charge par Mobile Security v7.1 des dispositifs mobiles iOS et Blackberry.
Intégré à Active Directory	Mobile Security v7.1 tire profit de l'Active Directory (AD) d'entreprise pour importer des utilisateurs et les authentifier.
Architecture mise à jour	Dans Mobile Security v7.1, des modèles de déploiement sur un ou deux serveurs sont introduits. La passerelle SMS est également supprimée dans la version v7.1.
Stratégie de mise en service	Cette version introduit la stratégie de mise en service des dispositifs mobiles.

Nouveautés de la version v7.0

Cette section décrit les fonctions supplémentaires qui ont été introduites dans Trend Micro™ Mobile Security for Enterprise v7.0.

Nom des fonctions	Description
Prise en charge des dispositifs mobiles Android	Ajout de la prise en charge par Mobile Security v7.0 des dispositifs mobiles Android v2.1 ou supérieure.
Stratégies de filtrage des appels	Permet à l'administrateur de contrôler les appels entrants ou sortants sur les dispositifs mobiles Android.
Fonction verrouillage mise à jour	Permet à l'administrateur de contrôler la disponibilité de certains composants pour les dispositifs mobiles Android qui se trouvent dans la plage de certains points d'accès.

Nom des fonctions	Description
Localiser un dispositif à distance	Permet à l'administrateur de localiser le dispositif à distance par le biais du réseau sans fil ou à l'aide du GPS du dispositif mobile et d'afficher sa position sur Google Maps. Cette nouvelle fonctionnalité permet de localiser les dispositifs mobiles perdus, volés ou égarés.
Architecture mise à jour	Dans Mobile Security v7.0, la passerelle SMS est ajoutée comme alternative à l'expéditeur de SMS pour l'envoi de SMS vers des dispositifs mobiles.

Principales fonctions de l'agent de dispositif mobile

Nom des fonctions	Description
Scan anti-programmes malveillants	Mobile Security intègre la technologie Trend Micro anti-programmes malveillants afin de détecter efficacement les menaces et d'éviter que des personnes malveillantes ne tirent profit des vulnérabilités des dispositifs mobiles. Mobile Security est spécialement conçu pour rechercher d'éventuelles menaces mobiles et vous permet de mettre en quarantaine et de supprimer les fichiers infectés.
Sécurité Web	Alors que les technologies des dispositifs mobiles évoluent, les menaces mobiles sont également de plus en plus sophistiquées. Trend Micro Mobile Security fournit la réputation de sites Web et le contrôle parental afin de protéger votre dispositif mobile contre les sites Web dangereux et contre les sites Web susceptibles de présenter un contenu inapproprié pour les enfants, les adolescents ou d'autres membres de la famille. Vous pouvez modifier le niveau des paramètres de Réputation de sites Web et de Contrôle parental en fonction de vos exigences. Mobile Security conserve également le journal des sites Web qui ont été bloqués par la Réputation de sites Web ou le Contrôle parental dans leurs journaux spécifiques.

Nom des fonctions	Description
Anti-spam SMS	Les dispositifs mobiles reçoivent souvent des messages indésirables ou du spam par le biais de messages SMS. Afin de filtrer les messages SMS non sollicités dans un dossier Spam, vous pouvez spécifier les numéros de téléphone à partir desquels tous les messages SMS envoyés seront considérés comme messages de spam. Vous pouvez également spécifier une liste de numéros de téléphone approuvés et configurer Mobile Security de manière à ce qu'il filtre tous les messages provenant d'expéditeurs non répertoriés dans la liste de numéros approuvés. Vous pouvez également filtrer les messages SMS non identifiés ou les messages sans numéro d'expéditeur. Votre dispositif mobile stockera automatiquement ces messages dans un dossier Spam de la boîte de réception. **Remarque** La fonction Anti-spam SMS n'est pas disponible sur les dispositifs mobiles non équipés de fonctionnalités téléphoniques.
Filtrage des appels	Mobile Security vous permet de filtrer les appels entrants ou sortants depuis le serveur. Vous pouvez configurer Mobile Security de sorte qu'il bloque les appels entrants de certains numéros de téléphone ou vous pouvez spécifier une liste de numéros de téléphone approuvés vers lesquels le dispositif mobile peut émettre des appels. Mobile Security permet également aux utilisateurs de dispositif mobile de spécifier leur propre liste bloquée ou approuvée afin de filtrer les appels entrants non sollicités. **Remarque** La fonction de filtrage des appels n'est pas disponible sur les dispositifs mobiles non équipés de fonctionnalités téléphoniques.

NOM DES FONCTIONS	DESCRIPTION
Protection WAP-Push	WAP-Push est une méthode puissante de remise automatique de contenu aux dispositifs mobiles. Pour initialiser la remise du contenu, des messages spéciaux appelés «messages WAP-Push» sont envoyés aux utilisateurs. Ces messages contiennent généralement des informations sur le contenu et permettent aux utilisateurs de l'accepter ou de le refuser. Il s'avère que des utilisateurs malveillants envoient des messages WAP-Push erronés ou contenant de fausses informations afin de tromper les utilisateurs pour qu'ils acceptent un contenu susceptible de comporter des applications et des paramètres système non sollicités, voire même des programmes malveillants. Mobile Security vous permet d'utiliser une liste d'expéditeurs de confiance pour filtrer les messages WAP-Push et empêcher les contenus indésirables d'atteindre les dispositifs mobiles. La fonction de protection WAP-Push n'est pas disponible sur les dispositifs mobiles non équipés de fonctionnalités téléphoniques.
Authentification	Après avoir installé l'agent de dispositif mobile, un dispositif mobile est associé à un utilisateur. L'utilisateur doit entrer un mot de passe (également appelé mot de passe de mise sous tension) pour se connecter au dispositif mobile.
Chiffrement des données	Mobile Security fournit une fonction de chiffrement dynamique des données pour les données stockées sur les dispositifs mobiles ou sur les cartes mémoire. Vous pouvez préciser le type de données à chiffrer et l'algorithme de chiffrement à utiliser.
Mises à jour régulières	Pour vous protéger des menaces les plus récentes, vous pouvez mettre à jour Mobile Security manuellement ou le configurer pour qu'il se mette à jour automatiquement. Pour réduire les coûts, vous pouvez également définir une fréquence de mise à jour différente pour les appareils mobiles qui sont en « itinérance ». Les mises à jour incluent des mises à jour de composants et des correctifs pour le programme Mobile Security.

NOM DES FONCTIONS	DESCRIPTION
Pare-feu (seulement pour BlackBerry, Symbian et Windows Mobile)	Mobile Security inclut le module de pare-feu de Trend Micro, fourni avec des niveaux de sécurité prédéfinis pour filtrer le trafic réseau. Vous pouvez également définir vos propres règles de filtrage et filtrer le trafic réseau à partir d'adresses IP spécifiques et sur des ports précis. Le système de détection d'intrusions (IDS) vous permet de bloquer les tentatives d'envoi continues de plusieurs paquets sur vos dispositifs mobiles. Ces tentatives représentent généralement une attaque de déni de service (DoS) et peuvent saturer votre dispositif mobile de sorte qu'il n'accepte pas d'autres connexions.

NOM DES FONCTIONS	DESCRIPTION

Journaux	Les journaux de l'agent de dispositif mobile suivants sont disponibles sur le serveur d'administration :
	• journal de protection contre les programmes malveillants
	• journal de protection contre les menaces Internet
	• journal de chiffrement
	• journal de pare-feu
	• journal d'événements
	• journal des violations
	Vous pouvez afficher les journaux suivants sur les dispositifs mobiles :
	• Windows Mobile et Symbian :
	  • journaux de virus/programmes malveillants
	  • journaux de pare-feu
	  • journaux d'anti-spam SMS
	  • journaux de protection WAP Push
	  • journaux de tâches
	• Android :
	  • historique de la recherche de programmes malveillants
	  • historique de l'analyse de la confidentialité
	  • historique du blocage web
	  • historique des appels bloqués
	  • historique des SMS bloqués
	  • historique des mises à jour

Fonctionnalités des systèmes d'exploitation des dispositifs mobiles pris en charge

Le tableau suivant donne la liste des fonctionnalités prises en charge par Trend Micro Mobile Security, par plate-forme.

TABLEAU 1-3. Matrice des fonctionnalités de Trend Micro Mobile Security 9.0 SP1

STRATÉGIE	FONCTIONNALITÉS	PARAMÈTRES					
Mise en service	Wi-Fi	Configuration Wi-Fi standard	●	●	●		
		Configuration hotspot héritée	●				
		Configuration Hotspot 2.0	●				
	Exchange ActiveSync	Configuration d'Exchange ActiveSync	●				
	VPN	Configuration VPN	●		●		
	Proxy HTTP global	Configuration du proxy HTTP global	●				
	Authentification unique	Configuration de l'authentification unique	●				
	Certificat	Configuration du certificat	●				
Sécurité de dispositif	Protection contre les programmes malveillants	Scan en temps réel		●		●	●
		Scan de la carte				●	●
		Scan après mise à jour du fichier de signatures		●			

Stratégie	Fonctionnalités	Paramètres					
Protection des données	Prévention anti-spam par SMS	Contrôle côté serveur		●	●	●	●
		Utiliser la liste des éléments bloqués		●	●	●	●
		Utiliser la liste des éléments approuvés		●	●	●	●
	Prévention anti-spam WAP Push	Contrôle côté serveur		●		●	●
		Utiliser la liste des éléments approuvés		●		●	●
	Filtrage des appels	Contrôle côté serveur		●	●		
		Utiliser la liste des éléments bloqués		●	●		
		Utiliser la liste des éléments approuvés		●	●		
	Pare-feu	Activer le pare-feu			●	●	●
		Activer le système de détection d'intrusions (IDS)				●	●
	Protection contre les menaces Internet	Contrôle côté serveur		●			
		Utiliser la liste des éléments bloqués		●			
		Utiliser la liste des éléments approuvés		●			
		Autoriser des sites Web spécifiques uniquement	●				
		Autoriser le contenu réservé aux adultes	●				

STRATÉGIE	FONCTIONNALITÉS	PARAMÈTRES					
Protection des données	Paramètres de mot de passe	Connexion à l'aide d'un mot de passe	●	●	●	●	
		Mot de passe administrateur				●	
		Autoriser un mot de passe simple	●	●	●	●	
		Exiger un mot de passe alphanumérique	●	●	●	●	
		Longueur minimale du mot de passe	●	●	●	●	
		Expiration du mot de passe	●	●		●	
		Historique des mots de passe	●	●		●	
		Verrouillage automatique	●	●		●	
		Action lors de l'échec du mot de passe	●	●	●	●	
	Chiffrement	Chiffrer PIM				●	
		Chiffrer les documents				●	
		Chiffrer les cartes mémoire				●	
	Verrouillage des fonctionnalités	Appareil photo	●	●		●	
		Temps en vis-à-vis	●				
		Capture d'écran	●				
		Installation d'applications	●				

Stratégie	Fonctionnalités	Paramètres					
Protection des données	Verrouillage des fonctionnalités	Synchronisation en itinérance	●				
		Composition vocale	●		●		
		Achat intégré	●				
		Jeu multi-joueurs	●				
		Ajouter des amis au Game center	●				
		Game Center (uniquement pour le mode surveillé)	●				
		Forcer les sauvegardes chiffrées	●				
		Musique et podcast explicites & iTunes U	●				
		Passbook lorsque le dispositif est verrouillé	●				
		Bluetooth et découverte Bluetooth		●		●	
		Infrarouge				●	
		Stockage USB				●	
		WLAN/Wi-Fi		●		●	
		Réseau de données 3G		●			

STRATÉGIE	FONCTIONNALITÉS	PARAMÈTRES					
Protection des données	Verrouillage des fonctionnalités	Mode modem		●			
		Mode développeur		●			
		Série				●	
		Haut-parleur/téléphone à haut-parleur/microphone			●	●	
		Microsoft ActiveSync				●	
		MMS/SMS				●	
		Restriction des cartes mémoire		●		●	
		Restriction du GPS				●	
		Siri	●				
		Siri lorsque le dispositif est verrouillé	●				
		Activer le filtre d'obscénités	●				
		Activer l'accès aux services iCloud	●				
		Sauvegarde Cloud	●				
		Synchronisation de documents Cloud	●				
		Galerie de photos	●				

Stratégie	Fonctionnalités	Paramètres					
Protection des données	Verrouillage des fonctionnalités	Galeries de photos partagées	●				
		Données de diagnostic	●				
		Accepter les TLS (Transport Layer Security) non approuvés	●				
		Forcer iTunes à stocker le mot de passe	●				
		YouTube	●				
		Ouvrir des documents d'applications gérées dans d'autres applications	●				
		Ouvrir des documents d'autres applications dans des applications gérées	●				
		iTunes	●				
		Navigateur Web Safari	●				
		Remplissage automatique	●				
		JavaScript	●				
		Fenêtres contextuelles	●				
		Forcer l'avertissement de fraude	●				
		Accepter les cookies	●				
		Suppression d'applications (uniquement pour le mode surveillé)	●				
		Librairie (uniquement pour le mode surveillé)	●				

STRATÉGIE	FONCTIONNALITÉS	PARAMÈTRES					
Protection des données	Verrouillage des fonctionnalités	Érotique (uniquement pour le mode surveillé)	●				
		Installation de profil de configuration (uniquement pour le mode surveillé)	●				
		iMessage (uniquement pour le mode surveillé)	●				
		Évaluations de la région	●				
		Films	●				
		Émissions télévisées	●				
		Applications	●				
Contrôle à distance		Inscription	●	●	●	●	●
		Mise à jour	●	●	●	●	●
	Protection antivol	Localisation à distance		●	●		
		Verrouillage à distance	●	●	●	●	
		Effacement à distance	●	●	●	●	
		Réinitialiser le mot de passe	●	●	●	●	

Chapitre 2

Mise en route avec Mobile Security

Ce chapitre vous aide à vous familiariser avec Mobile Security et vous y trouverez des instructions de base relatives à son utilisation. Avant d'aller plus loin, assurez-vous de bien installer le serveur d'administration, le serveur de communication, et l'agent de dispositif mobile sur les dispositifs mobiles.

Ce chapitre contient les sections suivantes :

Console Web d'administration

Vous pouvez accéder aux écrans de configuration via la console Web d'administration de Mobile Security.

La console Web d'administration constitue le point central à partir duquel Mobile Security est géré et surveillé à travers tout le réseau de l'entreprise. La console est fournie avec un ensemble de paramètres et de valeurs par défaut que vous pouvez adapter en fonction de vos spécifications et exigences en matière de sécurité.

Vous pouvez utiliser la console Web pour effectuer les opérations suivantes de la :

- Gestion des agents de dispositifs mobiles installés sur les dispositifs mobiles
- Configuration de stratégies de sécurité pour les agents de dispositif mobile
- Configuration des paramètres d'analyse sur un ou plusieurs dispositifs mobiles
- Regroupement des dispositifs en groupes logiques pour une configuration et une gestion facilitées
- Affichage des informations de mise à jour et d'enregistrement

Accès à la console Web d'administration

Procédure

1. Connectez-vous à la console Web d'administration en utilisant la structure d'URL suivante :

   ```
   https://
   <External_domain_name_or_IP_address>:<HTTPS_port>/mdm/web
   ```

   Remarque

   Remplacer <External_domain_name_or_IP_address> avec l'adresse IP réelle, et <HTTPS_port> avec le numéro de port réel du serveur d'administration.

L'écran suivant s'affiche.

FIGURE 2-1. Écran de connexion de la console Web d'administration

2. Saisissez un nom d'utilisateur et un mot de passe dans les champs prévus et cliquez sur **Connexion**.

Remarque

Le **Nom d'utilisateur** par défaut pour la console d'administration Web est « racine » et le **Mot de passe** est « mobilesecurity ».

Assurez-vous que vous modifiez le mot de passe administrateur pour l'utilisateur "racine" après votre première connexion. Voir *Modification de compte d'administrateur à la page 2-16* pour la procédure.

Important

Si vous utilisez Internet Explorer pour accéder à la console Web d'administration, vérifiez les points suivants :

- l'option **Affichage de compatibilité des sites Web** est désactivée. Voir *Désactivation du mode de compatibilité sur Internet Explorer à la page 2-4* pour plus de détails.
- JavaScript est activé sur votre navigateur.

Remarque

Si vous ne parvenez pas à accéder à la console Web d'administration de Windows 2012 en utilisant Internet Explorer 10 en mode Metro, vérifiez que l'option **Mode protégé renforcé** est désactivée dans Internet Explorer.

Désactivation du mode de compatibilité sur Internet Explorer

Trend Micro Mobile Security ne prend pas en charge l'**Affichage de compatibilité** sur Internet Explorer. Si vous utilisez Internet Explorer pour accéder à la console d'administration de Mobile Security, désactivez l'affichage de compatibilité du navigateur Web pour le site Web, s'il est activé.

Procédure

1. Ouvrez Internet Explorer et cliquez sur **Outils** > **Paramètres d'affichage de compatibilité**.

   La fenêtre des **Paramètres d'affichage de compatibilité** s'affiche.

2. Si la console d'administration est ajoutée à la liste **Affichage de compatibilité**, sélectionnez le site Web et cliquez sur **Supprimer**.

3. Effacer les cases à cocher **Afficher les sites intranet dans l'affichage de compatibilité** et **Afficher tous les sites Web dans l'affichage de compatibilité** , puis cliquez sur **Fermer** .

Licence du produit

À l'expiration de la licence d'évaluation, toutes les fonctions du programme sont désactivées. Une version de licence complète vous permet de continuer à utiliser toutes les fonctions, même après expiration de la licence. Il convient cependant de noter que l'agent de dispositif mobile ne sera pas en mesure d'obtenir des mises à jour depuis le serveur, ce qui rend les composants anti-programmes malveillants vulnérables aux risques de sécurité les plus récents.

Si votre licence expire, vous devrez enregistrer le serveur Mobile Security avec un nouveau code d'activation. Consultez votre service commercial Trend Micro pour plus d'informations.

Pour télécharger les mises à jour et autoriser la gestion à distance, l'agent de dispositif mobile doit s'inscrire sur le serveur Mobile Security. Pour obtenir des instructions sur l'inscription manuelle de l'agent de dispositif mobile sur des dispositifs mobiles, consultez le *Guide d'installation et de déploiement*.

Pour afficher les instructions de mise à niveau de la licence pour le serveur d'administration, cliquez sur le lien Afficher les instructions de mise à niveau de la licence sur l'écran **Licence du produit** Mobile Security.

Informations relatives au Tableau de bord

L'écran du **Tableau de bord** apparaît d'abord lorsque vous accédez au serveur d'administration. Cet écran présente l'état d'enregistrement du dispositif mobile et les détails des composants.

L'écran du Tableau de bord se compose de cinq onglets :

- **Résumé**—indique l'état de santé du dispositif et le résumé du système d'exploitation du dispositif.
- **Santé**—indique les mises à jour de composants et de stratégies et l'état de santé du dispositif mobile. Dans cette catégorie, vous pouvez :
    - Voir l'état des dispositifs mobiles :
        - **Sain**—indique que le dispositif est inscrit sur le serveur Mobile Security et que les composants et stratégies sur le dispositif mobile sont à jour.
        - **Non compatible**—indique que le dispositif est inscrit sur le serveur Mobile Security, mais qu'il n'est pas compatible avec les stratégies du serveur.
        - **Désynchronisé**—indique que le dispositif est inscrit sur le serveur Mobile Security, mais que les composants ou les stratégies sont obsolètes.

- **Inactif**—indique que le dispositif n'est pas encore inscrit sur le serveur Mobile Security.

- Afficher le nombre total de dispositifs mobiles inscrits et non inscrits gérés par Mobile Security.

  Un dispositif mobile peut rester non inscrit si l'une des situations suivantes se produit :

  - une connexion au serveur de communication échoue
  - l'utilisateur du dispositif mobile a supprimé le SMS d'inscription

- Consulter le programme correctif du dispositif mobile et l'état de la mise à jour d'un composant :

  - **Version actuelle**—le numéro de la version actuelle de l'agent de dispositif mobile ou des composants sur le serveur Mobile Security
  - **Mis à jour**—le nombre de dispositifs mobiles dont la version de l'agent de dispositif mobile ou le composant a été mis à jour
  - **Obsolète**—le nombre de dispositifs mobiles qui utilisent un composant obsolète
  - **Fréquence de mise à jour**—le pourcentage de dispositifs mobiles qui utilisent la version la plus récente des composants
  - **Mis à niveau**—le nombre de dispositifs mobiles qui utilisent la version la plus récente de l'agent de dispositif mobile
  - **Non mis à niveau**—le nombre de dispositifs mobiles qui n'ont pas été mis à niveau pour utiliser la dernière version de l'agent de dispositif mobile
  - **Fréquence de mise à niveau**—le pourcentage de dispositifs mobiles qui utilisent la version la plus récente de l'agent de dispositif mobile

- Afficher l'état de mise à jour du serveur :

  - **Serveur**—le nom du module
  - **Adresse**—le nom de domaine ou l'adresse IP de l'ordinateur hébergeant le module

        - **Version actuelle**—le numéro de la version actuelle des modules du serveur de Mobile Security
        - **Dernière mise à jour**—l'heure et la date de la dernière mise à jour

- **Inventaire**—affiche le résumé de la version du système d'exploitation du dispositif mobile, le résumé des entreprises de téléphonie, le résumé des revendeurs de dispositifs mobiles et les 10 principales applications installées sur les dispositifs mobiles.
- **Compatibilité**—affiche le contrôle d'application, l'état du débridage des dispositifs mobiles. Dans cette catégorie, vous pouvez :
    - Afficher l'état de débridage des dispositifs mobiles.
        - **Débridé**—le nombre de dispositifs mobiles débridés
        - **Non débridé**—le nombre de dispositifs mobiles non débridés
    - Afficher l'état de chiffrement du dispositif mobile :
        - **Chiffré**—le nombre de dispositifs mobiles chiffrés
        - **Non Chiffré**—le nombre de dispositifs mobiles non chiffrés
    - Afficher l'état du contrôle d'application du dispositif mobile :
        - **Compatible**—le nombre de dispositifs mobiles compatibles avec la stratégie de compatibilité et de contrôle des applications Mobile Security
        - **Non compatible**—le nombre de dispositifs mobiles qui ne sont pas compatibles avec la stratégie de compatibilité et de contrôle des applications Mobile Security
- **Protection**—affiche les cinq (5) principales menaces de sécurité et les cinq (5) principaux sites Web bloqués.

Remarque

Sur chacun des widgets de l'écran du **Tableau de bord,** vous pouvez sélectionner **Tous**, ou le nom du groupe dans la liste déroulante pour afficher les informations des dispositifs pertinents.

Personnalisation du Tableau de bord

Mobile Security vous permet de personnaliser les informations du **Tableau de bord** en fonction de vos besoins et exigences.

Ajout d'un nouvel onglet

Procédure

1. Dans l'écran **Tableau de bord**, cliquez sur le bouton +.
2. La fenêtre contextuelle **Nouvel onglet** s'affiche, procédez comme suit :
   - **Titre** : tapez le nom de l'onglet.
   - **Disposition** : sélectionnez la disposition des widgets affichés dans l'onglet.
   - **Ajustement automatique** : sélectionnez **Activé** ou **Désactivé** pour activer ou désactiver les paramètres des widgets sur l'onglet.
3. Cliquez sur **Enregistrer**.

Suppression d'un onglet

Procédure

1. Cliquez sur l'onglet, puis cliquez sur le bouton × affiché sur l'onglet.
2. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

Ajout de widgets

Procédure

1. Sur l'écran du **Tableau de bord**, cliquez sur l'onglet sur lequel vous souhaitez ajouter des widgets.

2. Cliquez sur **Ajouter Widgets** en haut à droite de l'onglet.

   L'écran **Ajouter Widgets** s'affiche.

3. Sélectionnez la catégorie à partir du menu de gauche et/ou tapez les mots clés dans le champ de recherche pour afficher la liste des widgets pertinents.

4. Sélectionnez les widgets que vous voulez ajouter et cliquez sur **Ajouter**.

   Les widgets sélectionnés apparaissent sur le **Tableau de bord**.

Supprimer des widgets

Procédure

1. Sur l'écran **Tableau de bord**, cliquez sur l'onglet contenant les widgets que vous souhaitez supprimer.

2. Sur le widget que vous souhaitez supprimer, cliquez sur × en haut à droite du widget.

Changement de position des widgets

Procédure

1. Sur l'écran **Tableau de bord**, cliquez sur l'onglet contenant les widgets que vous souhaitez réorganiser.

2. Cliquez sur la barre de titre du widget et, en la maintenant sélectionnée, faites-la glisser et déposez-la à son nouvel emplacement.

Actualisation des informations sur les Widgets

Procédure

1. Sur l'écran **Tableau de bord**, cliquez sur l'onglet contenant le widget que vous souhaitez actualiser.
2. Sur le widget que vous souhaitez actualiser, cliquez sur en haut à droite du widget.

Affichage ou modification des paramètres d'un onglet

Procédure

1. Sur l'écran **Tableau de bord**, cliquez sur l'onglet que vous souhaitez afficher ou modifier.
2. Cliquez sur **Paramètres de l'onglet**.
3. Modifiez les paramètres au besoin et puis cliquez sur **Enregistrer**.

Paramètres d'administration

Configuration des paramètres Active Directory (AD)

Trend Micro Mobile Security vous permet de configurer l'autorisation utilisateur basée sur Active Directory (AD). Vous pouvez également ajouter des dispositifs mobiles à la liste des dispositifs à l'aide de votre AD. Consultez la section *Configuration initiale du serveur* dans le *Manuel d'installation et de déploiement* pour obtenir les étapes de configuration complètes.

Configuration de l'authentification des dispositifs

Trend Micro Mobile Security vous permet de configurer l'authentification des dispositifs basée sur Active Directory (AD) ou sur la base de données de Mobile Security. Vous

pouvez également autoriser l'inscription de dispositifs mobiles sur le serveur Mobile Security sans authentification. Consultez la section *Configuration initiale du serveur* dans le *Manuel d'installation et de déploiement* pour obtenir les étapes de configuration complètes.

Configuration des paramètres de base de données

Consultez la section *Configuration initiale du serveur* dans le *Manuel d'installation et de déploiement* pour obtenir les étapes de configuration complètes.

Configuration des paramètres de serveur de communication

Consultez la section *Configuration initiale du serveur* dans le *Manuel d'installation et de déploiement* pour obtenir les étapes de configuration complètes.

Gestion des comptes d'administrateur

L'écran **Gestion des comptes d'administrateur** vous permet de créer des comptes d'utilisateur avec un rôle d'accès différent pour le serveur d'administration.

Nom et rôle du compte administrateur par défaut

Le compte administrateur par défaut est « racine » (Mot de passe : « mobilesecurity »). Le compte racine ne peut pas être supprimé, il peut uniquement être modifié. Voir *Modification de compte d'administrateur à la page 2-16* pour la procédure complète.

TABLEAU 2-1. Propriétés du compte racine

PROPRIÉTÉS DU COMPTE RACINE		PEUT ÊTRE MODIFIÉ ?
Comptes d'administrateur	Nom du compte	Non
	Nom et prénom	Oui
	Mot de passe	Oui
	Adresse de messagerie	Oui
	Numéro de téléphone portable	Oui
Rôles d'administrateur	Modification du rôle Administrateur	Non

Le rôle administrateur par défaut est **Super administrateur**, qui dispose de l'accès maximal à tous les paramètres. Le rôle du **Super administrateur** ne peut pas être supprimé, il peut uniquement être modifié. Voir *Modification d'un rôle d'administrateur à la page 2-18* pour la procédure complète.

TABLEAU 2-2. Propriétés du rôle Super administrateur

PROPRIÉTÉS DU RÔLE SUPER ADMINISTRATEUR		PEUT ÊTRE MODIFIÉ ?
Détails des rôles	Rôle d'administrateur	Non
	Description	Oui
Contrôle d'administration de groupe	Groupes administrés	Non
Contrôle du domaine du serveur Exchange	Sélection de domaine	Non

TABLEAU 2-3. Droits d'accès du Super administrateur et de l'Administrateur de groupe

COMPOSANTS DU SERVEUR	AUTORISATIONS	SUPER ADMINISTRATEUR	ADMINISTRATEUR DE GROUPE
Administration	Mises à jour	Pris en charge	Non pris en charge
	Gestion des comptes d'administrateur	Peut modifier tout le compte	Ne peuvent modifier que les informations propres au compte
	Paramètres d'inscription des dispositifs	Pris en charge	Non pris en charge
	Gestion des certificats	Pris en charge	Pris en charge
	Gestion de la file de commandes	Peut gérer toutes les commandes	Ne peut afficher que les commandes des groupes connexes
	Paramètres de base de données	Pris en charge	Non pris en charge
	Paramètres du serveur de communication	Pris en charge	Non pris en charge
	Paramètres Active Directory	Pris en charge	Non pris en charge
	Paramètres du serveur d'administration	Pris en charge	Non pris en charge
	Intégration d'Exchange Server	Pris en charge	Non pris en charge
	Configuration et vérification	Pris en charge	Non pris en charge
	Licence du produit	Pris en charge	Non pris en charge

Composants du serveur	Autorisations	Super Administrateur	Administrateur de groupe
Notifications/ rapports	Requête des journaux	Tous les groupes	Groupes administrés uniquement
	Maintenance des journaux	Tous les groupes	Groupes administrés uniquement
	Notifications/rapports administrateur	Pris en charge	Non pris en charge
	Notification utilisateur	Pris en charge	Non pris en charge
	Paramètres	Pris en charge	Non pris en charge
App Store	App Store	Pris en charge	Non pris en charge
Stratégie	Créer une stratégie	Pris en charge	Pris en charge pour les groupes administrés uniquement
	Afficher une stratégie	Pris en charge	Pris en charge pour les groupes administrés uniquement
	Copier une stratégie	Pris en charge	Pris en charge pour les groupes administrés uniquement
	Supprimer une stratégie	Pris en charge	Pris en charge pour les groupes administrés uniquement

COMPOSANTS DU SERVEUR	AUTORISATIONS	SUPER ADMINISTRATEUR	ADMINISTRATEUR DE GROUPE
Dispositifs	Afficher les dispositifs	Pris en charge	Pris en charge pour les groupes administrés uniquement
	Ajouter un groupe	Pris en charge	Pris en charge
	Inviter des dispositifs	Pris en charge	Pris en charge pour les groupes administrés uniquement
	Dispositifs Exchange ActiveSync	Pris en charge	Pris en charge pour les groupes administrés uniquement

Ajout de comptes d'administrateur

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Gestion des comptes d'administrateur**.
3. Dans l'onglet **Comptes d'administrateur**, cliquez sur **Créer** pour ajouter un nouveau compte.

   L'écran **Créer un compte d'administrateur** apparaît.
4. Sous la section **Détails du compte**, effectuez l'une des actions suivantes :
   - Sélectionnez **Utilisateur Trend Micro Mobile Security**, et précisez les détails du compte utilisateur suivants :
     - **Nom du compte** : nom utilisé pour se connecter au Serveur d'administration.
     - **Nom complet** : nom complet de l'utilisateur.

- **Mot de passe** (et **Confirmez le mot de passe**).
- **Adresse électronique** : adresse électronique de l'utilisateur.
- **Numéro de téléphone portable** : numéro de téléphone de l'utilisateur.

- Sélectionnez **Utilisateur d'Active Directory**, et procédez de la façon suivante :

  a. Saisissez le nom d'utilisateur dans le champ de recherche et cliquez sur **Rechercher**.

  b. Sélectionnez le nom d'utilisateur à partir de la liste de gauche et cliquez sur **>** pour déplacer l'utilisateur vers la liste **Utilisateurs sélectionnés** sur la droite.

Remarque

Pour supprimer l'utilisateur de la liste des **utilisateurs sélectionnés** sur la droite, sélectionnez le nom d'utilisateur, puis cliquez sur **<**.

Vous pouvez également sélectionner plusieurs utilisateurs en même temps en maintenant appuyées les touches Ctrl ou Shift pendant que vous cliquez sur le nom d'utilisateur.

---

5. Sous la section **Rôle de l'administrateur**, sélectionnez la liste déroulante : **Choisir le rôle d'administrateur**.

   Voir *Création d'un rôle d'administrateur à la page 2-18* pour la procédure de création des rôles d'administrateur

6. Cliquez sur **Enregistrer**.

Modification de compte d'administrateur

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Gestion des comptes d'administrateur**.

3. Dans l'onglet **Comptes d'administrateur**, cliquez sur **Créer** pour ajouter un nouveau compte.

   L'écran **Modifier un compte d'administrateur** apparaît.

4. Modifiez les détails du compte d'administrateur et le rôle d'accès au besoin.

   - Détails du compte
     - **Nom du compte** : nom utilisé pour se connecter au Serveur d'administration.
     - **Nom complet** : nom complet de l'utilisateur.
     - **Adresse électronique** : adresse électronique de l'utilisateur.
     - **Numéro de téléphone portable** : numéro de téléphone de l'utilisateur.
     - **Mot de passe** : cliquez sur **Réinitialiser le mot de passe** pour changer le mot de passe du compte utilisateur, tapez le nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**, puis cliquez sur **Sauvegarder**.
   - **Rôle d'administrateur**
     - **Choisir le rôle d'administrateur** : sélectionnez le rôle de l'administrateur dans la liste déroulante.

       Pour connaître la procédure pour créer un rôle d'administrateur, voir *Création d'un rôle d'administrateur à la page 2-18*.

5. Cliquez sur **Enregistrer**.

Suppression de comptes d'administrateur

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Gestion des comptes d'administrateur**.

3. Sur l'onglet **Comptes d'administrateur**, sélectionnez les comptes d'administrateur que vous souhaitez supprimer et cliquez sur **Supprimer**.

Création d'un rôle d'administrateur

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Gestion des comptes d'administrateur**.
3. Dans l'onglet**Rôles d'administrateur**, cliquez sur **Créer**.

   L'écran **Créer un rôle d'administrateur** apparaît.
4. Sous la section **Détails des rôles**, fournir les informations suivantes :
   - Rôle d'administrateur
   - Description
5. Sous la section **Contrôle d'administration de groupe** sélectionnez les groupes de dispositifs mobiles que ce rôle d'administrateur peut gérer.
6. Cliquez sur **Enregistrer**

Modification d'un rôle d'administrateur

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Gestion des comptes d'administrateur**.
3. Dans l'onglet **Rôles d'administrateur**, cliquez sur **Créer**.

   L'écran **Créer un rôle d'administrateur** apparaît.

4. Modifiez les détails du rôle au besoin et cliquez sur **Enregistrer** .

Suppression d'un rôle d'administrateur

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Gestion des comptes d'administrateur**.
3. Sur l'onglet **Rôles d'administrateur**, sélectionnez les rôles d'administrateur que vous souhaitez supprimer et cliquez sur **Supprimer**.

Modification du mot de passe de l'administrateur

Consultez la rubrique *Modification de compte d'administrateur à la page 2-16* sur la procédure de modification du mot de passe du compte administrateur.

Gestion de la file de commandes

Mobile Security enregistre toutes les commandes que vous avez exécutées depuis la console Web et vous permet d'annuler ou de renvoyer une commande, si nécessaire. Vous pouvez également supprimer les commandes qui ont déjà été exécutées et qu'il n'est pas nécessaire d'afficher sur la liste.

Pour accéder à l'écran **Gestion de la file de commandes,** accédez à **Administration** > **Gestion de la file de commandes**.

Le tableau suivant décrit tous les états des commandes sur l'écran **Gestion de la file de** commandes.

ÉTAT DE LA COMMANDE	DESCRIPTION
En attente d'envoi	Le serveur Mobile Security est en train d'envoyer la commande au dispositif mobile. Vous pouvez annuler la commande pendant qu'elle est dans cet état.
En attente de confirmation	Le serveur Mobile Security a envoyé la commande au dispositif mobile et est dans l'attente de l'accusé de réception du dispositif mobile.
Échoué	Impossible d'envoyer la commande vers le dispositif mobile.
Réussi	La commande a été envoyée vers le dispositif mobile.
Annulé	La commande a été annulée avant d'être envoyée au dispositif mobile.

Intégration d'Exchange Server

Configuration des paramètres d'intégration d'Exchange Server

Consultez la rubrique *Paramètres de configuration initiale d'Exchange Server* dans le *Manuel d'installation et de déploiement* pour obtenir la procédure de configuration complète.

Configuration du connecteur Exchange

Vous pouvez configurer le connecteur Exchange pour que les mises à jour s'effectuent automatiquement à chaque fois qu'une version plus récente est disponible.

Procédure

1. Sur l'ordinateur où le connecteur Exchange est installé, cliquez sur le bouton **Afficher les icônes cachées** dans la zone de notification de la barre de tâches Windows (près de l'horloge système).

2. Faites un clic droit sur l'icône du **Connecteur Exchange**, puis cliquez sur **À propos de Trend Micro Mobile Security - Connecteur Exchange**.

   L'écran À propos de Trend Micro Mobile Security - Connecteur Exchange s'affiche.

3. Configurez ce qui suit :

   - **Activez la mise à niveau automatique**—lorsque cette option est sélectionnée, le connecteur Exchange se met automatiquement à niveau sur une nouvelle version à chaque fois que celle-ci est disponible.
   - **Adresse du serveur**—adresse IP du serveur Mobile Security.
   - **Port HTTPS**—numéro de port HTTPS du serveur Mobile Security pour la console Web d'administration.

Gestion des certificats

Utilisez l'écran de **Gestion des certificats** pour télécharger `.pfx`, `.p12`, `.cer`, `.crt`, `.der` des certificats sur le serveur Mobile Security.

Télécharger un certificat

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Gestion des certificats**.
3. Cliquez sur **Ajouter**.

   La fenêtre **Ajouter un certificat** s'affiche.

4. Cliquez sur **Choisir fichier** puis choisissez un fichier certificat `.pfx`, `.p12`, `.cer`, `.crt`, `.der`.
5. Entrez le mot de passe du certificat dans le champ **Mot de passe**.

6. Cliquez sur **Enregistrer**.

Suppression de certificats

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Gestion des certificats**.
3. Sélectionnez les certificats que vous voulez supprimer puis cliquez sur **Supprimer**.

Chapitre 3

Gestion des dispositifs mobiles

Ce chapitre vous permet de vous familiariser avec Mobile Security. Il fournit des instructions de base relatives à la configuration et à l'utilisation. Avant d'aller plus loin, assurez-vous de bien installer le serveur d'administration, le serveur de communication, et l'agent de dispositif mobile sur les dispositifs mobiles.

Le chapitre contient les sections suivantes :

Onglet Dispositifs administrés

L'onglet **Dispositifs administrés** sur l'écran **Dispositifs** vous permet d'effectuer les tâches de configuration, d'organisation ou de recherche des agents de dispositif mobile. La barre d'outils située au-dessus de l'afficheur de l'arborescence des dispositifs vous permet d'effectuer les tâches suivantes :

- configurer l'arborescence des dispositifs (comme créer, supprimer ou renommer des groupes et créer ou supprimer des agents de dispositif mobile)
- rechercher et afficher l'état des agents de dispositif mobile
- mettre à jour des composants de l'agent de dispositif mobile à la demande, effacer/verrouiller/localiser un dispositif à distance et mettre à jour la stratégie
- configurer les informations des agents de dispositif mobile
- exporter des données pour une analyse ou une sauvegarde ultérieure

Groupes dans Mobile Security

Le serveur Mobile Security crée automatiquement un groupe racine **Dispositifs mobiles** comportant deux sous-groupes :

- **par défaut**—ce groupe contient des agents de dispositif mobile qui n'appartiennent à aucun autre groupe. Vous ne pouvez pas supprimer ni renommer le groupe **par défaut** dans l'arborescence des dispositifs Mobile Security.
- **non autorisé**—le serveur Mobile Security crée automatiquement ce groupe si **Authentification du dispositif** est activée dans **Paramètres d'inscription des dispositifs**, et qu'une liste des dispositifs mobiles est utilisée afin de les authentifier. Si un dispositif mobile inscrit ne figure pas dans la liste des dispositifs mobiles, Mobile Security déplace ce dispositif mobile vers le groupe **non autorisé**. Mobile Security crée également d'autres groupes et regroupe tous les dispositifs mobiles en fonction de la liste que vous utilisez.

Remarque

Si vous activez **Authentification du dispositif** dans **les paramètres d'inscription des dispositifs**, et que vous téléchargez une liste de dispositifs mobiles vierge pour la soumettre à l'authentification, Mobile Security déplacera tous les dispositifs mobiles actuels inscrits vers le groupe « non autorisé ».

Remarque

L'authentification du dispositif prend en charge uniquement les dispositifs mobiles Android et iOS.

Pour obtenir des instructions, consultez l'*Aide en ligne*du serveur Mobile Security.

Gestion des groupes

Vous pouvez ajouter, modifier ou supprimer des groupes dans le groupe racine **Dispositifs mobiles**. Cependant, vous ne pouvez pas renommer ni supprimer le groupe racine **Dispositifs mobiles** ni le groupe **par défaut**.

Ajout d'un groupe

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Sur l'onglet **Dispositifs administrés**, cliquez sur le groupe racine **Dispositifs mobiles**, puis cliquez sur **Ajouter un groupe**.
4. Saisissez le **Nom du groupe** et sélectionnez la **Stratégie** que vous souhaitez appliquer au groupe à partir de la liste déroulante.
5. Cliquez sur **Ajouter**.

Modification du nom d'un groupe

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Sur l'onglet **Dispositifs administrés**, cliquez sur le groupe que vous souhaitez renommer.
4. Cliquez sur **Modifier**.
5. Modifiez le nom du groupe et puis cliquez sur **Renommer**.

Suppression d'un groupe

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Sur l'onglet **Dispositifs administrés**, cliquez sur le groupe que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**, puis cliquez sur **OK** sur la boite de dialogue de confirmation.

Gestion des dispositifs mobiles

Vous pouvez envoyer une invitation aux dispositifs mobiles, modifier les informations des dispositifs mobiles, supprimer des dispositifs mobiles, ou changer le groupe des dispositifs mobiles sur l'écran **Dispositifs**.

Envoi d'invitations aux dispositifs mobiles

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Vous pouvez désormais inviter un dispositif mobile, un lot de dispositifs mobiles, un groupe d'utilisateurs ou d'adresses électroniques (liste de distribution) depuis Active Directory :

   - Pour inviter un dispositif mobile :

     a. Cliquez sur **Inviter des utilisateurs** > **Inviter un seul utilisateur**.

        La fenêtre **Inviter un seul utilisateur** s'ouvre.

     b. Dans la fenêtre **Inviter un seul utilisateur**, configurez les champs suivants :

        - **Numéro de téléphone**—saisissez le numéro de téléphone d'un dispositif portable. Pour vous assurer que le dispositif mobile peut correctement recevoir des messages de notification d'un expéditeur de SMS, vous pouvez entrer l'indicatif de pays (contenant entre 1 et 5 chiffres). Inutile de saisir le préfixe international de numérotation directe.
        - **Courriel**—entrez l'adresse électronique de l'utilisateur pour envoyer un courriel de notification.
        - **Nom d'utilisateur**—tapez le nom du dispositif mobile pour l'identifier dans l'arborescence des dispositifs.

- **Groupe**—sélectionnez le nom du groupe auquel le dispositif mobile appartient depuis la liste déroulante. Vous pourrez modifier ultérieurement le groupe auquel l'agent de dispositif mobile appartient.

Conseil

Pour ajouter d'autres dispositifs, cliquez sur le bouton  .

- Pour inviter un lot de dispositifs mobiles :

  a. Cliquez sur **Inviter des utilisateurs** > **Inviter un lot**.

  b. Entrez les informations des dispositifs en utilisant le format suivant dans la zone de texte de la fenêtre qui s'affiche :

  numéro_téléphone, adresse_électronique, nom_dispositif, nom_groupe, numéro_inventaire (facultatif), description (facultatif) ;

Remarque

Utilisez des points virgules (;) ou «CR» pour séparer chaque information de dispositif.

  c. Cliquez sur **Valider** pour vérifier si les informations des dispositifs sont conformes au format indiqué.

- Pour inviter un groupe d'utilisateurs ou d'adresses électroniques (liste de distribution) à partir d'Active Directory :

  a. Cliquez sur **Inviter des utilisateurs** > **Inviter à partir d'Active Directory**.

  b. Entrez les informations utilisateur dans le champ de recherche fourni et cliquez sur **Rechercher**.

  c. Sélectionnez l'utilisateur parmi les résultats de la recherche et cliquez sur **Inviter des dispositifs**.

4. Cliquez sur **Enregistrer**.

Mobile Security envoie un SMS ou un courriel d'invitation aux utilisateurs des dispositifs invités.

Modification des informations d'un dispositif mobile

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Dans l'onglet **Dispositifs administrés**, cliquez sur le dispositif mobile dont vous souhaitez modifier les informations dans l'arborescence des dispositifs.
4. Cliquez sur **Modifier**.
5. Mettez à jour les informations dans les champs suivants :

   - **Numéro de téléphone**—numéro de téléphone du dispositif mobile. Pour vous assurer que le dispositif mobile peut correctement recevoir des messages de notification d'un expéditeur de SMS, vous pouvez entrer l'indicatif de pays (contenant entre 1 et 5 chiffres). Inutile de saisir le préfixe international de numérotation directe.
   - **E-mail**—adresse électronique de l'utilisateur pour l'envoi de courriel de notification.
   - **Nom du dispositif**—nom du dispositif mobile pour l'identifier dans l'arborescence des dispositifs.
   - **Groupe**—sélectionnez le nom du groupe auquel le dispositif mobile appartient depuis la liste déroulante.
   - **Numéro d'inventaire**—tapez le numéro d'inventaire affecté au dispositif mobile.
   - **Description**—toutes informations ou notes supplémentaires relatives au dispositif mobile ou à l'utilisateur.

6. Cliquez sur **Enregistrer**.

Suppression de dispositifs mobiles

Mobile Security propose les deux options suivantes pour supprimer des dispositifs mobiles :

- *Suppression d'un seul dispositif mobile à la page 3-8*
- *Suppression de plusieurs dispositifs mobiles à la page 3-8*

Suppression d'un seul dispositif mobile

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Dans l'onglet **Dispositifs administrés**, cliquez sur le dispositif mobile que vous souhaitez supprimer dans l'arborescence des dispositifs.
4. Cliquez sur **Supprimer**, puis cliquez sur **OK** sur la boite de dialogue de confirmation.

Le dispositif mobile est supprimé de l'arborescence des dispositifs mobiles, et n´est plus inscrit sur le serveur de Mobile Security.

Suppression de plusieurs dispositifs mobiles

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.

3. Dans l'onglet **Dispositifs administrés**, cliquez sur le groupe contenant les dispositifs mobiles que vous souhaitez supprimer dans l'arborescence des dispositifs.

4. Sélectionnez les dispositifs mobiles dans la liste du volet droit, cliquez sur **Supprimer**, puis cliquez sur **OK** sur la boîte de dialogue de confirmation.

   Les dispositifs mobiles sont supprimés de l'arborescence des dispositifs mobiles, et ne sont plus inscrits sur le serveur de Mobile Security.

Déplacement de dispositifs mobiles vers un autre groupe

Vous pouvez déplacer les dispositifs mobiles d'un groupe à un autre. Mobile Security enverra automatiquement la notification des stratégies que vous avez appliquées au groupe à l'utilisateur.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Sur l'onglet **Dispositifs administrés**, cliquez sur le groupe contenant les dispositifs mobiles que vous souhaitez déplacer.
4. Sélectionnez les dispositifs mobiles de la liste dans le volet de droite, puis cliquez sur **Déplacer**.

   La boîte de dialogue **Déplacer les dispositifs** s'affiche.
5. Dans la liste déroulante, sélectionnez le groupe cible, puis cliquez sur **OK**.

État du dispositif mobile

Sur l'onglet **Dispositifs administrés** de l'écran **Dispositifs,** sélectionnez le dispositif mobile pour afficher les informations relatives à son état sur le panneau de droite. Les informations relatives au dispositif mobile sont répartie dans les sections suivantes :

- **Éléments de base**—inclut l'état d'enregistrement, le numéro de téléphone, le compte LDAP ainsi que les informations relatives à la plate-forme.
- **Matériel, Système d'exploitation**—affiche les informations détaillées du dispositif mobile, dont le nom du dispositif et du modèle, la version du système d'exploitation, les informations relatives à la mémoire, la technologie cellulaire, les numéros IMEI et les numéros MEID ainsi que les informations relatives à la version du micrologiciel.
- **Sécurité**—affiche l'état de chiffrement du dispositif mobile et indique si le dispositif mobile est débridé ou non.
- **Réseau**—affiche l'identité de la carte circuit intégré (ICCID), les informations relatives aux MAC bluetooth et WiFi, les informations détaillées relatives au réseau, comprenant le nom du réseau du fournisseur, la version des paramètres, le statut d'itinérance ainsi que les informations relatives aux indicatifs de pays pour les mobiles (MCC) et codes de réseau mobile (MNC).
- **Stratégie**—affiche les date et heure auxquelles la stratégie de sécurité et la configuration ont été mises à jour pour la dernière fois.
- **Applications installées**—affiche la liste de toutes les applications installées sur le dispositif mobile et le résultat de la vérification de la compatibilité. Cet onglet est uniquement disponible pour les dispositifs mobiles Android et iOS.

Recherche simple d'un agent de dispositif mobile

Pour rechercher un agent de dispositif mobile à partir du nom du dispositif ou du numéro de téléphone, saisissez l'information dans l'écran **Dispositifs** et cliquez sur **Rechercher**. Les résultats de la recherche s'affichent dans l'arborescence des dispositifs.

Recherche avancée des agents de dispositif mobile

Vous pouvez utiliser l'écran **Recherche avancée** pour indiquer davantage de critères pour la recherche d'agents de dispositif mobile.

Procédure

1. Dans l'écran **Dispositifs**, cliquez sur le lien **Recherche avancée**. Une fenêtre contextuelle s'affiche.

2. Sélectionnez les critères de recherche et tapez les valeurs dans les champs prévus (le cas échéant):

   - **Nom du dispositif**—nom descriptif qui identifie le dispositif mobile
   - **Numéro de téléphone**—numéro de téléphone d'un dispositif mobile
   - **Numéro d'actif**—numéro d'actif d'un dispositif mobile
   - **Description** —description d'un dispositif mobile
   - **Système d'exploitation**—système d'exploitation du dispositif mobile
   - **Groupe**—groupe auquel appartient le dispositif mobile
   - **Version de l'agent**—numéro de version des agents du dispositif mobile sur le dispositif mobile
   - **Version du fichier de signatures de programmes malveillants**—numéro de version du fichier de signatures de programmes malveillants sur le dispositif mobile
   - **Version du moteur de scan contre les programmes malveillants**—numéro de version du moteur de scan anti-programmes malveillants du dispositif mobile
   - **Agent de dispositif mobile infecté**—limite la recherche aux dispositifs mobiles avec le nombre spécifié de programmes malveillants détectés
   - **État du dispositif** —limite la recherche à un ou plusieurs états des dispositifs mobiles sélectionnés

3. Cliquez sur **Rechercher**. Les résultats de la recherche s'affichent dans l'arborescence des dispositifs.

Options d'affichage de l'arborescence du dispositif

Si vous sélectionnez un groupe dans l'arborescence des dispositifs, vous pouvez utiliser la case **Colonne** de la liste déroulante pour sélectionner l'une des vues prédéfinies : **Affichage général** et **Afficher tout**. Cela vous permet d'afficher rapidement les informations présentées dans l'arborescence du dispositif. Les informations affichées dans l'arborescence des dispositifs varient en fonction de l'option sélectionnée.

Tâches de l'agent de dispositif mobile

Trend Micro Mobile Security vous permet d'effectuer différentes tâches sur les dispositifs mobiles à partir de l'écran **Dispositifs**.

Mise à jour des agents de dispositif mobile

Vous pouvez envoyer la notification de mise à jour aux dispositifs mobiles possédant des composants ou des stratégies de sécurité obsolètes depuis l'onglet **Dispositifs administrés** dans l'écran **Dispositifs**.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Sur l'onglet **Dispositifs administrés**, cliquez sur le groupe pour lequel vous souhaitez mettre à jour les dispositifs mobiles.
4. Cliquez sur **Mise à jour**.

Mobile Security envoie la notification de mise à jour à tous les dispositifs mobiles avec les composants ou les stratégies de sécurité obsolètes.

Vous pouvez également utiliser l'écran **Mise à jour** pour définir l'envoi automatique des notifications de mise à jour de Mobile Security vers les dispositifs mobiles avec les

composants ou les stratégies obsolètes ou vous pouvez initier le processus manuellement.

Voir *Mise à jour des composants de Mobile Security à la page 6-2* pour de plus amples informations.

Sur les dispositifs mobiles Windows Mobile ou Symbian, si vous n'avez pas activé la fonction de messagerie SMS pour Mobile Security, vous devez configurer la programmation de mise à jour dans l'écran **Stratégies courantes** (voir *Stratégie courante à la page 4-7*) pour mettre régulièrement à jour les composants. Cependant, pour les dispositifs mobiles Android, si vous n'avez pas activé la fonction de messagerie SMS pour Mobile Security, vous pouvez également mettre à jour les composants et synchroniser les stratégies par le biais d'instructions push.

Protection contre la perte du dispositif

Si un utilisateur perd ou égare le dispositif mobile, vous pouvez localiser, verrouiller ou effacer toutes les données de ce dispositif mobile à distance.

Localisation à distance d'un dispositif mobile

Vous pouvez localiser le dispositif mobile via le réseau sans fil ou en utilisant le GPS du dispositif mobile. Le serveur de Mobile Security affiche la localisation du dispositif mobile sur Google Maps.

Cette fonction est disponible pour les dispositifs mobiles Android uniquement.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Dans l'onglet **Dispositifs administrés**, cliquez sur le dispositif mobile que vous souhaitez localiser dans l'arborescence des dispositifs.
4. Cliquez sur **Localisation du dispositif**, puis cliquez sur **OK** sur la boite de dialogue de confirmation.

Le serveur de Mobile Security tente de localiser le dispositif mobile et affiche le lien Google Maps sur l'écran **Localisation à distance de dispositif**.

5. Cliquez sur le lien de Google Maps sur l'écran **Localisation à distance de dispositif** pour voir la plus récente position GPS du dispositif mobile sur la carte.

Verrouillage à distance d'un dispositif mobile

Vous pouvez envoyer une instruction de verrouillage depuis la console Web d'administration pour verrouiller à distance un dispositif mobile. Les utilisateurs doivent entrer le mot de passe de mise sous tension pour déverrouiller le dispositif mobile.

Remarque

Cette fonction est prise en charge pour Android, iOS, BlackBerry et Windows Mobile uniquement.

Pour utiliser cette fonction avec des dispositifs Windows Mobile, le chiffrement doit être activé sur le dispositif mobile.

Un dispositif Windows Mobile ne peut être verrouillé que par le biais d'un message de notification par SMS. Si vous souhaitez verrouiller un dispositif Windows Mobile, assurez-vous que vous avez configuré un expéditeur de SMS. Consultez le *Manuel d'installation et de déploiement* pour une configuration détaillée.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Dans l'onglet **Dispositifs administrés**, cliquez sur le dispositif mobile que vous souhaitez verrouiller dans l'arborescence des dispositifs.
4. Cliquez sur **Verrouillage à distance**, puis cliquez sur **OK** sur la boite de dialogue de confirmation.

   Le message **Réussi** s'affiche à l'écran si la commande de verrouillage est générée correctement. Pour vérifier si le dispositif mobile est verrouillé correctement, vous

pouvez vérifier l'état de la commande sur l'écran **Gestion de la file de commandes**. Voir *Gestion de la file de commandes à la page 2-19* pour plus de détails.

Effacement à distance d'un dispositif mobile

Vous pouvez réinitialiser à distance le dispositif mobile aux réglages d'usine et effacer la carte SD ou la mémoire interne du dispositif mobile. Cette fonction permet de garantir la sécurité des données pour les dispositifs mobiles perdus, volés ou égarés. Vous pouvez également choisir d'effacer sur le dispositif mobile uniquement les données professionnelles suivantes :

- pour Android : Courriels, calendrier et contacts Exchange
- pour iOS : Profils, stratégies connexes, configurations et données MDM

AVERTISSEMENT!

Utilisez cette fonction avec précaution, cette action est IRRÉVERSIBLE. Toutes les données seront perdues et irrécupérables.

Remarque

Cette fonction est prise en charge pour Android, iOS, BlackBerry et Windows Mobile uniquement.

Pour obtenir des instructions sur l'effacement d'un dispositif mobile qui utilise ActiveSync, voir *Effacement à distance d'un dispositif mobile ActiveSync à la page 3-24*.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Dans l'onglet **Dispositifs administrés**, cliquez sur le dispositif mobile que vous souhaitez effacer dans l'arborescence des dispositifs.

4. Cliquez sur **Effacement à distance**.

   L'écran **Effacement à distance de dispositif** s'affiche.

5. Sélectionnez la case Nom du dispositif appropriée.

6. Effectuez l'une des actions suivantes :

   - Pour un dispositif mobile Android, sélectionnez une des options suivantes :

     - **Réinitialiser toutes les données avec les paramètres d'usine. (Toutes les applications et les données enregistrées seront supprimées. La carte mémoire insérée sera formatée. Cette action est irréversible.)**

     - **Effacer courriels, calendrier et liste de contacts.**—cette action est également appelée « suppression sélective ».

       Si vous sélectionnez cette option, vous pouvez également sélectionner la case **Réinitialiser toutes les données aux paramètres d'usine si la Suppression sélective a échoué.**.

   - Pour un dispositif mobile iOS, sélectionnez une des options suivantes :

     - **Réinitialiser toutes les données avec les paramètres d'usine. (Toutes les applications et les données enregistrées seront supprimées. La carte mémoire insérée sera formatée. Cette action est irréversible.)**

     - **Effacer tous les profils, stratégies, configurations en service et leurs données correspondantes.**

7. Cliquez sur **Effacement à distance du dispositif**.

   Les données sélectionnées sont supprimées du dispositif mobile et l'agent de dispositif mobile n'est plus enregistré sur le serveur.

Réinitialisation du mot de passe à distance

Si un utilisateur oublie le mot de passe de mise sous tension, vous pouvez le réinitialiser à distance et déverrouiller le dispositif mobile à partir du serveur d'administration. Une

fois le dispositif mobile déverrouillé, l'utilisateur peut se connecter et modifier le mot de passe de mise sous tension.

Remarque

Cette fonction est prise en charge uniquement sur les dispositifs Android, iOS et Windows Mobile.

Réinitialisation du mot de passe pour un dispositif mobile Android

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Sélectionnez le dispositif mobile depuis l'arborescence, puis cliquez sur **Réinitialisation du mot de passe**.
4. Entrez et confirmez le nouveau mot de passe à six chiffres dans la boîte de dialogue contextuelle qui apparaît.

Suppression du mot de passe pour un dispositif mobile iOS

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Sélectionnez le dispositif mobile dans l'arborescence, puis cliquez sur **Réinitialisation du mot de passe**.

4. Cliquez sur **OK** dans la boîte de dialogue de confirmation qui apparaît. Le mot de passe de mise sous tension pour le dispositif mobile iOS sélectionné sera alors supprimé.

Réinitialisation du mot de passe pour un dispositif Windows Mobile

Pour réinitialiser le mot de passe d'un dispositif Windows Mobile, vous devrez demander à l'utilisateur de générer un code d'accès (nombre hexadécimal à 16 chiffres) sur le dispositif mobile avant de pouvoir déverrouiller le dispositif mobile à distance.

Procédure

1. Obtenez le nom du dispositif mobile et le code d'accès généré par l'utilisateur sur le dispositif mobile. Conseillez aux utilisateurs de consulter l'Aide de l'agent de dispositif mobile ou le *Guide de l'utilisateur* pour obtenir des instructions relatives à la génération du code d'accès.
2. Connectez-vous à la console d'administration Mobile Security.
3. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
4. Dans l'onglet **Dispositifs administrés**, cliquez sur le dispositif mobile dont vous souhaitez réinitialiser le mot de passe dans l'arborescence des dispositifs.
5. Cliquez sur **Réinitialisation du mot de passe** puis sur **Sélectionner un dispositif** dans l'écran **Déverrouillage à distance**. L'arborescence des dispositifs s'affiche.
6. Sélectionnez le dispositif mobile que vous souhaitez déverrouiller à distance, puis cliquez sur **Sélectionner**.
7. Saisissez le code d'accès dans le champ prévu, puis cliquez sur **Générer**.
8. Le serveur de Mobile Security génère le code de réponse et l'affiche sur un écran contextuel.

9. Demandez à l'utilisateur de cliquer sur **Suivant** dans l'écran **Mot de passe** du dispositif mobile et de saisir le code de réponse pour déverrouiller le dispositif mobile.

Exportation de données

Sur l'onglet **Dispositifs administrés** dans l'écran **Dispositifs**, vous pouvez exporter les données pour une analyse plus approfondie ou une sauvegarde.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Sélectionnez dans l'arborescence des dispositifs le groupe de dispositifs mobiles dont vous souhaitez exporter les données.
4. Cliquez sur **Exporter**.
5. Si nécessaire, cliquez sur **Enregistrer** sur la fenêtre contextuelle qui apparaît pour enregistrer le fichier `.zip` sur votre ordinateur.
6. Extrayez le contenu du fichier téléchargé `.zip` et ouvrez le fichier `.csv` pour afficher les informations du dispositif mobile.

Onglet Dispositifs invités

L'onglet **Dispositifs invités** dans l'écran **Dispositifs** enregistre les invitations que Mobile Security a envoyées aux dispositifs mobiles afin qu'ils s'inscrivent.

Le courriel d'invitation par défaut contient les informations suivantes :

- Introduction à Trend Micro Mobile Security
- URL de téléchargement de l'agent de dispositif mobile

- Informations sur le serveur pour l'inscription du dispositif mobile
- Code QR pour une inscription facile

Sur l'onglet **Dispositifs invités**, vous pouvez :

- voir la liste d'invitation
- renvoyer les messages d'invitation aux dispositifs mobiles
- annuler les invitations actuelles
- supprimer les anciens enregistrements d'invitation

Affichage de la liste d'invitation

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Cliquez sur l'onglet **Dispositifs invités**.

   Le tableau suivant fournit la description de tous les états d'invitation affichés sur l'onglet **Dispositifs invités**.

ÉTAT DE L'INVITATION	DESCRIPTION
Active	L'invitation est valable et l'utilisateur peut utiliser les informations contenues dans le message d'invitation pour s'inscrire.
Expirée	L'invitation a expiré et l'utilisateur ne peut plus utiliser les informations contenues dans le message d'invitation pour s'inscrire.

ÉTAT DE L'INVITATION	DESCRIPTION
Utilisée	L'utilisateur a déjà utilisé les informations contenues dans le message d'invitation pour s'inscrire et la clé d'inscription n'est plus valide. **Remarque** Ce état ne s'affiche que lorsque l'**option de limitation d'utilisation de clé d'inscription** est définie à **Utiliser une seule fois** dans les paramètres d'inscription de dispositifs.
Annulée	L'invitation est annulée dans le serveur et l'utilisateur ne peut pas utiliser les informations contenues dans le message d'invitation pour s'inscrire.

Nouvel envoi de messages d'invitation

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Cliquez sur l'onglet **Dispositifs invités**.
4. Sélectionnez les dispositifs mobiles de la liste auxquels vous souhaitez renvoyer l'invitation.
5. Cliquez sur **Renvoyer invitation**.

Annulation des invitations actives

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Cliquez sur l'onglet **Dispositifs invités**.
4. Sélectionnez les dispositifs mobiles de la liste pour lesquels vous souhaitez annuler l'invitation.
5. Cliquez sur **Annuler Invitation**.

Supprimer des invitations de la liste

Remarque

Vous ne pouvez supprimer que le message d'une invitation dont l'état est **Utilisée** ou **Annulée**.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Cliquez sur l'onglet **Dispositifs invités**.
4. Sélectionnez les dispositifs mobiles dans la liste pour lesquels vous souhaitez supprimer l'enregistrement d'invitation.
5. Cliquez sur **Supprimer Invitation**.

Onglet Dispositifs Exchange ActiveSync

Après avoir activé l'intégration d'Exchange Server sur le serveur Mobile Security, l'onglet **Dispositifs Exchange ActiveSync** sur l'écran **Dispositifs** affiche la liste des dispositifs mobiles qui se connectent à Exchange Server via le service ActiveSync.

Sur l'onglet **Dispositifs Exchange ActiveSync**, vous pouvez effectuer les actions suivantes :

- Inviter des dispositifs mobiles
- Autoriser ou bloquer l'accès à Exchange Server
- Activer l'effacement à distance sur demande
- Annuler l'effacement à distance
- Supprimer des dispositifs mobiles de la liste.

Invitation des dispositifs mobiles Exchange ActiveSync

Avant d'inviter des dispositifs mobiles Exchange ActiveSync, assurez-vous que vous avez configuré les paramètres de notifications/rapports sur le serveur d'administration. Consultez la rubrique *Paramètres de configuration des notifications/rapports* dans le *Manuel d'installation et de déploiement*.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Cliquez sur l'onglet **Dispositifs Exchange ActiveSync**.
4. Choisissez un dispositif mobile que vous souhaitez inviter à accéder à Exchange ActiveSync.
5. Cliquez sur **Inviter**, puis cliquez sur **OK** sur l'écran de confirmation.

Mobile Security envoie SMS et courriels d'invitation à l'utilisateur du dispositif mobile invité. Une fois le dispositif mobile inscrit sur le serveur Mobile Security, la colonne **Dispositif administré** indique l'état de l'agent de dispositif mobile.

Autorisation ou blocage de l'accès à Exchange Server

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Cliquez sur l'onglet **Dispositifs Exchange ActiveSync**.
4. Sélectionnez un dispositif mobile auquel vous souhaitez autoriser ou bloquer l'accès au Serveur Exchange.
5. Cliquez sur **Autoriser accès** ou **Bloquer accès**, puis cliquez sur **OK** sur la boite de dialogue de confirmation.

   L'état du dispositif mobile dans la colonne **État de l'accès à Exchange** affiche le nouvel état après la synchronisation du dispositif mobile avec Exchange Server.

Effacement à distance d'un dispositif mobile ActiveSync

Vous pouvez réinitialiser à distance le dispositif mobile ActiveSync aux réglages d'usine et effacer la carte SD ou la mémoire interne du dispositif mobile. Cette fonction permet de garantir la sécurité des données pour les dispositifs mobiles perdus, volés ou égarés.

AVERTISSEMENT!

Utilisez cette fonction avec précaution, cette action est IRRÉVERSIBLE. Toutes les données seront perdues et irrécupérables.

Pour obtenir des instructions sur l'effacement d'un dispositif mobile qui n'utilise pas ActiveSync, voir *Effacement à distance d'un dispositif mobile à la page 3-15*.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.
3. Cliquez sur l'onglet **Dispositifs Exchange ActiveSync**.
4. Sélectionnez les dispositifs mobiles à effacer.
5. Cliquez sur **Effacement à distance**.

   L'écran **Effacement à distance de dispositif** apparaît.
6. Sélectionnez le dispositif, puis cliquez sur **Effacement à distance de dispositif**.

Suppression d'un dispositif mobile ActiveSync

Le dispositif mobile que vous avez effacé à distance à partir du serveur Mobile Security ne sera plus en mesure d'accéder Exchange Server. Vous pouvez supprimer les informations de ce dispositif mobile de l'onglet **Dispositifs Exchange ActiveSync** sur l'écran **Dispositifs**.

Remarque

Vous ne pouvez que supprimer des dispositifs mobiles qui sont effacés à distance depuis le serveur Mobile Security.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.

3. Cliquez sur l'onglet **Dispositifs Exchange ActiveSync**.
4. Sélectionnez les dispositifs mobiles que vous souhaitez supprimer de la liste.
5. Cliquez sur **Supprimer**, puis cliquez sur **OK** sur l'écran de confirmation.

Intégration avec le gestionnaire de contrôle de Trend Micro

Trend Micro Mobile Security assure l'intégration avec le gestionnaire de contrôle de Trend Micro(également dénommé Control Manager ou TMCM). Cette intégration permet à l'administrateur du gestionnaire de contrôle de :

- créer, modifier ou supprimer les stratégies de sécurité de Mobile Security
- distribuer des stratégies de sécurité aux dispositifs mobiles inscrits
- afficher l'écran du **Tableau de bord** de Mobile Security.

Pour des informations détaillées sur le gestionnaire de contrôle de Trend Micro etla gestion des stratégies de Mobile Securitydans le gestionnaire de contrôle, consultez la documentation du produit à l'URL suivante :

http://docs.trendmicro.com/fr-fr/enterprise/control-manager.aspx

Création de stratégies de sécurité dans le gestionnaire de contrôle

La console Web du gestionnaire de contrôle Trend Micro affiche les mêmes stratégies de sécurité que celles disponibles dans Mobile Security. Si un administrateur du gestionnaire de contrôle crée une stratégie de sécurité pour Mobile Security, Mobile Security créera un nouveau groupe pour cette stratégie et déplacera tous les dispositifs mobiles cibles vers ce groupe. Pour différencier les stratégies qui sont créées dans Mobile Security des stratégies créées dans le gestionnaire de contrôle, Mobile Security ajoute le préfixe **TMCM_** au nom du groupe.

Suppression ou Modification de stratégies de sécurité

L'administrateur du gestionnaire de contrôle peut modifier une stratégie à tout moment et la stratégie sera déployée sur les dispositifs mobiles immédiatement.

Le gestionnaire de contrôle de Trend Micro synchronise les stratégies avec Trend Micro Mobile Security toutes les 24 heures. Si vous supprimez ou modifiez une stratégie qui est créée et déployée à partir du Gestionnaire de contrôle, la stratégie sera renvoyée aux paramètres d'origine ou créée à nouveau après la synchronisation.

États des stratégies de sécurité sur le gestionnaire de contrôle

Sur la console Web du gestionnaire de contrôle Trend Micro, les états suivants relatifs aux stratégies de sécurité sont affichés :

- **En attente** : la stratégie est créée sur la console Web du gestionnaire de contrôle et n'a pas encore été remise aux dispositifs mobiles.
- **Déployée** : la stratégie a été distribuée et déployée sur tous les dispositifs mobiles cibles.

Chapitre 4

Protection des dispositifs à l'aide de stratégies

Ce chapitre décrit comment configurer et appliquer des stratégies de sécurité sur des dispositifs mobiles d'un groupe Mobile Security. Vous pouvez utiliser des stratégies relatives à la mise en service, à la sécurité des dispositifs et à la protection des données.

Ce chapitre contient les sections suivantes :

À propos des stratégies de sécurité

Vous pouvez configurer des stratégies de sécurité pour un groupe Mobile Security sur le serveur d'administration. Ces stratégies s'appliquent à tous les dispositifs mobiles du groupe. Vous pouvez appliquer des stratégies de sécurité à tous les groupes Mobile Security en sélectionnant le groupe **Dispositifs mobiles** (groupe racine). Le tableau ci-dessous répertorie les stratégies de sécurité disponibles dans Mobile Security.

TABLEAU 4-1. Stratégies de sécurité de Mobile Security

GROUPE DE STRATÉGIES	STRATÉGIE	RÉFÉRENCE
Généralités	Stratégie commune	Voir la section *Stratégie courante à la page 4-7*.
Mise en service	Stratégie WiFi	Voir la section *Stratégie WiFi à la page 4-9*.
	Stratégie Exchange ActiveSync	Voir la section *Stratégie Exchange ActiveSync à la page 4-10*.
	Stratégie VPN	Voir la section *Stratégie VPN à la page 4-10*.
	Stratégie du proxy HTTP global	Voir la section *Stratégie du proxy HTTP global à la page 4-10*.
	Stratégie des certificats	Voir la section *Stratégie des certificats à la page 4-10*.
	Stratégie d'authentification unique	Voir la section *Stratégie d'authentification unique à la page 4-11*.

Groupe de stratégies	Stratégie	Référence
Sécurité de dispositif	Stratégie de protection contre les programmes malveillants	Voir la section *Stratégie de protection contre les programmes malveillants à la page 4-12*.
	Stratégie de prévention anti-spam	Voir la section *Stratégie de prévention anti-spam à la page 4-14*.
	Stratégie de filtrage des appels	Voir la section *Stratégie de filtrage des appels à la page 4-17*.
	Stratégie de pare-feu	Voir la section *Stratégie de pare-feu à la page 4-19*.
	Stratégie de protection contre les menaces Internet	Voir la section *Stratégie de protection contre les menaces Internet à la page 4-21*.
Dispositifs	Stratégie de mot de passe et de chiffrement	Voir la section *Stratégie de mot de passe et de chiffrement à la page 4-21*.
	Stratégie de verrouillage des fonctionnalités	Voir la section *Stratégie de verrouillage des fonctions à la page 4-26*.
	Stratégie de conformité	Voir la section *Stratégie de compatibilité à la page 4-27*.
Gestion des applications	Stratégie de surveillance et de contrôle des applications	Voir la section *Stratégie de surveillance et de contrôle des applications à la page 4-28*.
	Stratégie du programme d'achats en grande quantité	Voir la section *Stratégie du programme d'achats en volume à la page 4-30*.

Gestion des stratégies

Mobile Security vous permet de créer rapidement une stratégie à l'aide des modèles de stratégie de sécurité par défaut.

Utilisez l'écran **Stratégie** pour créer, modifier, copier ou supprimer des stratégies de sécurité pour les dispositifs mobiles.

Création d'une stratégie

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Stratégies** dans la barre de menu.

   L'écran **Stratégie** apparaît.
3. Cliquez sur **Créer**.

   L'écran **Créer stratégie** s'affiche.
4. Tapez le nom de la stratégie et la description dans leurs champs respectifs, puis cliquez sur **Enregistrer**.

   Mobile Security crée une stratégie avec les paramètres par défaut. Cependant, la stratégie n'est pas attribuée à un groupe. Pour attribuer la stratégie à un groupe, voir *Attribution ou suppression de la stratégie d'un groupe à la page 4-6*.

Modification d'une stratégie

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Stratégies** dans la barre de menu.

   L'écran **Stratégie** apparaît.
3. Dans la liste des stratégies, cliquez sur le nom de la stratégie que vous souhaitez modifier.

   L'écran **Modifier stratégie** s'affiche.

4. Modifiez les détails de la stratégie et puis cliquez sur **Enregistrer**.

Attribution ou suppression de la stratégie d'un groupe

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Stratégies** dans la barre de menu.

   L'écran **Stratégie** apparaît.
3. Dans la colonne **Groupes appliqués** d'une stratégie, cliquez sur le nom du groupe. Si la stratégie n'est pas attribuée à un groupe, cliquez sur **Aucun**.
4. Effectuez l'une des actions suivantes :
   - Pour attribuer une stratégie à un groupe : à partir des **Groupes disponibles** de la liste sur le côté gauche, sélectionnez le groupe auquel vous souhaitez appliquer la stratégie, puis cliquez sur **>** pour déplacer le groupe vers la droite.
   - Pour supprimer une stratégie d'un groupe : à partir de la liste des groupes sur le côté droit, sélectionnez un groupe que vous souhaitez supprimer, puis cliquez sur **<** pour déplacer le groupe vers la liste des **Groupes disponibles** sur le côté gauche.
5. Cliquez sur **Enregistrer**.

Copie d'une stratégie

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Stratégies** dans la barre de menu.

   L'écran **Stratégie** apparaît.

3. Sélectionnez la stratégie que vous voulez copier et puis cliquez sur **Copier**.

Suppression de stratégies

Vous ne pouvez pas supprimer la stratégie **Par défaut** ni une stratégie qui est appliquée à un groupe. Veillez à supprimer la stratégie de tous les groupes avant de supprimer une stratégie. Voir *Attribution ou suppression de la stratégie d'un groupe à la page 4-6* pour la procédure.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Stratégies** dans la barre de menu.

   L'écran **Stratégie** apparaît.
3. Sélectionnez la stratégie que vous voulez supprimer puis cliquez sur **Supprimer**.

Stratégies de sécurité de Mobile Security

Cette section présente les stratégies de sécurité qui sont disponibles dans Mobile Security.

Stratégie courante

La stratégie courante fournit les stratégies courantes de sécurité pour les dispositifs mobiles. Pour configurer les paramètres de stratégie courante de sécurité, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie courante**.

Dans **Stratégie courante** vous pouvez également attribuer des stratégies aux dispositifs mobiles BlackBerry.

- **Privilèges utilisateur** : Vous pouvez activer ou désactiver l'option permettant aux utilisateurs de désinstaller l'agent de dispositif mobile. De plus, vous pouvez choisir

d'autoriser ou non les utilisateurs à configurer les paramètres de l'agent de dispositif Mobile Security.

La liste suivante présente les fonctions associées à la désinstallation de la protection :

- activez/désactivez la désinstallation de la protection à partir de la console d'administration
- la longueur du mot de passe doit être d'un minimum de six (6) et d'un maximum de douze (12) caractères ; le mot de passe peut contenir chiffres, caractères ou symboles.
- un mot de passe peut être défini pour chaque groupe à partir de la console d'administration.

Si vous ne cochez pas la case **Autoriser les utilisateurs à configurer les paramètres clients de Mobile Security**, les utilisateurs ne peuvent pas modifier les paramètres de l'agent de dispositif mobile. Toutefois, les listes de filtrage pour la **Stratégie de prévention anti-spam**, la **Stratégie de filtrage des appels** et la **Stratégie de Protection contre les menaces Internet** ne sont pas affectées lorsque cette option est sélectionnée. Pour de plus amples informations, voir *Stratégies de prévention anti-spam par SMS à la page 4-14*, *Stratégies de prévention anti-spam WAP-Push à la page 4-16* et *Stratégie de protection contre les menaces Internet à la page 4-21*.

- **Paramètres de mise à jour**: Vous pouvez configurer le serveur Mobile Security pour qu'il avertisse les agents de dispositif mobile lorsqu'un nouveau composant est disponible pour mise à jour. Vous pouvez aussi sélectionner l'option de vérification automatique pour que les agents de dispositif mobile vérifient régulièrement la disponibilité de mises à jour de configuration ou de composants sur le serveur de Mobile Security.

  Lorsque vous activez l'option de notification de connexion sans fil, un écran d'invite s'affiche sur les dispositifs mobiles avant que les agents de dispositif mobile ne se connectent au serveur de communication via une connexion sans fil (de type

3G ou GPRS). Les utilisateurs peuvent choisir d'accepter ou de refuser la demande de connexion.

FIGURE 4-1. Stratégie courante, section des paramètres de mise à jour

- **paramètres des journaux** : Lorsque les agents de dispositif mobile détectent un risque de sécurité, par exemple un fichier infecté ou une violation de pare-feu, un journal est généré sur les dispositifs mobiles. Si le module de chiffrement est activé, les journaux de chiffrement sont également générés. Vous pouvez paramétrer les dispositifs mobiles afin qu'ils envoient ces journaux au serveur Mobile Security. Utilisez ce paramètre si vous voulez analyser le nombre d'infections ou identifier les éventuelles attaques de réseau et prendre les mesures adéquates pour empêcher la propagation de ces menaces.
- **Paramètres de notification/rapport** : Choisissez d'afficher ou non un écran d'invite sur les dispositifs mobiles lorsqu'un agent de dispositif mobile tente d'établir une connexion au serveur de communication.
- **Paramètres Blackberry** : Vous permet de configurer les paramètres de stratégie courante pour les dispositifs mobiles BlackBerry.

Remarque

Vous devez configurer les paramètres BlackBerry dans les paramètres du serveur de communication pour pouvoir configurer les paramètres de stratégie. Consultez la rubrique *Paramètres du serveur de communication de configuration de BlackBerry* dans le *Manuel d'installation et de déploiement*.

Stratégie WiFi

La stratégie Wi-Fi vous permet de fournir les informations du réseau Wi-Fi de votre organisation aux dispositifs mobiles Android et iOS, en particulier le nom, le type de sécurité et le mot de passe du réseau.

Pour configurer les paramètres de Stratégie Wi-Fi, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie Wi-Fi**.

Stratégie Exchange ActiveSync

La stratégie Exchange ActiveSync vous permet de créer une stratégie Exchange ActiveSync pour votre organisation et de la diffuser aux dispositifs mobiles iOS.

Pour configurer les paramètres de stratégie Exchange ActiveSync, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie Exchange ActiveSync**.

Stratégie VPN

La stratégie VPN vous permet de créer une stratégie VPN pour votre organisation et de la distribuer aux dispositifs mobiles iOS.

Pour configurer les paramètres de stratégie VPN, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **stratégie VPN**

Stratégie du proxy HTTP global

La stratégie du proxy HTTP global vous permet de fournir des informations sur le proxy de votre organisation aux dispositifs mobiles. Cette stratégie s'applique uniquement aux dispositifs mobiles iOS qui sont en mode surveillé.

Pour configurer les paramètres du proxy HTTP global, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie du proxy HTTP global**

Stratégie des certificats

La stratégie des certificats vous permet d'importer des certificats que vous avez besoin de déployer sur des dispositifs mobiles iOS.

Pour configurer les paramètres de stratégie des certificats, cliquez sur **Stratégies**, puis sur le nom de la stratégie, et enfin sur **Stratégie des certificats**.

Stratégie d'authentification unique

La stratégie d'authentification unique (SSO) permet l'utilisation des mêmes informations d'authentification sur un ensemble d'applications, y comprisMobile Security et des applications de l'App Store. Chaque nouvelle application configurée avec une certification SSO vérifie les autorisations des utilisateurs sur les ressources de l'entreprise et les connecte sans leur demander de saisir à nouveau leur mot de passe.

La stratégie d'authentification unique comprend les informations suivantes :

- **Nom** : le nom principal Kerberos.
- **Zone** : le nom de zone Kerberos.

  La casse du nom de zone Kerberos doit être respectée.
- **Préfixes des URL** (facultatif) : liste des URL permettant l'utilisation d'un compte pour l'authentification Kerberos sur HTTP. Si ce champ est vide, le compte peut fonctionner avec toutes les URL http et https. Les modèles de correspondance des URL doivent commencer par http ou https.

  Chaque entrée de la liste doit contenir un préfixe d'URL. Seules les URL commençant par l'une des chaînes d'un compte sont autorisées à accéder au ticket Kerberos. Les modèles de correspondance d'URL doivent inclure le schéma. Par exemple, http://www.exemple.com/. Si un modèle de correspondance ne se termine pas par /, un / est automatiquement ajouté à l'URL.
- **Identifiants d'applications** (facultatif) : liste des identifiants d'applications autorisés à utiliser le compte. Si ce champ est vide, ce compte correspond à tous les identifiants d'applications.

  Le tableau **Identifiants d'applications** doit contenir des chaînes correspondant aux ID d'offres groupées d'applications. Ces chaînes doivent être des correspondances exactes (par exemple, com.monentreprise.monapp) ou peuvent avoir un préfixe correspondant à l'ID d'offre groupée grâce à l'utilisation du caractère générique *. Le caractère générique doit figurer après un point (.), et peut uniquement se trouver en fin de chaîne (par exemple, com.monentreprise.*). Lorsqu'un caractère générique est utilisé, toute application dont l'ID d'offre groupée commence par ce préfixe peut accéder au compte.

Pour configurer les paramètres de la stratégie d'authentification unique pour iOS, cliquez sur **Stratégies**, puis sur le nom de la stratégie, et enfin sur **Stratégie d'authentification unique**.

Stratégie de protection contre les programmes malveillants

Vous pouvez configurer des stratégies de protection contre les menaces comprenant : Type d'analyse (analyse en temps réel et analyse de la carte), mesures prises contre les programmes malveillants, nombre de couches de compression à analyser et type de fichier.

Pour configurer les paramètres de stratégie de protection contre les programmes malveillants, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie de protection contre les programmes malveillants**.

- **Types d'analyse** : Mobile Security fournit plusieurs types d'analyse pour protéger les dispositifs mobiles des programmes malveillants.
    - **Analyse en temps réel** : L'agent de dispositif mobile analyse les fichiers des dispositifs mobiles en temps réel. Si l'agent de dispositif mobile ne détecte aucun risque de sécurité, les utilisateurs peuvent alors ouvrir ou enregistrer le fichier. Si l'agent de dispositif mobile détecte un risque de sécurité, le résultat d'analyse s'affiche et indique le nom du fichier et le risque de sécurité en question. Mobile Security génère un journal contenant le résultat d'analyse sur le dispositif mobile. Le journal d'analyse est envoyé et stocké dans la base de données de Mobile Security.
    - **Analyser après insertion de la carte SD** : Si vous sélectionnez cette option dans l'écran **Stratégie de protection contre les programmes malveillants**, Mobile Security analyse les données sur une carte mémoire lorsqu'elle est insérée dans le dispositif mobile. Ainsi, les fichiers infectés ne peuvent pas être propagés.
    - **Analyse après mise à jour des signatures** : Si vous sélectionnez cette option dans l'écran **Stratégie de protection contre les programmes malveillants**, Mobile Security lance une analyse automatique pour détecter les menaces de sécurité après une mise à jour réussie des signatures sur les dispositifs mobiles Android.

- **Options d'analyse**

  - **Action sur les programmes malveillants** : Lorsqu'un programme malveillant est détecté sur un dispositif mobile, Mobile Security peut supprimer ou placer en quarantaine le fichier infecté. Si le fichier est en cours d'utilisation, le système d'exploitation peut en refuser l'accès.

    - Quarantaine—renomme puis déplace un fichier infecté dans le répertoire de quarantaine du dispositif mobile`\TmQuarantine` (pour Windows Mobile) ou `{Disk Label}\TmQuarantine` (pour Symbian OS).

    - Supprimer—supprime le fichier infecté.

    Lorsqu'ils sont connectés, les agents de dispositif mobile envoient des journaux de programmes malveillants au serveur de Mobile Security.

    

    Remarque

    Les actions associées à l'analyse s'appliquent uniquement à l'analyse en temps réel.

  - **Couches de compression à analyser** : Pour les fichiers ZIP et CAB, vous pouvez spécifier le nombre de couches de compression à analyser. Si le nombre de compressions dans un fichier ZIP/CAB dépasse ce nombre, Mobile Security n'effectuera pas d'analyse du fichier. Mobile Security ne prendra aucune mesure supplémentaire tant que le nombre de couches de compression approprié n'est pas spécifié.

    Vous pouvez paramétrer Mobile Security afin qu'il analyse les fichiers exécutables, les fichiers ZIP/CAB ou tous les fichiers sur les dispositifs mobiles.

  - **Analyser l'emplacement** : Pour les dispositifs mobiles Android, sélectionnez si vous souhaitez analyser la mémoire interne du dispositif mobile et/ou la carte SD insérée. Pour Symbian, Mobile Security analyse la mémoire interne du dispositif mobile ainsi que la carte SD insérée.

  - **Type de fichier** : Sélectionnez les types de fichier à analyser dans les dispositifs mobiles.

Stratégie de prévention anti-spam

La stratégie de prévention anti-spam de Mobile Security fournit une protection contre les messages spam WAP-push et SMS.

Pour configurer les paramètres de stratégie de prévention anti-spam, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie de prévention anti-spam**.

Stratégies de prévention anti-spam par SMS

Cette fonction vous offre un contrôle côté serveur des stratégies de prévention anti-spam par SMS. Les fonctions suivantes sont disponibles lors de la configuration des stratégies de prévention anti-spam par SMS :

- activer ou désactiver la prévention anti-spam par SMS sur le dispositif mobile
- configurer le dispositif mobile de manière à utiliser une liste de numéros bloqués, une liste de numéros approuvés, ou désactiver la fonction anti-spam par SMS sur le dispositif mobile.
- configurer une liste approuvée à partir de la console d'administration
- configurer une liste bloquée à partir de la console d'administration

Consultez le tableau ci-dessous pour les détails de configuration des listes de filtrage approuvée et bloquée.

TABLEAU 4-2. Configuration de la liste de filtrage de la stratégie de prévention anti-spam par SMS

CONTRÔLE CENTRAL	CONTRÔLE UTILISATEUR	DESCRIPTION
Désactivé	Activé	L'utilisateur peut modifier la liste approuvée/bloquée sur l'agent de dispositif mobile. Mobile Security autorise ou bloque les messages selon l'ordre de priorité suivant : 1. Liste approuvée sur l'agent de dispositif mobile 2. Liste bloquée sur l'agent de dispositif mobile
Activé	Désactivé	L'utilisateur peut uniquement modifier la liste approuvée/bloquée sur l'agent de dispositif mobile. Mobile Security autorise ou bloque les messages selon l'ordre de priorité suivant : 1. Liste approuvée ou liste bloquée sur le serveur 2. Liste approuvée sur l'agent de dispositif mobile 3. Liste bloquée sur l'agent de dispositif mobile
Activé	Activé	L'utilisateur peut afficher ou modifier la liste approuvée/bloquée définie par l'administrateur et peut également utiliser la liste approuvée/bloquée sur l'agent de dispositif mobile. Lorsque les stratégies de sécurité se synchronisent avec l'agent de dispositif mobile, les listes de filtrage ne sont pas synchronisées, et tous les autres paramètres sont mis à jour en fonction des stratégies. Mobile Security autorise ou bloque les messages selon l'ordre de priorité suivant : 1. Liste approuvée sur l'agent de dispositif mobile 2. Liste bloquée sur l'agent de dispositif mobile 3. Liste approuvée ou liste bloquée sur le serveur

Remarque

Pour la liste bloquée ou approuvée de filtrage des SMS, le format suivant doit être utilisé : «[nom1:]numéro1;[nom2:]numéro2;...».

La longueur du champ « nom » ne doit pas dépasser 30 caractères, tandis que le numéro de téléphone doit être de 4 à 20 caractères et peut contenir les éléments suivants : 0 à 9, +, -, #, (,) et espaces. Le nombre d'entrées ne doit pas dépasser un maximum de 200.

Stratégies de prévention anti-spam WAP-Push

Cette fonction vous offre un contrôle côté serveur de la protection WAP-Push. Si elle est activée, vous pouvez choisir d'utiliser ou non une liste approuvée de WAP. La liste suivante présente les fonctions disponibles lors de la configuration des stratégies de protection WAP-Push :

- activer ou désactiver la protection WAP-Push pour le dispositif mobile
- configurer le dispositif mobile de manière à utiliser une liste approuvée ou désactiver la protection WAP-Push sur le dispositif mobile
- configurer une liste approuvée à partir de la console d'administration
- si l'administrateur a activé le contrôle côté serveur, l'utilisateur ne sera pas en mesure de modifier le type de protection WAP-Push défini par l'administrateur
- si l'administrateur a désactivé le contrôle côté serveur, et a autorisé les utilisateurs à configurer les paramètres de Mobile Security sur leur dispositif mobile, l'utilisateur ne sera pas en mesure d'afficher ou de modifier la liste de protection WAP-Push configurée par l'administrateur ; mais il pourra modifier la liste personnelle de protection WAP-Push du côté du dispositif mobile

Les paramètres personnels seront effacés après que la stratégie du serveur est remise à un dispositif mobile.

Remarque

Pour la liste approuvée WAP, le format suivant doit être utilisé : «[nom1:]numéro1; [nom2:]numéro2;...».

La longueur du champ « nom » ne doit pas dépasser 30 caractères, tandis que le numéro de téléphone doit être de 4 à 20 caractères et peut contenir les éléments suivants : 0 à 9, +, -, #, (,) et espaces. Le nombre d'entrées ne doit pas dépasser un maximum de 200.

Remarque

Les paramètres personnels de l'utilisateur relatifs aux spams seront effacés après que la stratégie de prévention des spams est appliquée sur les agents de dispositif mobile.

Stratégie de filtrage des appels

Cette fonction vous offre un contrôle côté serveur des stratégies de filtrage des appels. Pour configurer les paramètres de stratégie de filtrage des appels, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie de filtrage**.

Les fonctions suivantes sont disponibles lors de la configuration des stratégies de filtrage des appels :

- activer ou désactiver le filtrage des appels pour le dispositif mobile
- configurer le dispositif mobile de manière à utiliser une liste bloquée ou une liste approuvée
- configurer une liste approuvée à partir de la console d'administration
- configurer une liste bloquée à partir de la console d'administration

Reportez-vous au tableau ci-dessous pour les détails de configuration des listes de filtrage approuvée et bloquée.

TABLEAU 4-3. Configuration de la liste de filtrage de la stratégie de filtrage des appels

CONTRÔLE CENTRAL	CONTRÔLE UTILISATEUR	DESCRIPTION
Désactivé	Activé	L'utilisateur peut modifier la liste approuvée/bloquée sur l'agent de dispositif mobile. Mobile Security autorise ou bloque les URL selon l'ordre de priorité suivant : 1. Liste approuvée sur l'agent de dispositif mobile 2. Liste bloquée sur l'agent de dispositif mobile
Activé	Désactivé	L'utilisateur peut uniquement modifier la liste approuvée/bloquée sur l'agent de dispositif mobile. Mobile Security autorise ou bloque les appels entrants selon l'ordre de priorité suivant : 1. Liste bloquée sur le serveur 2. Liste approuvée sur l'agent de dispositif mobile 3. Liste bloquée sur l'agent de dispositif mobile Vous pouvez également configurer le contrôle côté serveur pour les appels sortants sur les dispositifs mobiles Android.

CONTRÔLE CENTRAL	CONTRÔLE UTILISATEUR	DESCRIPTION
Activé	Activé	L'utilisateur peut afficher ou modifier la liste approuvée/bloquée définie par l'administrateur et peut également utiliser la liste approuvée/bloquée sur l'agent de dispositif mobile. Lorsque les stratégies de sécurité se synchronisent avec l'agent de dispositif mobile, les listes de filtrage ne sont pas synchronisées, et tous les autres paramètres sont mis à jour en fonction des stratégies. Mobile Security autorise ou bloque les appels entrants selon l'ordre de priorité suivant : 1. Liste approuvée sur l'agent de dispositif mobile 2. Liste bloquée sur l'agent de dispositif mobile 3. Liste bloquée sur le serveur Vous pouvez également configurer le contrôle côté serveur pour les appels sortants sur les dispositifs mobiles Android.

Remarque

Pour la liste bloquée ou approuvée de filtrage des appels, le format suivant doit être utilisé : «[nom1:]numéro1;[nom2:]numéro2;...».

La longueur du champ « nom » ne doit pas dépasser 30 caractères, tandis que le numéro de téléphone doit être de 4 à 20 caractères et peut contenir les éléments suivants : 0 à 9, +, -, #, (,) et espaces. Le nombre d'entrées ne doit pas dépasser un maximum de 200.

Stratégie de pare-feu

Le pare-feu Mobile Security protège les dispositifs mobiles sur le réseau grâce à la «stateful inspection», au contrôle du trafic réseau haute performance et au système de détection d'intrusions (IDS). Vous pouvez créer des règles pour filtrer les connexions par adresse IP, numéro de port ou protocole, puis les appliquer aux dispositifs mobiles dans des groupes Mobile Security spécifiques.

Remarque

Trend Micro recommande de désinstaller toute autre application logicielle de pare-feu présente sur les dispositifs mobiles avant de déployer et d'activer le pare-feu Mobile Security. Disposer de plusieurs installations de pare-feu sur le même ordinateur peut engendrer des résultats inattendus.

Pour configurer les paramètres de stratégie de pare-feu, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie de pare-feu**.

Une stratégie de pare-feu comprend les éléments suivants :

- **Stratégie de pare-feu** : Activer/désactiver le pare-feu Mobile Security et le IDS. Une stratégie courante permet également de bloquer ou d'autoriser tout le trafic entrant et/ou sortant sur les dispositifs mobiles
  - **Activer le système de détection d'intrusions (IDS)** : Le pare-feu Mobile Security dispose du Système de détection d'intrusions (IDS) et contribue à empêcher les attaques de type saturation SYN (un type d'attaque de déni de service). Au cours de ces attaques, un programme envoie une succession de paquets de synchronisation TCP (SYN) vers un ordinateur. Le dispositif mobile envoie alors sans cesse des accusés de réception de synchronisation (SYN/ACK). Ce processus peut épuiser les ressources du système et empêcher les dispositifs mobiles de gérer les autres requêtes.
  - **Niveau de sécurité** : Le pare-feu Mobile Security inclut trois niveaux de sécurité prédéfinis qui vous permettent de définir rapidement les stratégies de pare-feu. Ces niveaux de sécurité limitent le trafic réseau en fonction de sa direction.
    - **Faible**—autorise tout le trafic entrant et sortant.
    - **Normal**—autorise tout le trafic sortant, mais bloque tout le trafic entrant.
    - **Élevée**—bloque tout le trafic entrant et sortant.
- **Exception** : Les règles d'exception proposent des paramètres spécifiques supplémentaires pour autoriser ou bloquer différents types de trafic en fonction des adresses IP et des numéros de ports des dispositifs mobiles. Les règles de la liste remplacent la stratégie **Niveau de sécurité**.

Les paramètres des règles d'exception sont les suivants :

- **Action**—bloque ou autorise/journalise le trafic qui répond aux critères des règles.
- **Direction**—trafic réseau entrant ou sortant sur les dispositifs mobiles
- **Protocole**—type de trafic : TCP, UDP, ICMP
- **Port(s)**—ports des dispositifs mobiles sur lesquels les actions sont exercées
- **Adresses IP**—adresses IP des dispositifs réseau pour lesquels les critères de trafic sont appliqués.

Stratégie de protection contre les menaces Internet

Vous permet de gérer la stratégie de protection contre les menaces Internet depuis le serveur Mobile Security et la déploie sur les dispositifs mobiles Android et iOS. Cela permet également aux dispositifs mobiles Android de renvoyer au serveur le journal de protection contre les menaces Internet.

Pour configurer les paramètres de stratégie de protection contre les menaces Internet, cliquez sur **Stratégies**, puis sur le nom de la stratégie, et enfin sur **Stratégie de protection contre les menaces Internet**.

Stratégie de mot de passe et de chiffrement

Le module de chiffrement et de mot de passe fournit des fonctions d'authentification par mot de passe et de chiffrement de données sur les dispositifs mobiles. Ces fonctions empêchent tout accès non autorisé aux données contenues sur les dispositifs mobiles.

Pour configurer les paramètres de stratégie de mot de passe et de chiffrement, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie de mot de passe et de chiffrement** dans le menu de gauche.

Paramètres de sécurité par mot de passe

Lorsque l'agent de dispositif mobile est installé, chaque dispositif mobile est associé à un utilisateur. L'utilisateur doit saisir le mot de passe de mise sous tension approprié pour se

connecter au dispositif mobile. Lorsqu'un utilisateur a oublié le mot de passe de mise sous tension, vous pouvez saisir le mot de passe administrateur afin de déverrouiller un dispositif mobile.

Le tableau suivant décrit les stratégies de mot de passe de mise sous tension que vous pouvez configurer :

OPTION	DESCRIPTION
Type de mot de passe	Les mots de passe doivent contenir des nombres ou des caractères alphanumériques uniquement.
Longueur minimale du mot de passe	Les mots de passe doivent dépasser le nombre de caractères spécifié.
Complexité du mot de passe	Pour les mots de passe alphanumériques, les utilisateurs doivent configurer des mots de passe contenant certains des éléments suivants pour les rendre plus difficiles à deviner : majuscules, minuscules, caractères spéciaux ou chiffres.
Mot de passe initial de l'agent de dispositif mobile	Mot de passe qui permet aux utilisateurs de se connecter à leurs dispositifs Windows Mobile après l'installation de l'agent de dispositif mobile et du module de chiffrement. Par défaut, "123456".
Mot de passe administrateur	Mot de passe utilisé par un administrateur pour déverrouiller un dispositif mobile.
Période d'expiration	Nombre de jours de validité d'un mot de passe de connexion. Une fois le mot de passe expiré, l'utilisateur doit configurer un nouveau mot de passe pour se connecter.
Délai d'inactivité	Nombre de minutes pendant lesquelles l'utilisateur reste inactif avant que le dispositif mobile entre automatiquement en mode sécurisé et affiche l'écran de connexion.

OPTION	DESCRIPTION
Limiter les tentatives de connexion	Limite le nombre de tentatives de connexion pour empêcher les attaques de mot de passe par force brute. Lorsque la limite est atteinte, les actions possibles sont : • **Réinitialisation à chaud**—redémarre le dispositif mobile. • **Accès administrateur uniquement**—nécessite une connexion à l'aide du mot de passe administrateur. • **Réinitialisation à froid**—réinitialise les stratégies par défaut du dispositif mobile. • **Effacer toutes les données**—réinitialise les stratégies par défaut du dispositif mobile et efface toutes les données figurant sur le dispositif mobile et sur la carte mémoire. **AVERTISSEMENT!** Après une action «Effacer toutes les données», les utilisateurs doivent reformater la carte mémoire pour pouvoir la réutiliser pour le stockage de données.
Modification du mot de passe de mise sous tension initiale	Demander aux utilisateurs de modifier le mot de passe après la connexion initiale.
Questions relatives aux mots de passe oubliés	Si un utilisateur a oublié le mot de passe de mise sous tension, cette fonction lui permet de déverrouiller les dispositifs mobiles et de configurer un nouveau mot de passe en répondant à la question sélectionnée.

Remarque

Lorsque vous indiquez les caractères pour le mot de passe initial ou administrateur, tenez compte du mode de saisie utilisé par les dispositifs mobiles. Sinon l'utilisateur risque de ne plus être en mesure de déverrouiller le dispositif après avoir activé le chiffrement.

Paramètres de chiffrement

L'agent de dispositif mobile fournit une fonction de chiffrement de données à la volée afin de sécuriser les données sur les dispositifs mobiles. Deux algorithmes de chiffrement sont disponibles : AES (Advanced Encryption Standard, avec des clés de 128, 192 ou 256 bits), et XTS-Advanced Encryption Standard (AES).

Remarque

Mobile Security gère la stratégie de sécurité des données des dispositifs Windows Mobile uniquement.

Vous pouvez sélectionner les types de fichiers spécifiques à chiffrer sur les dispositifs Windows Mobile, l'algorithme de chiffrement à utiliser, les applications approuvées autorisées à accéder aux données chiffrées, ou appliquer le chiffrement de données aux cartes mémoire insérées dans les dispositifs mobiles.

L'agent de dispositif mobile ne chiffre pas les fichiers Dynamic Link Library (`*.DLL`). L'agent de dispositif mobile ne chiffre que les fichiers qui ont été modifiés par un utilisateur. La lecture d'un fichier et sa fermeture sans modifications ne provoquent pas le chiffrement du fichier.

Une fois que le module de chiffrement est activé, certains types de fichiers et les informations PIM sont chiffrés. Ces types de fichiers et informations PIM sont répertoriés dans le tableau suivant.

INFORMATIONS CHIFFRÉES	TYPES
Types de fichiers	• doc • txt • ppt • pxl • pdf • xls • psw • docx
Informations PIM	• Contacts • Courrier • Tâches • Calendrier • SMS • MMS

Le module de chiffrement ne permet qu'aux applications de confiance d'accéder aux données chiffrées. Par conséquent, vous devez ajouter ces applications à la liste des applications de confiance. Pour ajouter un logiciel à la liste d'applications de confiance, ajoutez le chemin d'accès complet vers la liste adéquate sous : «**Autoriser plus d'applications à accéder aux données chiffrées**».

Remarque

Pour une configuration avancée, vous pouvez paramétrer Mobile Security pour qu'il chiffre d'autres types de fichiers. Pour activer le chiffrement de types de fichiers personnalisés, définissez le paramètre **Enable_Custom_Extension** à `1` dans le fichier `TmOMSM.ini` (situé sous `\Trend Micro\Mobile Security`). Lorsque le paramètre est défini à **"1"** dans le fichier `TmOMSM.ini`, le champ **Chiffrer d'autres types de fichiers** s'affiche sur l'écran **Stratégies de sécurité des données**. Spécifiez les types de fichiers dans ce champ.

Pour désactiver cette fonction, définissez le paramètre **Enable_Custom_Extension** à `0`. Lorsque le paramètre est défini à **"0"** dans le fichier `TmOMSM.ini`, le champ **Chiffrer d'autres types de fichiers** n'est pas disponible sur l'écran **Stratégies de sécurité des données**.

Après avoir effectué la modification dans le fichier `TmOMSM.ini`, redémarrez le service **Service de module de gestion de Mobile Security** afin que la modification prenne effet.

AVERTISSEMENT!

Trend Micro ne recommande pas la personnalisation de types de fichiers pour le chiffrement. Vous ne pouvez pas chiffrer certains types de fichiers (par exemple, `.exe`, `.cert`, `.dll`, etc.). Des erreurs système inattendues sont susceptibles de survenir si vous paramétrez Mobile Security pour chiffrer des types de fichiers qui ne devraient pas l'être.

Stratégie de verrouillage des fonctions

Grâce à cette fonctionnalité, vous pouvez restreindre (désactiver) ou autoriser (activer) l'utilisation de certaines fonctionnalités ou de certains composants des dispositifs mobiles. Par exemple, vous pouvez désactiver l'appareil photo pour tous les dispositifs mobiles d'un groupe en particulier.

Pour configurer les paramètres de stratégie de verrouillage des fonctions, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **stratégie de verrouillage des fonctions** dans le menu de gauche.

Voir *Fonctionnalités des systèmes d'exploitation des dispositifs mobiles pris en charge à la page 1-18* pour la liste des fonctions/composants pris en charge.

Remarque

La stratégie de verrouillage des fonctions n'est PAS disponible pour les dispositifs mobiles Symbian.

AVERTISSEMENT!

Soyez prudent lorsque vous désactivez les options WLAN/WiFi et/ou Microsoft ActiveSync. Il se peut que le dispositif mobile ne puisse plus communiquer avec le serveur si ces deux options ne sont pas disponibles.

Pour les dispositifs mobiles Android, vous pouvez également ajouter des points d'accès afin de contrôler la disponibilité des composants du dispositif dans la plage de ces points d'accès.

Remarque

Il se peut que les dispositifs Windows Mobile nécessitent un redémaarage pour que les modifications prennent effet.

Stratégie de compatibilité

La stratégie de compatibilité vous permet de définir les critères de compatibilité pour les dispositifs mobiles. Si l'un des dispositifs mobiles ne correspond pas aux critères, Mobile Security affiche l'état de non-compatibilité sur l'interface utilisateur du serveur. Mobile Security envoie également un e-mail au dispositif mobile iOS non compatible, alors qu'il affiche une notification sur les dispositifs mobiles Android non compatibles. La vérification de la compatibilité comprend :

- **Débridé**—vérifie si le dispositif mobile est débridé ou non.
- **Non chiffré**—vérifie si le chiffrement est ou non activé sur le dispositif mobile
- **Vérification de la version SE**—vérifie si la version du système d'exploitation correspond ou non aux critères définis.

Pour configurer les paramètres de Stratégie de compatibilité, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie de compatibilité**.

Stratégie de surveillance et de contrôle des applications

Les stratégies de surveillance et de contrôle des applications vous offrent un contrôle côté serveur des applications installées sur les dispositifs mobiles et poussent les applications requises vers les dispositifs mobiles.

Pour configurer les paramètres de stratégie de surveillance et de contrôle des applications, cliquez sur **Stratégies**, puis sur le nom de la stratégie, et enfin sur **Stratégie de surveillance et de contrôle des applications**.

- **Applications requises** : la sélection de cette option pousse toutes les applications que vous ajoutez à la liste vers les dispositifs mobiles. Vous pouvez également lier un VPN à des applications, de sorte que ces applications utilisent toujours ce VPN pour se connecter au réseau.
- **Applications autorisées** : contrôle les applications installées sur les dispositifs mobiles en utilisant des listes d'applications approuvées et bloquées.

  Pour les dispositifs mobiles iOS, Mobile Security envoie une notification à l'administrateur et à l'utilisateur pour toutes les applications qui ne sont pas conformes à la stratégie.

  Pour les dispositifs mobiles Android, Mobile Security bloque l'application qui n'est pas conforme à la stratégie et autorise toutes les autres.

  - **Activer le blocage des applications du système** (Android uniquement) :

    si ce paramètre est sélectionné, Mobile Security bloque toutes les applications du système sur les dispositifs mobiles Android.

  - **Activer la catégorie d'applications** : sélectionnez la catégorie d'applications que vous souhaitez activer ou désactiver sur les dispositifs mobiles. Vous pouvez aussi faire une exception en ajoutant à la liste des applications approuvées ou bloquées les applications qui appartiennent à ces catégories. Par exemple, si vous avez désactivé une catégorie de type Jeux, Mobile Security bloque toutes les applications qui appartiennent à cette catégorie, à moins qu'une telle application figure dans la liste des applications approuvées.

    Mobile Security autorise ou bloque les applications selon l'ordre de priorité suivant :

1. **Liste des applications approuvées** : Mobile Security autorise les applications qui sont sur la liste des applications approuvées, même si elles appartiennent à la catégorie que vous avez désactivée.

2. **Liste des applications bloquées** : Mobile Security bloque les applications qui sont sur la liste des applications bloquées, même si elles appartiennent à la catégorie que vous avez activée.

3. **Autorisations des applications** : Mobile Security autorise ou bloque les applications en fonction de l'état des autorisations que vous avez sélectionné pour la catégorie à laquelle elles appartiennent.

- **Activer les autorisations d'application** (pour Android uniquement) : sélectionnez les services d'applications que vous souhaitez activer ou désactiver sur les dispositifs mobiles Android. Vous pouvez aussi faire une exception en ajoutant les applications qui utilisent ces services à la liste des applications approuvées ou bloquées. Par exemple, si vous avez désactivé un service du type **Lire les données**, Mobile Security bloque toutes les applications qui utilisent le service Lire les données, à moins qu'une telle application figure dans la liste des applications approuvées.

  Mobile Security autorise ou bloque les applications selon l'ordre de priorité suivant :

  1. **Liste des applications approuvées** : Mobile Security autorise les applications qui sont sur la liste des applications approuvées, même si elles utilisent les services que vous avez désactivés.

  2. **Liste des applications bloquées** : Mobile Security bloque les applications qui sont sur la liste des applications bloquées, même si elles utilisent les services que vous avez activés.

  3. **Autorisations des applications** : Mobile Security autorise ou bloque les applications en fonction de l'état des autorisations que vous avez sélectionné pour les services qu'elles utilisent.

- **Autoriser uniquement les applications suivantes** : ajoute à la liste des applications approuvées les applications dont vous souhaitez autoriser l'utilisation par les utilisateurs sur leurs dispositifs mobiles. Si cette fonction est activée :

- Mobile Security affiche un message d'avertissement sur les dispositifs mobiles Android si des applications qui ne sont pas sur la liste des applications approuvées sont détectées.
- Sur les dispositifs mobiles iOS, si Mobile Security détecte une application qui n'est pas dans la liste des applications approuvées, Mobile Security envoie une notification par e-mail à l'utilisateur.

- **Bloquer uniquement les applications suivantes** : ajoute à la liste des applications bloquées les applications que vous ne souhaitez pas que les utilisateurs utilisent sur leurs dispositifs mobiles. Si cette fonction est activée :
  - Mobile Security affiche un message d'avertissement sur les dispositifs mobiles Android si des applications qui sont sur la liste des applications bloquées sont détectées.
  - Sur les dispositifs mobiles iOS, si Mobile Security détecte une application qui est dans la liste des applications bloquées, Mobile Security envoie une notification par e-mail à l'utilisateur.
- **Verrouillage pour application (uniquement pour le mode Surveillé)** : limite le dispositif mobile iOS à l'application spécifiée.

Mobile Security vérifie les applications restreintes et envoie une alerte par e-mail aux utilisateurs :

- automatiquement en fonction des paramètres de **Fréquence de recueil d'informations** sous **Administration** > **Paramètres du serveur de communication** > **Paramètres communs (onglet)**, ou
- lors de la mise à jour des paramètres de **Fréquence de recueil d'informations** sous **Administration** > **Paramètres du serveur de communication** > **Paramètres communs (onglet)**.

Stratégie du programme d'achats en volume

Cette stratégie permet à l'administrateur d'importer les applications iOS qui sont achetées par le biais du programme d'achats en volume d'Apple sur la console Web d'administration Mobile Security. Mobile Security poussera toutes les applications figurant dans la liste du programme d'achats en volume vers les dispositifs mobiles d'un groupe.

Pour configurer la stratégie du programme d'achats en volume :

1. Ajoutez des applications sur la Banque d'applications d'entreprise. Voir *Ajout d'une application à la page 5-2* pour la procédure.
2. Cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, puis sur **Stratégie du programme d'achats en volume**.
3. Cliquez sur **Importer** puis sélectionnez les applications à importer depuis la Banque d'applications d'entreprise.
4. Cliquez sur **Enregistrer** pour pousser toutes les applications vers les dispositifs mobiles iOS.

Chapitre 5

Gestion de la Banque d'applications d'entreprise

Ce chapitre vous explique comment gérer la Banque d'applications d'entreprise sur des dispositifs mobiles iOS et Android.

Le chapitre contient les sections suivantes :

À propos de la Banque d'applications d'entreprise

La banque d'applications d'entreprise vous permet de créer une liste de webclips et d'applications que les utilisateurs peuvent télécharger et installer sur leurs dispositifs mobiles Android ou iOS.

Vous pouvez également télécharger des applications iOS, achetées par l'intermédiaire du programme d'achat en volume d'Apple, sur la banque d'applications d'entreprise de la console Web d'administration de Mobile Security.

Gestion des applications d'entreprise

Ajout d'une application

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Banque d'applications** dans la barre de menu.

   L'écran **Banque d'applications d'entreprise** s'affiche.
3. Cliquez sur l'onglet **Applications iOS** ou sur l'onglet **Applications Android**.
4. Cliquez sur **Ajouter**.

   La fenêtre **Ajouter une application** s'affiche.
5. Vous pouvez désormais ajouter des applications à la liste par l'une des options suivantes :

   - **Ajouter à partir d'un ordinateur local**—sélectionnez un fichier d'installation pour les dispositifs mobiles Android et iOS.
   - **Ajouter un webclip**—saisissez l'URL de l'application et l'icône de l'application apparaîtra sur l'écran d'accueil du dispositif mobile de l'utilisateur, et le lien s'ouvrira dans le navigateur Web par défaut du dispositif mobile.

- (Android) **Ajouter à partir d'une banque d'applications externe**—saisissez le lien de l'application dans une banque d'applications externe. L'icône de l'application apparaîtra sur l'écran d'accueil du dispositif mobile de l'utilisateur, et le lien s'ouvrira dans le navigateur web par défaut sur le dispositif.

- (IOS) **Veuillez entrer une recherche par mot clé**—saisissez le nom de l'application VPP que vous souhaitez rechercher et sélectionnez un pays pour consulter l'application dans son App Store Apple, puis sélectionnez l'application que vous souhaitez ajouter à partir des résultats de recherche. Une fois ajoutée, l'application VPP n'est disponible que dans la **Banque d'applications** sur la console Web d'administration de Mobile Security. Pour pousser l'application vers les dispositifs mobiles, vous aurez besoin d'ajouter l'application à la **Stratégie du programme d'achats en volume**. Voir *Stratégie du programme d'achats en volume à la page 4-30* pour la procédure.

6. Cliquez sur **Continuer**.

   L'écran **Modifier une application** s'affiche.

7. Configurez ce qui suit :

   - **Nom de l'application** : saisissez le nom de l'application.

   - **Icône de l'application** : si l'icône de l'application n'apparaît pas, cliquez sur Télécharger l'icône de l'application pour sélectionner et télécharger l'icône de l'application.

   - **ID de l'application** : si l'ID de l'application n'apparaît pas, saisissez l'ID de l'application.

   - **Fichier des codes VPP** : Pour un application VPP iOS, téléchargez les fichiers de codes d'achats en volume qu'Apple vous a envoyés.

   - **Catégorie** : Sélectionnez une catégorie pour l'application.

     Remarque

     Vous devez sélectionner une catégorie dans la liste déroulante. Pour ajouter ou supprimer une catégorie, cliquez sur le bouton **Catégorie**.

   - **Description** : saisissez la description de l'application.

- **Publier** : sélectionnez une des options suivantes :
  - **Ne pas publier** —pour télécharger l'application sur le serveur, mais la cacher aux dispositifs mobiles.
  - **Publier en tant que version de production**—pour télécharger l'application sur le serveur, et la publier pour que les dispositifs mobiles la téléchargent.
  - **Publier en tant que version beta**—pour télécharger l'application sur le serveur, et la publier comme version beta pour que les dispositifs mobiles la téléchargent.
- **Captures d'écran** : sélectionnez et téléchargez des captures d'écran d'applications.

8. Cliquez sur **Continuer**.

   L'application apparaît dans la liste des applications.

Modification des informations des applications

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Banque d'applications** dans la barre de menu.

   L'écran **Banque d'applications d'entreprise** s'affiche.
3. Cliquez sur l'onglet **Applications iOS** ou sur l'onglet **Applications Android**.
4. Cliquez sur le nom de l'application dont vous souhaitez modifier les informations.

   La fenêtre **Modifier application** s'affiche.
5. Modifier les détails sur l'écran.
6. Cliquez sur **Continuer**.

Suppression d'applications de la Banque d'applications

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Banque d'applications** dans la barre de menu.

   L'écran **Banque d'applications d'entreprise** s'affiche.
3. Cliquez sur l'onglet **Applications iOS** ou sur l'onglet **Applications Android**.
4. Sélectionnez les applications à supprimer.
5. Cliquez sur **Supprimer**, puis cliquez sur **OK** sur la boite de dialogue de confirmation.

Gestion des catégories d'applications

Ajout d'une catégorie d'application

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Banque d'applications** dans la barre de menu.

   L'écran **Banque d'applications d'entreprise** s'affiche.
3. Cliquez sur l'onglet **Applications iOS** ou sur l'onglet **Applications Android**.
4. Cliquez sur **Gérer catégorie**.
5. Cliquez sur **Ajouter**.

   La fenêtre **Ajouter catégorie** s'affiche.

6. Tapez le nom de la catégorie et la description, puis cliquez sur **Enregistrer**.

Modification d'une catégorie d'application

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Banque d'applications** dans la barre de menu.

   L'écran **Banque d'applications d'entreprise** s'affiche.
3. Cliquez sur l'onglet **Applications iOS** ou sur l'onglet **Applications Android**.
4. Cliquez sur **Gérer catégorie**.
5. Cliquez sur le nom de la catégorie que vous souhaitez modifier.

   La fenêtre **Modifier catégorie** s'affiche.
6. Modifiez les détails de la catégorie et puis cliquez sur **Enregistrer**.

Suppression d'une catégorie d'application

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Banque d'applications** dans la barre de menu.

   L'écran **Banque d'applications d'entreprise** s'affiche.
3. Cliquez sur l'onglet **Applications iOS** ou sur l'onglet **Applications Android**.
4. Cliquez sur **Gérer catégorie**.
5. Sélectionnez les catégories que vous souhaitez supprimer, cliquez sur **supprimer**, puis cliquez sur **OK** sur la boîte de dialogue de confirmation.

Chapitre 6

Mise à jour des composants

Ce chapitre décrit comment configurer des mises à jour manuelles et programmées du serveur, puis comment indiquer la source de mise à jour pour ActiveUpdate. Vous apprendrez également à effectuer des mises à jour de composants sur des agents de dispositif mobile déterminés.

Le chapitre contient les sections suivantes :

À propos des mises à jour de composants

Dans Mobile Security, les composants ou fichiers suivants sont mis à jour via ActiveUpdate, la fonction Internet de mise à jour des composants de Trend Micro :

- Serveur Mobile Security—Package d'installation de programme pour le serveur Mobile Security.
- Signatures de programmes malveillants—fichier contenant des milliers de signatures de virus/programmes malveillants et déterminant la capacité de Mobile Security à détecter ces types de fichiers. Trend Micro met régulièrement à jour les fichiers de signatures pour assurer la protection contre les toutes dernières menaces.
- Moteur de scan anti-programmes malveillants—composant qui effectue les fonctions réelles d'analyse et de nettoyage. Le moteur de scan utilise une technologie de correspondance de signatures, qui fait appel au fichier de signatures pour détecter les programmes malveillants. Trend Micro publie de temps à autre un nouveau moteur de scan qui intègre les technologies les plus récentes.
- Programme d'installation des agents de dispositif mobile—pack d'installation de programme pour les agents de dispositif mobile.
- Correctif du programme de l'agent de dispositif mobile—fichier correctif de programme qui inclut les dernières mises à jour de l'agent de dispositif mobile installé sur les dispositifs mobiles.

Mise à jour des composants de Mobile Security

Vous pouvez configurer des mises à jour manuelles ou programmées de composants sur le serveur de Mobile Security afin d'obtenir les fichiers de composants les plus à jour à partir du serveur ActiveUpdate. Lorsqu'une version plus récente d'un composant est téléchargée sur le serveur de Mobile Security, ce dernier avertit automatiquement les dispositifs mobiles de la disponibilité de mises à jour de composants.

Mise à jour manuelle

Vous pouvez effectuer une mise à jour manuelle du serveur et de l'agent de dispositif mobile dans l'onglet **Manuelle**sur l'écran**Mises à jour**. Pour cela, vous devez avoir configuré la source de téléchargement dans l'écran **Source** (voir*Indication d'une source de téléchargement à la page 6-6* pour plus d'informations).

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Mises à jour**.

   L'écran **Mises à jour** s'affiche.
3. Cliquez sur l'onglet **Manuelles**.

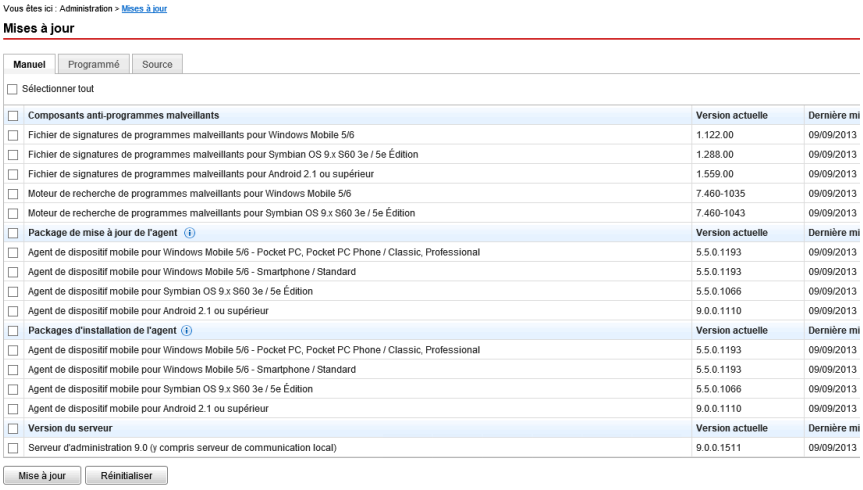

FIGURE 6-1. L'onglet Manuelles sur l'écran Mises à jour

4. Sélectionnez la case à cocher du composant à mettre à jour. Sélectionnez les cases à cocher **Composants anti-programmes malveillants**, **Programme** et/ou **Pack d'installation du programme** pour sélectionner tous les composants de ce groupe. Cet écran affiche également la version actuelle de chaque composant et

l'heure à laquelle il a été mis à jour pour la dernière fois. Voir *À propos des mises à jour de composants à la page 6-2* pour plus d'informations sur chaque composant de mise à jour.

5. Cliquez sur **Mise à jour** pour démarrer le processus de mise à jour du ou des composants.

Mise à jour programmée

Les mises à jour programmées vous permettent d'effectuer des mises à jour régulières sans intervention de l'utilisateur, et réduisent donc votre charge de travail. Pour cela, vous devez avoir configuré la source de téléchargement dans l'écran **Source** (consultez *Indication d'une source de téléchargement à la page 6-6* pour plus d'informations).

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Mises à jour**.

   L'écran **Mises à jour** s'affiche.
3. Cliquez sur l'onglet **Programmées**.

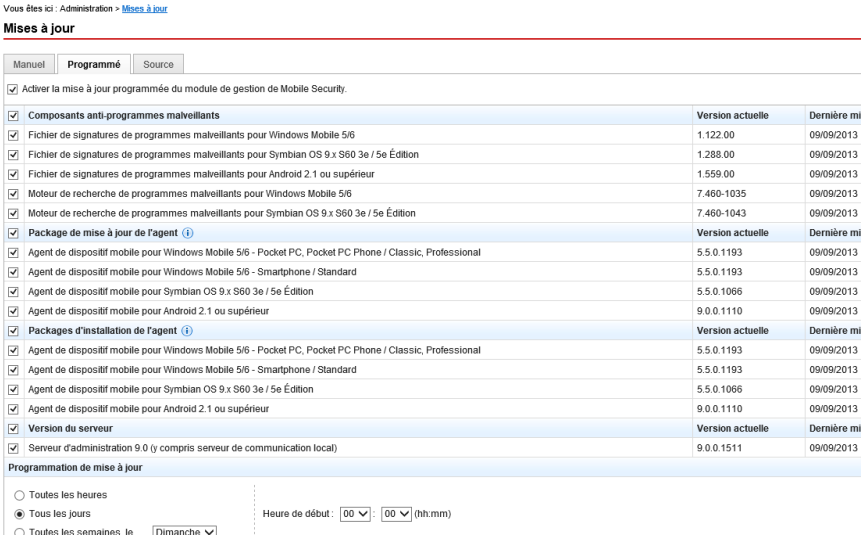

FIGURE 6-2. L'onglet Programmées sur l'écran Mises à jour

4. Sélectionnez la case à cocher du composant à mettre à jour. Sélectionnez les cases à cocher **Composants anti-programmes malveillants**, **Packages de mise à jour de l'agent**, **Packages d'installation de l'agent** et/ou **Version du serveur** pour sélectionner tous les composants de ce groupe. Cet écran affiche également la version actuelle de chaque composant et l'heure à laquelle il a été mis à jour pour la dernière fois.

5. Sous **Programmation de mise à jour**, configurez l'intervalle de temps pour la mise à jour du serveur. Les options sont **Toutes les heures**, **Tous les jours**, **Toutes les semaines** et **Tous les mois**.

   - Pour les programmations hebdomadaires, indiquez le jour de la semaine (par exemple, dimanche, lundi, etc.)
   - Pour les programmations mensuelles, indiquez le jour du mois (par exemple, le premier jour, ou 01, du mois, etc.).

Remarque

La fonction **Mettre à jour pour une période de x heures** est disponible pour les options `Tous les jours`, `Toutes les semaines`et `Tous les mois`. Cela signifie que votre mise à jour aura lieu à un moment donné au cours du nombre x d'heures indiqué, après l'heure sélectionnée dans le champ **Heure de début**. Cette fonction aide à équilibrer la charge sur le serveur ActiveUpdate.

- Sélectionnez l'**Heure de début** lorsque vous souhaitez que Mobile Security lance le processus de mise à jour.

6. Pour **enregistrer** les paramètres, cliquez sur Enregistrer.

Indication d'une source de téléchargement

Vous pouvez configurer Mobile Security pour qu'il utilise la source ActiveUpdate par défaut ou une source de téléchargement précise pour les mises à jour du serveur.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Administration** > **Mises à jour**.

   L'écran **Mises à jour** s'affiche. Pour obtenir de plus amples informations sur les mises à jour, consultez *Mise à jour manuelle à la page 6-3* ou pour la mise à jour programmée, consultez *Mise à jour programmée à la page 6-4*.
3. Cliquez sur l'onglet **Source**.

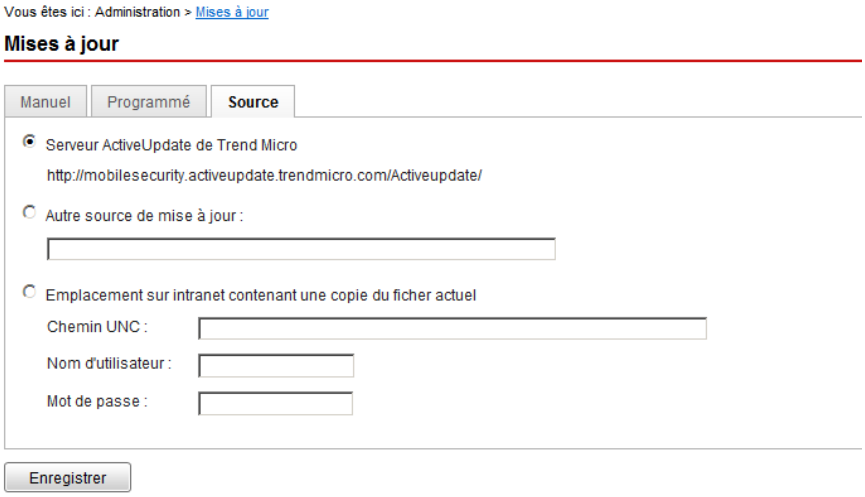

FIGURE 6-3. L'onglet Source sur l'écran Mises à jour

4. Sélectionnez l'une des sources de téléchargement suivantes:

   - **Serveur ActiveUpdate de Trend Micro**—source de mise à jour par défaut.
   - **Autre source de mise à jour**—indiquez le site Web HTTP ou HTTPS (par exemple, votre site Web intranet local), ainsi que le numéro de port à utiliser à partir de l'emplacement où les agents de dispositifs mobiles peuvent télécharger les mises à jour.

     Remarque

     Les composants mis à jour doivent être disponibles sur la source de mise à jour (serveur Web). Fournissez le nom d'hôte ou l'adresse IP, ainsi que le répertoire (par exemple, `https://12.1.123.123:14943/source`).

   - **Emplacement Intranet contenant une copie du fichier actuel**—la source de mise à jour intranet locale. Spécifiez ce qui suit :
     - **Chemin d'accès UNC** : tapez le chemin d'accès de l'emplacement du fichier source.

- **Nom d'utilisateur** et **Mot de passe** : tapez le nom d'utilisateur et mot de passe si l'emplacement de la source requiert une authentification.

Mise à jour manuelle d'un serveur AutoUpdate local

Si le serveur/dispositif est mis à jour via un serveur AutoUpdate local mais si le serveur d'administration de Mobile Security ne peut pas se connecter à Internet, le serveur AutoUpdate local doit être mis à jour manuellement avant la mise à jour du serveur/dispositif.

Procédure

1. Demandez le pack d'installation à votre représentant Trend Micro.
2. Extrayez le pack d'installation.
3. Copiez les dossiers sur le serveur AutoUpdate local.

Remarque

Lorsque vous utilisez un serveur AutoUpdate local, vérifiez les mises à jour disponibles régulièrement.

Chapitre 7

Affichage et maintenance des journaux

Ce chapitre décrit comment afficher les journaux des agents de dispositifs mobiles sur la console Web d'administration de Mobile Security, et comment configurer les paramètres de suppression des journaux.

Le chapitre contient les sections suivantes :

À propos des journaux des agents de dispositif mobile

Lorsque les agents de dispositif mobile génèrent un journal de protection contre les programmes malveillants, de protection contre les menaces Internet, de pare-feu, de chiffrement, d'événements ou de violation de stratégie, ce journal est envoyé au serveur Mobile Security. Ainsi, les journaux des agents de dispositifs mobiles sont stockés dans un emplacement central afin que vous puissiez évaluer les stratégies de protection de votre organisation et identifier les dispositifs mobiles soumis à un niveau de risque d'infection ou d'attaque plus élevé.

Remarque

Vous pouvez visualiser les journaux de protection WAP Push, anti-spam SMS et de filtrage des appels sur les dispositifs mobiles.

Affichage des journaux des agents de dispositif mobile

Vous pouvez afficher les journaux des agents de dispositif mobile sur les dispositifs mobiles eux-mêmes ou afficher tous les journaux des agents de dispositif mobile sur le serveur de Mobile Security. Sur le serveur Mobile Security, vous pouvez afficher les journaux suivants de l'agent de dispositif mobile :

- Journal de protection contre les programmes malveillants—l'agent de dispositif mobile génère un journal lorsqu'un programme malveillant est détecté sur le dispositif mobile. Ces journaux vous permettent d'assurer le suivi des programmes malveillants qui ont été détectés et des mesures qui ont été prises pour vous en débarrasser.
- Journal de protection contre les menaces Internet—l'agent Mobile Security génère un journal lorsqu'il bloque une page Internet dangereuse ou infectée par des programmes malveillants, puis il télécharge le journal sur le serveur.

- Journal de pare-feu—ces journaux sont générés lorsqu'une règle de pare-feu est appliquée ou lorsque la fonction de pare-feu (telle que le niveau de sécurité prédéfini ou IDS) bloque une connexion.
- Journal de chiffrement—contient des informations telles que les tentatives de connexion réussies de l'utilisateur et les actions prises une fois le nombre maximal de tentatives de connexion atteint.
- Journal d'événements—ces journaux sont générés lorsque certaines actions sont entreprises par le serveur et par l'agent de dispositif mobile.
- Journal de violation de stratégies—ces journaux contiennent des informations relatives à l'état de conformité de la stratégie des agents de dispositif mobile.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Notifications et rapports** > **Requête de journaux**.

   L'écran **Requête de journaux** s'affiche.

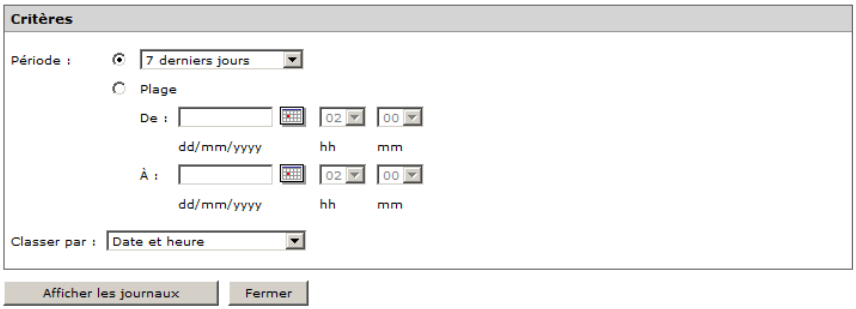

FIGURE 7-1. Écran Requête de journaux

3. Indiquez les critères des journaux que vous souhaitez afficher. Les paramètres sont les suivants :
   - **Types de journal**—sélectionnez le type de journal dans le menu déroulant.
   - **Catégorie**—sélectionnez la catégorie dans le menu déroulant.

- **Nom de l'administrateur**—saisissez le nom de l'administrateur dont vous souhaitez rechercher les journaux générés.
- **Période**—sélectionnez une plage de dates prédéfinie. Les options sont : **Tout**, **24 dernières heures**, **7 derniers jours**, et **30 derniers jours**. Si la période que vous demandez n'est pas couverte par les options ci-dessus, sélectionnez **Plage**, puis spécifiez une plage.
  - **De**—saisissez la date du premier journal que vous souhaitez afficher. Cliquez sur l'icône pour sélectionner une date dans le calendrier.
  - **À**—saisissez la date du dernier journal que vous souhaitez afficher. Cliquez sur l'icône pour sélectionner une date dans le calendrier.
- **Classer par**—indiquez l'ordre et le regroupement des journaux.

4. Cliquez sur **Requête** pour commencer la requête.

Maintenance des journaux

Lorsque les agents de dispositif mobile génèrent des journaux d'événements sur la détection de risques de sécurité, ils sont envoyés et stockés dans le module de gestion de Mobile Security. Utilisez ces journaux pour évaluer les stratégies de protection de votre organisation et identifier les dispositifs mobiles représentant un niveau de risque d'infection ou d'attaque plus élevé.

Pour que les journaux des agents de dispositifs mobiles n'occupent pas trop d'espace sur votre disque dur, supprimez-les manuellement ou configurez la console Web d'administration de Mobile Security pour qu'elle les supprime automatiquement de façon programmée définie dans l'écran Maintenance des journaux.

Planification de suppression de journaux

Procédure

1. Connectez-vous à la console d'administration Mobile Security.

2. Cliquez sur **Notifications et rapports** > **Maintenance des journaux**.

   L'écran **Maintenance des journaux** s'affiche.

3. Sélectionnez **Activer la suppression programmée des journaux**.

4. Sélectionnez les types de journaux à supprimer : Programmes malveillants, pare-feu, chiffrement, événements ou violation de stratégie.

5. Indiquez si la suppression concerne tous les types de journaux sélectionnés ou ceux antérieurs au nombre de jours indiqué.

6. Indiquez la fréquence et l'heure de suppression des journaux.

7. Cliquez sur **Enregistrer**.

Suppression manuelle des journaux

Procédure

1. Connectez-vous à la console d'administration Mobile Security.

2. Cliquez sur **Notifications et rapports** > **Maintenance des journaux**.

   L'écran **Maintenance des journaux** s'affiche.

3. Sélectionnez les types de journaux à supprimer.

4. Indiquez si la suppression concerne tous les types de journaux sélectionnés ou seulement les journaux antérieurs au nombre de jours indiqué.

5. Cliquez sur **Supprimer maintenant**.

Chapitre 8

Utilisation des notifications et rapports

Ce chapitre décrit comment configurer et utiliser les notifications et rapports dans Mobile Security.

Le chapitre contient les sections suivantes :

À propos des messages de notification et des rapports

Vous pouvez configurer Mobile Security pour envoyer des notifications par courriel ou SMS aux administrateurs et/ou aux utilisateurs.

- **Notifications/rapports administrateur**—envoie des notifications et rapports par courriel à l'administrateur en cas d'anomalie du système.
- **Notifications utilisateur**—envoie un courriel et/ou un SMS pour signaler aux dispositifs mobiles de télécharger et d'installer l'agent de dispositif mobile.

Configuration des paramètres de notification

Configuration des notifications par courriel

Si vous souhaitez envoyer des courriels de notification aux utilisateurs, vous devez configurer ces paramètres.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Notifications et Rapports** > **Paramètres**.

   L'écran **Paramètres de Notifications/Rapports** s'affiche.
3. Sous la section **Paramètres de courriel**, entrez l'adresse électronique de l'**expéditeur**, l'adresse IP du serveur SMTP et son numéro de port.
4. Si le serveur SMTP nécessite une **authentification**, sélectionnez Authentification, puis entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur **Enregistrer**.

Information associée

↳ *Configuration de la liste d'expéditeurs de SMS*

Configuration des paramètres de l'expéditeur de SMS

Le serveur d'administration contrôle et surveille les expéditeurs de SMS connectés au serveur. Les expéditeurs de SMS envoient des messages aux dispositifs mobiles pour effectuer l'installation, l'enregistrement de l'agent de dispositif mobile, la mise à jour de composant, le paramétrage de la stratégie de sécurité et l'effacement, le verrouillage ou la localisation à distance .

Utilisez les paramètres de l'expéditeur de SMS pour :

- configurer les numéros de téléphone de l'expéditeur de SMS
- afficher l'état de la connexion de l'expéditeur de SMS
- configurer le message d'installation de l'agent de dispositif mobile
- configurer la notification de déconnexion de l'expéditeur de SMS

Liste d'expéditeurs de SMS

Il est nécessaire de configurer les numéros de téléphone des dispositifs des expéditeurs de SMS avant que le serveur d'administration ne puisse indiquer aux expéditeurs de SMS d'envoyer les messages vers les dispositifs mobiles.

Remarque

Si vous ne configurez pas le numéro de téléphone d'un expéditeur de SMS dans la liste des expéditeurs de SMS, le serveur d'administration empêche l'expéditeur de SMS d'envoyer des messages aux dispositifs mobiles.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Notifications et Rapports** > **Paramètres**.

L'écran **Paramètres de Notifications/Rapports** s'affiche. Dans la section **Paramètres des expéditeurs de SMS**, la liste des numéros de téléphone et l'état de la connexion des expéditeurs de SMS s'affichent. Si l'expéditeur de SMS se connecte au serveur d'administration avec succès, le champ **État** indique : **Connecté**.

Remarque

Après trois (3) tentatives infructueuses d'envoi d'un SMS, le dispositif mobile affichera "déconnecté".

Configuration de la liste d'expéditeurs de SMS

Indiquez le numéro de téléphone d'un expéditeur de SMS pour autoriser le serveur de Mobile Security à gérer les expéditeurs de SMS. Les expéditeurs de SMS envoient des messages pour avertir les dispositifs mobiles qu'ils doivent effectuer les tâches suivantes :

- télécharger et installer l'agent de dispositif mobile
- s'enregistrer dans le module de gestion de Mobile Security
- annuler l'enregistrement au module de gestion de Mobile Security
- mettre à jour les composants de l'agent de dispositif mobile
- synchroniser les paramètres de stratégies de sécurité avec le module de gestion de Mobile Security
- supprimer à distance les données du dispositif mobile
- verrouiller à distance le dispositif mobile
- localiser à distance le dispositif mobile

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Notifications et Rapports** > **Paramètres**.

   L'écran **Paramètres de Notifications/Rapports** s'affiche.

3. Dans la section **Paramètres des expéditeurs de SMS**, cliquez sur **Ajouter**, saisissez le numéro de téléphone d'un expéditeur de SMS puis cliquez sur **Enregistrer**. L'expéditeur de SMS apparaît dans la liste.

4. Vérifiez que le champ **État** affiche **"Connecté"** pour le numéro que vous avez configuré. Si le champ **État** affiche **"Déconnecté"**, assurez-vous que le dispositif de l'expéditeur de SMS est connecté au serveur d'administration.

Remarque

Les expéditeurs de SMS existants peuvent être modifiés en cliquant sur le numéro de téléphone.

Surveillance des expéditeurs de SMS

Mobile Security peut surveiller l'état des expéditeurs de SMS et envoyer des notifications par courriel si l'un des expéditeurs de SMS est déconnecté pendant plus de dix minutes. Le dispositif de l'expéditeur de SMS affiche également l'état de connexion : Agent interrompu, Agent en cours d'exécution, Agent non utilisé, ou Agent déconnecté. Voir *Notifications et Rapports administrateur programmés à la page 8-8* pour des détails de configurations.

Modification d'un expéditeur de SMS

Procédure

1. Connectez-vous à la console d'administration Mobile Security.

2. Cliquez sur **Notifications et Rapports** > **Paramètres**.

   L'écran **Paramètres de Notifications/Rapports** s'affiche.

3. Dans la section **Paramètres de l'expéditeur de SMS**, cliquez sur le numéro de téléphone que vous souhaitez modifier.

   Une boîte de dialogue s'affiche.

4. Modifiez le numéro de téléphone dans le champ fourni, puis cliquez sur **Enregistrer**.

5. Cliquez sur **Enregistrer** pour enregistrer les paramètres.

Suppression d'un expéditeur de SMS

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Notifications et Rapports** > **Paramètres**.

   L'écran **Paramètres de Notifications/Rapports** s'affiche.
3. Dans la section **Paramètres expéditeur de SMS**, sélectionnez l'expéditeur de SMS que vous souhaitez supprimer et cliquez sur **Supprimer**.
4. Cliquez sur **Enregistrer** pour enregistrer les paramètres.

Gestion de l'application client Expéditeur de SMS

Configuration de l'application client Expéditeur de SMS

Procédure

1. Ouvrez le l'application Expéditeur de SMS sur le dispositif mobile Android.
2. Cliquez sur **Paramètres**, puis saisissez ce qui suit pour pour configurer :
   - **Adresse du serveur** : tapez le nom du serveur d'administration ou l'adresse IP et cliquez sur **OK**.
   - **Port du serveur** : tapez le numéro de port de la console Web d'administration, puis cliquez sur **OK**.
   - **Numéro de téléphone** : saisissez le numéro de téléphone pour l'expéditeur de SMS.
   - **Type de protocole** : sélectionnez le protocole HTTP ou HTTPS pour envoyer des messages.

3. Cliquez sur **Démarrer** pour lancer l'expéditeur de SMS.

Arrêt de l'expéditeur de SMS

Procédure

1. Ouvrez le l'application Expéditeur de SMS sur le dispositif mobile Android.
2. Cliquez sur **Arrêter** pour arrêter l'expéditeur de SMS.

État des expéditeurs de SMS

Mobile Security met à jour l'état de l'expéditeur de SMS sur le dispositif mobile. En fonction de l'état de connexion, les états suivants apparaîtront sur le dispositif :

- Normal : L'expéditeur de SMS est connecté au serveur d'administration.
- Arrêté : L'expéditeur de SMS est arrêté.
- Non utilisé : les paramètres de l'application Expéditeur de SMS ne correspondent pas aux paramètres du serveur Mobile Security.

Affichage de l'historique de l'expéditeur de SMS

Procédure

1. Ouvrez l'application Expéditeur de SMS sur le dispositif mobile Android.
2. Cliquez sur **Historique** pour afficher les messages qui sont envoyés aux dispositifs mobiles.

Affichage des journaux d'expéditeurs de SMS en cours

Procédure

1. Lancez l'application Expéditeur de SMS sur le dispositif mobile Android.
2. Cliquez sur **Journaux en cours** pour afficher les journaux d'évènements d'expéditeurs de SMS en cours.

Notifications et Rapports administrateur programmés

Utilisez l'écran **Notifications/Rapports administrateur** pour configurer les éléments suivants :

- Notifications :
  - **Erreur système**—envoie une notification par courriel à l'administrateur en cas d'anomalie du système. Les variables jetons `<%PROBLEM%>`, `<%REASON%>` et `<%SUGGESTION%>` seront remplacées par le problème, la raison et la suggestion réels en vue de résoudre le problème.
  - **Administrateur de dispositif désactivé pour Mobile Security**—envoie une notification par courriel à l'administrateur lorsque Mobile Security est désactivé dans la liste des **Administrateurs de dispositif** pour n'importe quel dispositif mobile Android. La variable jeton `<%DEVICE%>` sera remplacée par le nom du dispositif mobile dans le courriel.
  - **Avertissement d'expiration du Certificat APNs**—Envoie une notification par courriel à l'administrateur lorsque le certificat APNs expire.
- Rapports :
  - **Rapport d'inventaire de dispositifs**—il s'agit du rapport complet de tous les dispositifs mobiles gérés par Mobile Security.

- **Rapport de violation de compatibilité**—il s'agit du rapport de tous les dispositifs mobiles gérés par Mobile Security qui ne sont pas compatibles avec la stratégie configurée.
- **Rapport de détection de programmes malveillants**—il s'agit du rapport de toutes les menaces de sécurité détectées sur les dispositifs mobiles par Mobile Security.
- **Rapport de protection contre les menaces Internet**—il s'agit du rapport, géré par Mobile Security, de toutes les URL non sécurisées qui ont été visitées à partir des dispositifs mobiles.
- **Rapport de l'inventaire d'application**—il s'agit du rapport de toutes les applications installées sur les dispositifs mobiles gérés par Mobile Security.
- **Rapport d'inscription de dispositifs**—il s'agit du rapport des informations d'inscription des dispositifs mobiles gérés par Mobile Security.
- **Rapport de déclassement de dispositifs**—il s'agit du rapport des informations de déclassement des dispositifs mobiles gérés par Mobile Security.
- **Rapport de violation de stratégie**—il s'agit du rapport des dispositifs mobiles qui violent les stratégies de sécurité.

Configuration des notifications administrateur

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Notifications et Rapports** > **Paramètres**.

   L'écran **Paramètres de Notifications/Rapports** s'affiche.
3. Sélectionnez les notifications et les rapports que vous souhaitez recevoir par courriel puis cliquez sur les notifications et les rapports individuels pour modifier leurs contenus.

Remarque

Lorsque vous sélectionnez des rapports que vous souhaitez recevoir, vous pouvez également ajuster leur fréquence individuellement depuis la liste déroulante après chaque rapport.

Remarque

Lorsque vous modifiez le champ **Message** des messages de notification par courriel, assurez-vous d'inclure les variables jetons `<%PROBLEM%>`, `<%REASON%>` et `<%SUGGESTION%>`, qui seront remplacées par les valeurs réelles dans le courriel.

4. Cliquez sur **Enregistrer** quand vous avez terminé, afin de retourner à l'écran **Notifications/rapports administrateur**.

Notification utilisateur

Utilisez l'écran **Notifications utilisateur** pour configurer la notification par courriel et/ou par SMS suivante :

- **Inscription de dispositif mobile**—envoie un courriel et/ou un SMS pour signaler aux dispositifs mobiles de télécharger et d'installer l'agent de dispositif mobile. La variable jeton `<%DOWNLOADURL%>` sera remplacée par l'URL réelle du package d'installation.
- **Violation de la stratégie**—envoie une notification par courriel aux dispositifs mobiles si les critères de compatibilité ne sont pas respectés. Les variables jetons `<%DEVICE%>` et `<%VIOLATION%>` seront remplacées par le nom du dispositif mobile dans le courriel, et les stratégies qu'il viole.

Configuration des notifications utilisateur

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Notifications et Rapports** > **Paramètres**.

L'écran **Paramètres de notifications/rapports** s'affiche.

3. Sélectionnez les notifications que vous souhaitez envoyer à l'utilisateur par courriel ou par SMS, puis cliquez sur des notifications particulières pour modifier leur contenu.

   - Pour configurer les courriels de notification, il faut mettre à jour les détails suivants comme demandé :

     - **Sujet** : Le sujet du courriel.
     - **Message** : Le corps du courriel.

     Remarque

     En modifiant le champ **Message**, assurez-vous d'inclure les variables jetons < `%DOWNLOADURL%>` ou `<%DEVICE_NAME%>` et `<%VIOLATION%>`, qui seront remplacées par les véritables URL dans le courriel.

   - Pour configurer les SMS de notification, il faut mettre à jour le corps du message dans le champ **Message**.

     Remarque

     En modifiant le champ **Message**, assurez-vous d'inclure la variable jeton < `%DOWNLOADURL%>`, qui sera remplacée par la véritable URL dans le SMS.

4. Cliquez sur **Enregistrer** quand vous avez terminé, afin de retourner à l'écran **Notifications utilisateur**.

Chapitre 9

Dépannage et contact de l'assistance technique

Ce chapitre propose des réponses aux questions fréquemment posées et indique comment obtenir des informations supplémentaires sur Mobile Security.

Le chapitre contient les sections suivantes :

Dépannage

Cette section fournit des conseils pour traiter les problèmes rencontrés lors de l'utilisation de Mobile Security.

- **L'utilisateur ne peut pas saisir de mot de passe nanométrique sur ses dispositifs mobiles.**

  Le clavier des dispositifs mobiles ne peut prendre en charge qu'un certain jeu de caractères. Mobile Security recommande à l'administrateur de compiler la liste des caractères pris en charge par les dispositifs. Après avoir compilé la liste des caractères pris en charge, l'administrateur peut alors définir le mot de passe de protection contre les désinstallations de la console d'administration à l'aide de la liste des caractères pris en charge.

- **L'agent du dispositif mobile ne reçoit pas la notification SMS du serveur ou ne peut pas se connecter au serveur via le nom DNS public.**

  La version de l'agent du dispositif mobile prenant en charge un nom DNS doit être supérieure à 5.0.0.1099 pour la plate-forme Windows Mobile et supérieure à 5.0.0.1061 pour la plate-forme Symbian OS 9.x S60 3e Édition. Les versions précédentes peuvent seulement se connecter via l'adresse IP.

- **Une ou plusieurs applications ne fonctionnent pas après l'activation du module de chiffrement.**

  Lorsqu'un utilisateur utilise le module de chiffrement sur un dispositif, il est possible que certaines applications existantes ne fonctionnent pas. Ceci s'explique par le fait que ces applications existantes n'apparaissent pas dans la liste de confiance. Après l'activation du module de chiffrement, certains types de fichiers seront chiffrés (par exemple, `doc`, `txt`, `ppt`, `pdf`, `xls`, etc.). Le module de chiffrement autorise les seules applications de confiance à accéder aux données chiffrées. L'administrateur doit donc ajouter ces applications à la liste des applications de confiance. Pour obtenir de plus amples informations, voir la section *Paramètres de chiffrement à la page 4-24*.

- **Après l'annulation du processus de désinstallation du serveur de communication, le serveur de communication ne fonctionne pas normalement.**

Si la procédure de désinstallation a commencé à effacer les fichiers et les services qui sont nécessaires au bon fonctionnement du serveur de communication avant l'interruption de la procédure, le serveur de communication ne peut pas fonctionner normalement. Pour résoudre ce problème, installez et configurez à nouveau le serveur de communication.

- **Les dispositifs mobiles iOS ne parviennent pas à s'inscrire sur le serveur d'administration, et affichent le message d'erreur «URL non prise en charge».**

  Ce problème peut survenir si l'horloge système du serveur SCEP est réglée sur une heure incorrecte ou si le certificat SCEP (Extension du protocole d'inscription du certificat simple) n'est pas obtenue par Trend Micro Mobile Security. Assurez-vous que l'heure de l'horloge système du serveur SCEP est correcte. Si le problème persiste, suivez cete procédure :

  1. Connectez-vous à la console d'administration Mobile Security.
  2. Cliquez sur **Administration** > **Serveur de communication** Paramètres.
  3. Sans modifier les paramètres, cliquez sur **Enregistrer**.

- **Le serveur d'administration ne peut pas recevoir de stratégie de BlackBerry Enterprise Server (BES).**

  Le serveur de communication ne peut pas recevoir de stratégie de BlackBerry Enterprise Server (BES) si le nom de la stratégie contient des caractères spéciaux. Vérifiez si le nom de la stratégie contient des caractères spéciaux et remplacez-les par des lettres de l'alphabet et des chiffres.

- **Impossible d'enregistrer les paramètres de la base de données si vous utilisez SQL Server Express.**

  Si vous utilisez SQL Server Express, utilisez le format suivant dans le champ de l'adresse du serveur : `<SQL Server Express IP address>\sqlexpress`.

  

  Remarque

  Remplacez `<SQL Server Express IP address>` par l'adresse IP de SQL Server Express.

- **Impossible de se connecter à SQL Server 2005 ou SQL Server 2005 Express.**

Ce problème peut survenir lorsque SQL Server 2005 n'est pas configuré pour accepter des connexions à distance. Par défaut, SQL Server 2005 Express Edition et SQL Server 2005 Developer Edition n'autorisent pas les connexions à distance. Pour configurer SQL Server 2005 de sorte qu'il autorise les connexions à distance, suivez cette procédure :

1. Activez les connexions à distance sur l'instance du serveur SQL à laquelle vous souhaitez vous connecter depuis un ordinateur à distance.
2. Activez le service SQL Server Browser.
3. Configurez le pare-feu de manière à autoriser le trafic réseau relié au serveur SQL et au service SQL Server Browser.

- **Impossible de se connecter à SQL Server 2008 R2.**

  Ce problème peut survenir si Visual Studio 2008 n'est pas installé à l'emplacement par défaut et il est donc impossible de trouver le fichier de configuration devenv.exe.config lors de l'installation de SQL Server 2008. Pour résoudre ce problème, suivez la procédure suivante :

  1. Atteignez le dossier `<Visual Studio installation folder>\Microsoft Visual Studio 9.0\Common7\IDE`, localisez et copiez le fichier `devenv.exe.config`, puis collez-le dans le dossier suivant (vous pouvez avoir besoin d'activer les extensions d'affichage pour les types de fichiers connus dans les options de dossier) :

     - Pour un système d'exploitation 64 bits :

       ```
       C:\Program Files (x86)\Microsoft Visual Studio 9.0\Common7\IDE
       ```

     - Pour un système d'exploitation 32 bits :

       ```
       C:\Program Files\Microsoft Visual Studio 9.0\Common7\IDE
       ```

  2. Recommencez l'installation de SQL Server 2008 et ajoutez la fonction BIDS à l'instance existante de SQL Server 2008.

- **Impossible d'exporter la liste de dispositifs client dans la Gestion de dispositifs.**

Ceci peut se produire si le téléchargement de fichiers chiffrés est désactivé dans Internet Explorer. Suivez cette procédure pour activer le téléchargement de fichiers chiffrés :

1. Depuis votre navigateur Internet Explorer, accédez à **Outils** > **Options Internet**, puis cliquez sur l'onglet **Avancé** dans la fenêtre **Options Internet**.
2. Sous la section **Sécurité**, décochez **Ne pas enregistrer les pages chiffrées sur le disque**.
3. Sélectionnez **OK**.

- **L'état d'un dispositif mobile Android est toujours Désynchronisé.**

  Ceci s'explique par le fait que l'administrateur de dispositif Mobile Security n'est pas activé sur ce dispositif mobile. Si l'utilisateur n'active pas Mobile Security dans la liste des administrateurs de dispositif, Mobile Security ne peut pas synchroniser les stratégies de serveur avec le dispositif mobile et affiche comme état Désynchronisé.

- **Le contenu de la fenêtre contextuelle Stratégie ne s'affiche pas et est bloqué par Internet Explorer.**

  Cela se produit si Internet Explorer est configuré de manière à utiliser un fichier de configuration automatique .pac. Dans ce cas, Internet Explorer bloque l'accès à un site Web sécurisé contenant plusieurs fenêtres. Afin de résoudre ce problème, ajoutez l'adresse du serveur Mobile Security à la zone de sécurité des Sites de confiance dans Internet Explorer. Pour cela, suivez la procédure suivante :

  1. Démarrez Internet Explorer.
  2. Rendez-vous à **Outils** > **Options Internet**.
  3. Sur l'onglet **Sécurité**, cliquez sur **Sites de confiance**, puis cliquez sur **Sites**.
  4. Dans le champ de texte **Ajouter ce site Web à la zone**, saisissez l'URL du serveur Mobile Security, puis cliquez sur Ajouter.
  5. Sélectionnez **OK**.

  Pour plus de renseignements concernant ce problème, consultez l'URL suivante :

  http://support.microsoft.com/kb/908356

Avant de contacter l'assistance technique

Avant de contacter l'assistance technique, essayez de trouver la solution à votre problème :

- **Consultez votre documentation**—Le manuel et l'aide en ligne contiennent des informations complètes sur Mobile Security. Consultez ces deux supports pour vérifier s'ils contiennent la solution à votre problème.
- **Visitez notre site Web d'assistance technique**—Notre site Web d'assistance technique, appelé Base de connaissances, contient les informations les plus récentes sur tous les produits Trend Micro. Le site Web d'assistance contient les réponses aux questions déjà posées par les utilisateurs.

  Pour effectuer une recherche dans la Base de connaissances, visitez :

  http://esupport.trendmicro.com

Contacter l'assistance technique

Trend Micro propose une assistance technique, des téléchargements de signatures et des mises à jour de programmes pendant un an à tous les utilisateurs enregistrés. Au terme de cette période, vous devez acheter le renouvellement du contrat de maintenance. Si vous avez besoin d'aide ou si vous avez une question, contactez-nous. Vos commentaires sont également bienvenus.

- Obtenez une liste des bureaux d'assistance dans le monde entier sur *http://esupport.trendmicro.com*
- Obtenez les documentations les plus récentes sur les produits de Trend Micro sur *http://docs.trendmicro.com/fr-FR/home.aspx*

Aux États-Unis, vous pouvez contacter les représentants Trend Micro par téléphone, par fax ou par e-mail :

```
Trend Micro, Inc.
10101 North De Anza Blvd.,
Cupertino, CA 95014
```

```
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: http://www.trendmicro.com
Email: support@trendmicro.com
```

Envoi de fichiers infectés à Trend Micro

Vous pouvez envoyer des programmes malveillants et d'autres fichiers infectés à Trend Micro. Plus particulièrement, si vous pensez qu'un de vos fichiers est un programme malveillant mais que le moteur de scan ne le détecte pas ou ne le nettoie pas, vous pouvez envoyer ce fichier suspect à Trend Micro à l'adresse suivante :

http://esupport.trendmicro.com/srf/srfmain.aspx

Joignez une brève description au message pour décrire les symptômes que vous observez. Notre équipe d'ingénieurs spécialistes en programmes malveillants passera le fichier « à la loupe » pour détecter et identifier tout programme malveillant potentiel et vous renverra le fichier nettoyé, généralement sous 48 heures.

TrendLabs

Trend Micro TrendLabs℠ est un réseau mondial de recherche antivirus et de centres d'assistance technique qui offre un service continu, disponible 24h/24, 7j/7, aux clients Trend Micro du monde entier.

Avec une équipe de plus de 250 ingénieurs et un personnel d'assistance qualifié, les centres de service dédiés du monde entier traitent rapidement les épidémies de virus ou les problèmes d'assistance client urgents, partout dans le monde.

Le siège moderne de TrendLabs a obtenu la certification ISO 9002 pour ses procédures de gestion de la qualité en 2000. TrendLabs est l'une des premières installations de recherche et d'assistance antivirus à être ainsi certifiée. Trend Micro considère que les TrendLabs ont la meilleure équipe pour le service et l'assistance dans le secteur de l'antivirus.

Pour plus d'informations sur les TrendLabs, visitez le site suivant :

http://us.trendmicro.com/us/about/company/trendlabs/

À propos des mises à jour de logiciel

Après le lancement d'un produit, Trend Micro développe souvent des mises à jour pour le logiciel afin d'améliorer les performances du produit, ajouter des fonctionnalités ou résoudre un problème connu. Les types de mises à jour diffèrent en fonction de leur objectif.

Voici un récapitulatif des éléments que Trend Micro peut diffuser :

- **Correctif à chaud**—Un correctif à chaud constitue un contournement ou une solution à un problème unique signalé par le client. Les correctifs à chaud résolvent un problème précis et ne sont donc pas proposés à tous les clients. Les correctifs à chaud Windows contiennent un programme d'installation alors que les correctifs à chaud non-Windows n'en ont pas (généralement vous devez arrêter les démons, copier le fichier pour remplacer son correspondant dans votre installation et redémarrer les démons).
- **Patch de sécurité**—Un patch de sécurité est un correctif à chaud relatif à des problèmes de sécurité et il peut être déployé sur tous les clients. Les patchs de sécurité Windows contiennent un programme d'installation alors que les patchs non-Windows incluent en général un script d'installation.
- **Patch**—Un patch est un groupe de correctifs à chaud et de patchs de sécurité qui résolvent plusieurs problèmes du logiciel. Trend Micro publie régulièrement des patchs. Les patchs Windows contiennent un programme d'installation alors que les patchs non-Windows incluent en général un script d'installation.
- **Service Pack**—Un service pack est une consolidation de correctifs à chaud, de patchs et d'améliorations suffisamment significative pour être considérée comme une mise à niveau du produit. Les services packs Windows et non-Windows contiennent un programme d'installation et un script d'installation.

Consultez la Base de connaissances Trend Micro pour rechercher les correctifs à chauds publiés :

http://esupport.trendmicro.com

Consultez le site Web de Micro Trend régulièrement pour télécharger les patchs et les service packs :

http://downloadcenter.trendmicro.com/?regs=FR

Toutes les publications contiennent un fichier Lisez-moi proposant toutes les informations nécessaires pour installer, déployer et configurer votre produit. Consultez attentivement le fichier Lisez-moi avant d'installer un ou plusieurs fichiers de correctif à chaud, patch ou service pack.

Problèmes connus

Les problèmes connus sont des fonctions de Mobile Security susceptibles de nécessiter provisoirement une solution de contournement. Les problèmes connus sont généralement recensés dans le document Lisez-moi fourni avec votre produit. Vous pouvez également trouver les fichiers Lisez-moi relatifs aux produits Trend Micro dans le centre de téléchargements Trend Micro à l'adresse suivante :

http://downloadcenter.trendmicro.com/?regs=FR

Vous trouverez les problèmes connus dans la Base de connaissances de l'assistance technique :

http://esupport.trendmicro.com

Trend Micro recommande de toujours vérifier les informations contenues dans le fichier Lisez-moi relatives aux problèmes connus susceptibles d'affecter l'installation ou le fonctionnement de votre dispositif. Ce fichier contient également une description des nouveautés d'une version particulière, des informations sur la configuration requise et d'autres conseils.

Autres ressources utiles

Mobile Security propose de nombreux services par le biais de son site Web, http://www.trendmicro.com.

Les outils et services basés sur Internet sont les suivants :

- Carte des virus—surveillance des incidents liés à des programmes malveillants dans le monde entier.
- Évaluation des risques de virus—programme de Trend Micro pour l'évaluation en ligne de la protection contre les programmes malveillants pour les réseaux d'entreprise.

À propos de Trend Micro

Management Server, Inc., est un leader mondial dans la fourniture de services et de logiciels de sécurité de contenu Internet et d'anti-programmes malveillants réseau. Fondée en 1988, la société Trend Micro a permis à la protection anti-programmes malveillants d'être déployée non seulement sur les ordinateurs de bureau mais aussi sur les serveurs réseau et les passerelles Internet - se forgeant ainsi une solide réputation en matière d'innovation technologique et de vision.

Aujourd'hui, Trend Micro se concentre sur le développement de stratégies de sécurité complètes pour gérer les impacts des risques sur les informations, en offrant des services et produits de filtrage de contenu et de protection anti-programmes malveillants basés sur serveur et contrôlés centralement. En protégeant les informations qui transitent par les passerelles Internet, les serveurs de messagerie et les serveurs de fichiers, Trend Micro permet aux entreprises et aux fournisseurs de services du monde entier de bloquer les programmes et autres codes malveillants en un point central, avant qu'ils n'atteignent les postes de travail.

Pour plus d'informations ou pour télécharger des versions d'évaluation des produits Trend Micro, visitez notre site Web primé :

http://www.trendmicro.com

Index

N

O

P

R

S

T

TREND MICRO INCORPORATED

Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France

Tél. : +33 (0) 1 76 68 65 00 info@trendmicro.com

www.trendmicro.com

Item Code: TSFM96394/140410