



# 9.5 TREND MICRO™ Mobile Security™

Manuel de l'administrateur

Sécurité complète pour portables d'entreprise



Endpoint Security

Trend Micro Incorporated se réserve le droit de modifier ce document et les produits qu'il décrit sans préavis. Avant d'installer et d'utiliser le produit, veuillez donc consulter les fichiers Lisez-moi, les notes de mise à jour et la dernière version de la documentation utilisateur applicable que vous trouverez sur le site Web de Trend Micro à l'adresse suivante :

<http://docs.trendmicro.com/fr-FR/home.aspx>

Trend Micro, le logo t-ball, OfficeScan et TrendLabs sont des marques commerciales ou des marques déposées de Trend Micro Incorporated. Tous les autres noms de sociétés ou de produits sont des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

Copyright © 2015. Trend Micro Incorporated. Tous droits réservés.

Numéro de référence du document TSM97238/151028

Date de publication : septembre 2015

La documentation utilisateur de Trend Micro™ Mobile Security 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

Préface .....	vii
Public ciblé .....	viii
Documentation de Mobile Security .....	viii
Conventions typographiques du document .....	ix

## Chapitre 1: Introduction

Comprendre les menaces mobiles .....	1-2
À propos de Trend Micro Mobile Security 9.5 .....	1-2
Architecture du système Mobile Security .....	1-3
Composants du système Mobile Security .....	1-3
Comparaison entre le serveur local et le serveur de communication .....	1-6
Nouveautés de cette version (9.5) .....	1-7
Nouveautés de la version 9.3 .....	1-8
Nouveautés de la version 9.2 .....	1-9
Nouveautés de la version 9.1 .....	1-11
Nouveautés de la version 9.0 SP2 .....	1-12
Nouveautés de la version 9.0 SP1 .....	1-14
Nouveautés de la version 9.0 .....	1-16
Nouveautés de la version 8.0 SP1 .....	1-18
Nouveautés de la version 8.0 .....	1-19
Nouveautés de la version v7.1 .....	1-21
Nouveautés de la version 7.0 .....	1-21
Principales fonctions de l'agent de dispositif mobile .....	1-22
Fonctions des dispositifs mobiles OS prises en charge .....	1-25

## Chapitre 2: Mise en route avec Mobile Security

Console Web d'administration .....	2-2
Accès à la console Web d'administration .....	2-2
Désactivation du mode de compatibilité sur Internet Explorer .....	2-4
Licence du produit .....	2-4
Informations relatives au tableau de bord : .....	2-5
Personnalisation du Tableau de bord .....	2-8
Paramètres d'administration .....	2-10
Configuration des paramètres Active Directory (AD) .....	2-10
Configuration de l'authentification des utilisateurs .....	2-10
Configuration des paramètres de base de données .....	2-11
Configuration des paramètres de serveur de communication .....	2-11
Gestion des comptes d'administrateur .....	2-11
Gestion de la file de commandes .....	2-19
Configuration de la programmation de la suppression d'anciennes commandes .....	2-20
Suppression manuelle d'anciennes commandes .....	2-21
Intégration d'Exchange Server .....	2-21
Configuration des paramètres d'intégration d'Exchange Server ...	2-21
Configuration du connecteur Exchange .....	2-21
Gestion des certificats .....	2-22
Télécharger un certificat .....	2-22
Suppression de certificats .....	2-23

## Chapitre 3: Gestion des dispositifs mobiles

Onglet Dispositifs administrés .....	3-3
Groupes dans Mobile Security .....	3-3
Gestion des groupes .....	3-4
Gestion des dispositifs mobiles .....	3-6
État du dispositif mobile .....	3-11
Tâches de l'agent de dispositif mobile .....	3-14
Mise à jour des agents de dispositif mobile .....	3-14
Protection contre la perte du dispositif .....	3-15
Réinitialisation du mot de passe à distance .....	3-19

Gestion de Samsung KNOX Workspace à distance .....	3-20
Modification des paramètres iOS à distance .....	3-21
Exportation de données .....	3-22
Envoi de messages aux dispositifs mobiles .....	3-22
Onglet Dispositifs invités .....	3-23
Affichage de la liste d'invitation .....	3-24
Nouvel envoi de messages d'invitation .....	3-25
Annulation des invitations actives .....	3-25
Supprimer des invitations de la liste .....	3-26
Onglet Dispositifs Exchange ActiveSync .....	3-26
Invitation des dispositifs mobiles Exchange ActiveSync .....	3-27
Autorisation ou blocage de l'accès à Exchange Server .....	3-27
Effacement à distance d'un dispositif mobile ActiveSync .....	3-28
Suppression d'un dispositif mobile ActiveSync .....	3-29
Onglet Programme d'inscription des appareils .....	3-29
Expérience utilisateur du Programme d'inscription des appareils .....	3-30
Configuration de Mobile Security pour le Programme d'inscription des appareils .....	3-31
Intégration avec Trend Micro Control Manager .....	3-33
Création de stratégies de sécurité dans Control Manager .....	3-33
Suppression ou Modification de stratégies de sécurité .....	3-34
États des stratégies de sécurité dans Control Manager .....	3-34

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

À propos des stratégies de sécurité .....	4-3
Gestion des stratégies .....	4-6
Création d'une stratégie .....	4-6
Modification d'une stratégie .....	4-7
Attribution ou suppression de la stratégie d'un groupe .....	4-7
Copie d'une stratégie .....	4-8
Suppression de stratégies .....	4-8
Configuration de la disponibilité des applications .....	4-9
Stratégies de sécurité de Mobile Security .....	4-9
Stratégie courante .....	4-10
Stratégie WiFi .....	4-11

Stratégie Exchange ActiveSync .....	4-11
Stratégie VPN .....	4-12
Stratégie du proxy HTTP global .....	4-12
Stratégie des certificats .....	4-12
Stratégie d'authentification unique .....	4-12
Stratégie AirPlay/AirPrint .....	4-13
Stratégie de réseau cellulaire .....	4-14
Stratégie de thème .....	4-14
Stratégie de domaine géré .....	4-14
Stratégie de protection contre les programmes malveillants .....	4-15
Stratégie de prévention anti-spam .....	4-16
Stratégie de filtrage des appels .....	4-19
Stratégie de protection contre les menaces Internet .....	4-21
Stratégie de protection de la confidentialité .....	4-22
Stratégie de mot de passe .....	4-22
Stratégie de verrouillage des fonctions .....	4-23
Stratégie de compatibilité .....	4-23
Stratégie de surveillance et de contrôle des applications .....	4-24
Stratégie du programme d'achats en volume .....	4-26
Stratégie de conteneur .....	4-27

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

À propos de la Banque d'applications d'entreprise .....	5-2
Gestion des applications d'entreprise .....	5-2
Ajout d'une application .....	5-2
Modification des informations des applications .....	5-4
Suppression d'applications de la Banque d'applications .....	5-5
Gestion des catégories d'applications .....	5-5
Ajout d'une catégorie d'application .....	5-5
Modification d'une catégorie d'application .....	5-6
Suppression d'une catégorie d'application .....	5-6
Gestion des applications achetées via le Programme d'achats en volume .....	5-7
Configuration des licences du Programme d'achats en volume (VPP) .....	5-7



Attribution ou récupération de licences VPP .....	5-8
Vérification de l'état des utilisateurs VPP .....	5-10
Récupération de toutes les licences d'un utilisateur .....	5-10

## **Chapitre 6: Mise à jour des composants**

À propos des mises à jour de composants .....	6-2
Mise à jour des composants de Mobile Security .....	6-2
Mise à jour manuelle .....	6-2
Mise à jour programmée .....	6-3
Indication d'une source de téléchargement .....	6-5
Mise à jour manuelle d'un serveur AutoUpdate local .....	6-7

## **Chapitre 7: Affichage et maintenance des journaux**

À propos des journaux des agents de dispositif mobile .....	7-2
Affichage des journaux de l'agent de dispositif mobile .....	7-2
Maintenance des journaux .....	7-4
Planification de suppression de journaux .....	7-4
Suppression manuelle des journaux .....	7-5

## **Chapitre 8: Utilisation des notifications et rapports**

À propos des messages de notification et des rapports .....	8-2
Configuration des paramètres de notification .....	8-2
Configuration des notifications par courriel .....	8-2
Notifications et Rapports administrateur programmés .....	8-3
Activation des notifications et rapports administrateur .....	8-4
Configuration des paramètres de notification administrateur .....	8-5
Configuration des paramètres des rapports administrateur .....	8-6
Notification utilisateur .....	8-7
Configuration des notifications utilisateur .....	8-7

## **Chapitre 9: Dépannage et contact de l'assistance technique**

Dépannage .....	9-2
Avant de contacter l'assistance technique .....	9-5

Contacter Trend Micro .....	9-5
Envoi de contenu suspect à Trend Micro .....	9-6
Services de File Reputation .....	9-6
TrendLabs .....	9-6
À propos des mises à jour de logiciel .....	9-7
Problèmes connus .....	9-8
Autres ressources utiles .....	9-9
À propos de Trend Micro .....	9-9

## Index

Index .....	IN-1
-------------	------

# Préface

## Préface

Bienvenue au Manuel de l'administrateur Trend Micro™ Mobile Security for Enterprise version 9.5. 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 d'analyse, synchronisation des stratégies sur les dispositifs mobiles et utilisation des journaux et des rapports.

Cette préface aborde les sujets suivants :

- *Public ciblé à la page viii*
- *Documentation de Mobile Security à la page viii*
- *Conventions typographiques du document à la page ix*

## 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
- 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
<b>Gras</b>	Menus et commandes de menu, boutons de commande, onglets et options
<i>Italique</i>	Références à des documents annexes
Monospace	Exemples de lignes de commande, de code de programme, adresses Internet, noms de fichier et sortie de programme
<b>Navigation &gt; Chemin</b>	Le chemin de navigation pour atteindre un écran particulier  Par exemple, <b>Fichier &gt; Sauvegarder</b> signifie, cliquez sur <b>Fichier</b> puis cliquez sur <b>Sauvegarder</b> sur l'interface

CONVENTION	DESCRIPTION
 <b>Remarque</b>	Remarques de configuration
 <b>Conseil</b>	Recommandations ou suggestions
 <b>Important</b>	Informations relatives aux paramètres de configuration requis ou par défaut et aux limites des produits
 <b>AVERTISSEMENT!</b>	Actions stratégiques et options de configuration

# Chapitre 1

## Introduction

Trend Micro™ Mobile Security for Enterprise 9.5 est une solution de sécurité intégrée pour vos dispositifs mobiles. Ce chapitre décrit les composants et les fonctions de Mobile Security et vous explique comment Mobile Security protège vos dispositifs mobiles.

Ce chapitre contient les sections suivantes :

- *Comprendre les menaces mobiles à la page 1-2*
- *À propos de Trend Micro Mobile Security 9.5 à la page 1-2*
- *Architecture du système Mobile Security à la page 1-3*
- *Composants du système Mobile Security à la page 1-3*
- *Nouveautés de cette version (9.5) à la page 1-7*
- *Principales fonctions de l'agent de dispositif mobile à la page 1-22*
- *Fonctions des dispositifs mobiles OS prises en charge à la page 1-25*

## Comprendre les menaces mobiles

Avec la standardisation des plates-formes et l'extension de leur connectivité, 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 indésirables.

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 9.5

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

Les fonctions de filtrage intégrées permettent à Mobile Security de bloquer toute communication réseau indésirable vers les dispositifs mobiles. Parmi ces communications réseau indésirables, on trouve : les messages SMS et WAP push, ainsi que les 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.



### **AVERTISSEMENT!**

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

---



## Architecture du système Mobile Security

En fonction des besoins de votre entreprise, vous pouvez implémenter Mobile Security à l'aide de 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 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 la description des composants de Mobile Security.

**TABEAU 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

COMPOSANT	DESCRIPTION	REQUIS OU FACULTATIF
Serveur de communication	<p>Le serveur de communication gère les communications entre le serveur d'administration et les agents de dispositif mobile.</p> <p>Trend Micro Mobile Security fournit deux types de Serveur de communication :</p> <ul style="list-style-type: none"> <li>• Serveur de communication local (LCS)—il s'agit d'un Serveur de communication déployé localement sur votre réseau.</li> <li>• Serveur de communication du nuage (CCS)—il s'agit d'un Serveur de communication déployé sur le nuage ; vous n'aurez donc pas besoin de l'installer. Trend Micro gère le Serveur de communication du nuage et il vous suffit de vous-y connecter à partir du serveur d'administration.</li> </ul> <p>Voir la section <a href="#">Comparaison entre le serveur local et le serveur de communication</a> à la page 1-6.</p>	Requis
Connecteur Exchange	<p>Trend Micro Mobile Security utilise le connecteur Exchange pour communiquer avec Microsoft Exchange Server et détecte les dispositifs qui utilisent le service Exchange ActiveSync. En outre, il les affiche sur la console Web de Mobile Security.</p> <p>L'intégration de serveur Microsoft Exchange avec Mobile Security permet aux administrateurs de surveiller les dispositifs mobiles qui accèdent au serveur Microsoft Exchange. Lorsque la fonction est activée et configurée, les administrateurs de Mobile Security peuvent effectuer la suppression à distance et bloquer l'accès à Microsoft Exchange Server pour ces dispositifs mobiles.</p> <p>L'intégration de Microsoft Exchange Server avec Mobile Security permet également aux administrateurs de surveiller l'accès utilisateur aux données de coopération (telles que les courriels, calendrier, contacts, etc.).</p>	Facultatif

COMPOSANT	DESCRIPTION	REQUIS OU FACULTATIF
Agent de dispositif mobile (MDA)	L'agent de dispositif mobile est installé sur les dispositifs mobiles Android et iOS administrés. L'agent communique avec le serveur de communication de Mobile Security et exécute les paramètres de commandes et de stratégies sur le dispositif mobile.	Requis
Microsoft SQL Server	Le serveur Microsoft SQL héberge les bases de données du serveur d'administration Mobile Security.	Requis
Active Directory	Le serveur d'administration 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 de la sécurité ainsi que les clés publiques et privées pour une communication sécurisée.	Facultatif
SCEP	<p>Le certificat SCEP (Extension du protocole d'inscription du certificat simple) est un protocole de communication qui fournit une partie frontale en réseau à une autorité de certification privée.</p> <p>Dans certains environnements, il est important de s'assurer que les paramètres et les stratégies d'entreprise sont protégés des yeux indiscrets. Afin d'assurer cette protection, iOS vous permet de chiffrer les profils afin qu'ils ne puissent être lus que par un seul dispositif. Un profil chiffré est similaire à un profil de configuration normal, excepté que la charge utile du profil de configuration est chiffrée par la clé publique associée à l'identité X.509 du dispositif.</p> <p>Le protocole 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.</p>	Facultatif

COMPOSANT	DESCRIPTION	REQUIS OU FACULTATIF
Certificat APNs	Le serveur de communication Mobile Security communique à travers le service Apple Push Notification Service (APNs) vers 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 Windows Phone ou iOS
Serveur SMTP	Connectez le serveur SMTP pour vous assurer que les administrateurs peuvent obtenir des rapports du serveur d'administration Mobile Security, et envoyer des invitations aux utilisateurs.	Facultatif

## Comparaison entre le serveur local et le serveur de communication

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	Pris en charge	Pris en charge

<b>FONCTIONS</b>	<b>SERVEUR DE COMMUNICATION DU NUAGE</b>	<b>SERVEUR DE COMMUNICATION LOCAL</b>
Gestion de Windows Phone	Non pris en charge	Pris en charge

## Nouveautés de cette version (9.5)

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.5 :

<b>NOM DES FONCTIONS</b>	<b>DESCRIPTION</b>
Améliorations du programme d'achats en grande quantité (VPP) dans iOS 9	Permet à l'administrateur d'attribuer des licences d'application à des utilisateurs ou des dispositifs
Verrouillage de fonctions pour iOS 9 ou ultérieur	Nouvelles options de verrouillage de fonctions disponibles pour les dispositifs mobiles fonctionnant sous iOS 9 ou ultérieur.
Améliorations des rapports	Les améliorations suivantes sont apportées dans cette version : <ul style="list-style-type: none"> <li>• Nouvel affichage HTML pour un usage amélioré.</li> <li>• Les nouveaux graphiques fournissent des informations supplémentaires sur les dispositifs administrés et les applications.</li> </ul>
Détails sur la violation de conformité	Les causes de la violation de conformité sont désormais affichées sur la console Web pour chaque dispositif mobile non conforme.
Inscription du code QR dans la console Web	Les administrateurs peuvent désormais inscrire les utilisateurs à partir de la console Web à l'aide du nouveau code QR de la clé d'inscription disponible sur l'écran des paramètres d'inscription des dispositifs.

NOM DES FONCTIONS	DESCRIPTION
Améliorations de l'état d'accès à Exchange	<p>Les nouvelles options suivantes sont disponibles dans cette version :</p> <ul style="list-style-type: none"> <li>• Les administrateurs peuvent choisir de bloquer automatiquement l'accès au serveur Exchange des dispositifs non gérés.</li> <li>• Les administrateurs peuvent choisir d'activer automatiquement l'option Autorisation/blocage d'accès automatique pour tous les dispositifs administrés.</li> </ul>
Amélioration de la gestion des applications dans iOS 9	Les applications non gérées sont installées comme des applications administrées lorsque les utilisateurs les installent à partir de la banque d'applications d'entreprise ou lorsque l'administrateur ajoute une application requise à une stratégie.

## Nouveautés de la version 9.3

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.3 :

NOM DES FONCTIONS	DESCRIPTION
Agent de dispositif mobile disponible sur Google Play	À partir de cette version, les utilisateurs peuvent télécharger l'agent de dispositif mobile Android dans le magasin Google Play.
Analyse de Facebook pour Android et iOS	Analyse de vos paramètres de confidentialité Facebook et propose des réglages permettant d'améliorer votre confidentialité.
Analyse de sécurité pour iOS	Analyse de toutes les applications installées pour supprimer les virus, les applications malveillantes et les programmes espions susceptibles de voler vos informations et vous coûter cher.

NOM DES FONCTIONS	DESCRIPTION
Analyse depuis le nuage	Amélioration de l'analyse du cloud sur les dispositifs mobiles Android, lorsque les dispositifs mobiles utilisent un serveur proxy.
Sensibilisation sur l'emplacement pour le verrouillage de fonctions Android	Vous permet de faire respecter la stratégie de verrouillage des fonctions lorsque le dispositif mobile est à portée d'un point d'accès, puis de restaurer les paramètres des fonctionnalités lorsque l'utilisateur est hors portée.
Ajout de la prise en charge de l'expéditeur de SMS	Ajout de la prise en charge pour que l'expéditeur de SMS puisse envoyer des messages SMS aux utilisateurs.

## Nouveautés de la version 9.2

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.2 :

NOM DES FONCTIONS	DESCRIPTION
Gestion centralisée de l'analyse de la confidentialité	Permet aux administrateurs d'autoriser les utilisateurs à effectuer un scan manuel et à forcer les dispositifs mobiles à charger sur le serveur les journaux de confidentialité.
Modèles pour administrateurs de groupes	Permet au super-administrateur de convertir une stratégie en modèle et permet aux administrateurs de groupes d'utiliser ces modèles pour créer des stratégies pour les groupes qui leur sont attribués.
Localisation de dispositifs mobiles iOS	Comprend la prise en charge de la localisation des dispositifs mobiles iOS.
Évaluation des risques de sécurité pour les applications présentées dans Google Play	Effectue une évaluation des risques de sécurité et d'utilisation des ressources à l'aide de Mobile Application Reputation Service (MARS) avant d'ajouter une application provenant d'une banque d'applications externe (Google Play).

<b>NOM DES FONCTIONS</b>	<b>DESCRIPTION</b>
Notification par courriel en temps réel	Ajoute une notification par courriel afin d'avertir l'administrateur de la détection d'un programme malveillant sur un dispositif mobile Android.
Notification d'expiration du certificat APNs	Ajoute une notification dans le tableau de bord afin d'avertir l'administrateur de l'expiration prochaine du certificat APNs.
Diffusion de message	Vous permet de diffuser un message vers des dispositifs mobiles Android et iOS en une seule fois.
Utilisation plus conviviale de Stratégie de surveillance et de contrôle des applications	Vous permet d'importer une liste des applications dans Stratégie de surveillance et de contrôle des applications.
Annulation de l'enregistrement de l'agent de dispositif mobile	Les dispositifs mobiles Android et iOS comprennent une option permettant d'annuler l'enregistrement de l'agent de dispositif mobile du serveur.
SQL Server Express 2008	Comprend SQL Server Express 2008 avec package d'installation de Mobile Security.



NOM DES FONCTIONS	DESCRIPTION
Amélioration des fonctionnalités de gestion Apple iOS	<p>Les améliorations suivantes sont comprises :</p> <ul style="list-style-type: none"> <li>• Prise en charge du Programme d'inscription des appareils (DEP) et du Programme d'achats en volume (VPP) d'Apple.</li> <li>• La console Web d'administration affiche des informations supplémentaires pour les dispositifs mobiles iOS 8 ou version supérieure.</li> <li>• Possibilité d'ajouter un message personnalisé sous la forme de texte lors de l'envoi d'une commande de verrouillage d'un dispositif mobile.</li> <li>• Possibilité de configurer des domaines gérés.</li> <li>• Possibilité d'initier et d'interrompre la mise en miroir d'AirPlay pour les dispositifs mobiles.</li> <li>• Possibilité d'intégrer de nouvelles polices dans les dispositifs mobiles.</li> <li>• Possibilité de modifier le nom d'un dispositif mobile.</li> <li>• De nouvelles options de verrouillage des fonctionnalités sont ajoutées pour les dispositifs mobiles iOS 8 ou version supérieure.</li> </ul>
Suppression de la prise en charge des dispositifs BlackBerry	Les dispositifs mobiles BlackBerry ne sont plus pris en charge dans cette version.
Suppression de la prise en charge de l'expéditeur de SMS	L'expéditeur de SMS n'est plus pris en charge dans cette version.

## Nouveautés de la version 9.1

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.1 :

NOM DES FONCTIONS	DESCRIPTION
Protection par mot de passe des paramètres système	Offre une protection par mot de passe des paramètres système des dispositifs mobiles Android.
Amélioration des informations sur le dispositif	Elles comprennent plus de détails sur les dispositifs mobiles clients sur la console Web d'application et le dispositif mobile. En outre, le fichier CSV exporté comprend l'information « Heure de la dernière connexion » pour les dispositifs mobiles clients.
Amélioration de la recherche avancée	Elle comprend plus d'attributs de recherche afin d'améliorer la recherche avancée.
Amélioration de la banque d'applications d'entreprise	<p>Les améliorations suivantes sont apportées à la banque d'applications d'entreprise dans Trend Micro Mobile Security :</p> <ul style="list-style-type: none"> <li>• Vous pouvez désormais mettre à jour les applications installées sur les dispositifs mobiles.</li> <li>• Différentiation des applications iOS pour iPhone, iPad et iPod.</li> </ul>
Amélioration de l'exportation des journaux	Vous pouvez exporter tous les journaux.
Horodatage du journal d'événement	Affiche l'horodatage du journal d'événement mobile dans le fuseau horaire du serveur et du dispositif mobile.
Amélioration du processus d'inscription	Vous permet de configurer à l'avance les informations d'inscription du serveur de communication du nuage dans le fichier APK Android pour une inscription plus facile.
Sous-groupes dans une arborescence de dispositif	Permet aux administrateurs de créer des sous-groupes dans une arborescence de dispositif.

## Nouveautés de la version 9.0 SP2

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.0 SP2 :

NOM DES FONCTIONS	DESCRIPTION
Prise en charge de Windows Phone	Prend également en charge Windows Phone.
Gestion de Samsung KNOX Workspace	Prend également en charge Samsung KNOX Workspace.
Amélioration des fonctionnalités de gestion Apple iOS	<p>Les améliorations suivantes sont apportées dans cette version :</p> <ul style="list-style-type: none"> <li>• La console Web d'administration affiche des informations supplémentaires pour les dispositifs mobiles iOS 7 ou version supérieure.</li> <li>• Un plus grand nombre de commandes sont incluses pour la gestion des dispositifs mobiles iOS.</li> <li>• La mise en service de la stratégie AirPlay et AirPrint est ajoutée dans cette version.</li> <li>• La stratégie de réseau cellulaire est ajoutée afin de pouvoir configurer des paramètres APN sur des dispositifs mobiles iOS.</li> <li>• Des thèmes sont ajoutés pour définir des papiers peints sur des dispositifs mobiles iOS.</li> <li>• De nouvelles options de verrouillage des fonctionnalités sont ajoutées pour les dispositifs mobiles iOS 7 ou version supérieure.</li> </ul>
Suppression de la prise en charge de Windows Mobile et de Symbian	La prise en charge de Windows Mobile et de Symbian est supprimée dans cette version.

NOM DES FONCTIONS	DESCRIPTION
Amélioration de la banque d'applications d'entreprise	Les améliorations suivantes sont apportées à la banque d'applications d'entreprise dans Trend Micro Mobile Security : <ul style="list-style-type: none"><li>• Affiche les applications populaires dans la banque d'applications d'entreprise et les applications installées sur le dispositif mobile.</li><li>• Amélioration de la recherche d'applications dans la banque d'applications</li><li>• Permet aux administrateurs de définir des applications spécifiques comme invisibles pour des stratégies spécifiques.</li></ul>
Amélioration de la gestion de file de commandes	Permet aux administrateurs de vider manuellement la file de commandes ou selon une programmation prédéfinie.
Amélioration des tâches de l'agent de dispositif mobile	Permet de supprimer de manière sélective des dispositifs mobiles débridés.
Amélioration de l'affichage de l'état de l'agent de dispositif mobile	Lorsque l'état du dispositif mobile devient Inactif, l'écran d'état du dispositif mobile affiche le motif du changement d'état.

## Nouveautés de la version 9.0 SP1

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.0 SP1 :

NOM DES FONCTIONS	DESCRIPTION
Intégration avec Control Manager	<p>Intégration complète avec Trend Micro Control Manager.</p> <ul style="list-style-type: none"> <li>• Cette version permet le chargement du journal d'état, des informations utilisateur et des informations des dispositifs mobiles vers Trend Micro Control Manager.</li> <li>• Prise en charge de l'authentification unique pour permettre à l'administrateur de Trend Micro Control Manager d'accéder à la console Web de Trend Micro Mobile Security sans avoir à fournir d'informations d'authentification.</li> </ul>
Paramètres de point d'accès WiFi pour iOS	Paramètres de point d'accès Wi-Fi pour dispositifs mobiles iOS 7.0 ou version supérieure.
Amélioration de la sécurité des données d'entreprise	Paramètres de gestion « Open-in » accessibles aux administrateurs, leur permettant de protéger les données d'entreprise en limitant l'ouverture de fichiers dans certaines applications.
Prise en charge de l'authentification unique pour iOS	Prise en charge de l'authentification unique pour les dispositifs mobiles iOS 7.0 ou version supérieure afin de permettre l'utilisation des mêmes informations d'authentification sur un ensemble d'applications spécifiées par l'administrateur.
Prise en charge de la protection contre les menaces Internet pour iOS	Prise en charge de la protection contre les menaces Internet pour les dispositifs mobiles iOS 7.0 ou version supérieure afin de filtrer certains sites Web ou tout contenu réservé aux adultes.
Prise en charge du VPN par application pour iOS	Prise en charge du VPN par application pour les dispositifs mobiles iOS 7.0 ou version supérieure, afin de permettre aux administrateurs de lier un VPN à certaines applications, de sorte que ces dernières utilisent ce VPN pour accéder au réseau.
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.
Prise en charge IPv6	Prise en charge IPv6 pour les agents de serveur et de dispositif mobile.

NOM DES FONCTIONS	DESCRIPTION
Prise en charge du connecteur Exchange	Prise en charge du connecteur Exchange pour Microsoft Exchange Server 2013

## Nouveautés de la version 9.0

Le tableau suivant décrit les nouvelles fonctions incluses dans Trend Micro™ Mobile Security for Enterprise 9.0.

NOM DES FONCTIONS	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 sur le nuage (Serveur de communication du nuage). Les administrateurs n'ont pas besoin d'installer le Serveur de communication du nuage, et il est maintenu par Trend Micro.
Intégration d'Exchange Server	Fournit l'intégration de Microsoft Exchange Server, et prend en charge les 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 assigner à un groupe de dispositifs mobiles.
Prise en charge des comptes administrateur multiples	Vous permet de créer plusieurs comptes administrateur avec des rôles différents qui peuvent être personnalisés en fonction des besoins et au moment opportun.
États de dispositif mis à jour	Affiche l'état actuel des dispositifs mobiles de façon plus appropriée avec la liste des états des dispositifs mise à jour.

NOM DES FONCTIONS	DESCRIPTION
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 du dispositif en mode supervisé	Cette version apporte également une assistance aux dispositifs mobiles iOS en mode surveillé.
Gestion de l'écran du tableau de bord	Vous permet de gérer les informations affichées sur l' écran du <b>Tableau de bord</b> sous forme de widgets. Vous pouvez ajouter ou supprimer les widgets selon vos besoins.
Confirmation de commande du serveur	Fournit l'interface de <b>Gestion de la file de commandes</b> qui affiche l'état actuel de chaque commande exécutée à partir du serveur.
Contrôle d'application utilisant des catégories	Vous permet d'autoriser ou de bloquer l'installation de certaines applications qui appartiennent à des catégories sur les dispositifs mobiles iOS et Android disposant de listes bloquées ou approuvées.
Inscription de dispositif mobile en utilisant un code QR	Présente l'inscription du dispositif mobile à l'aide du code QR qui est envoyé par e-mail à l'utilisateur.
Stratégie de verrouillage des fonctions améliorée	Ajoute plus de fonctions et de composants OS à la fonction de la liste de blocage pour que l'administrateur contrôle leur disponibilité sur les dispositifs mobiles.
Prise en charge du programme d'achats en volume d'iOS	Vous permet d'importer les applications iOS qui sont achetées par le biais du programme d'achats en grande quantité d'Apple sur la console Web d'administration Mobile Security.
Interface de l'agent de dispositif mobile mise à jour	Introduit la nouvelle interface utilisateur pour les agents de dispositifs mobiles Android et iOS.
Intégration de MARS	Fournit le serveur et l'intégration de l'agent de dispositif mobile Android avec le service MicroMobile Application Reputation Service (MARS) pour le risque de sécurité des applications et pour l'utilisation des ressources.

NOM DES FONCTIONS	DESCRIPTION
Téléchargement de rapports administrateur	Permet de télécharger les rapports administrateur de la console Web d'administration de Mobile Security.
Journal de violation de la stratégie	Fournit un journal des violations de stratégies pour les dispositifs mobiles Android.
Intégration avec Trend MicroControl Manager	Trend Micro Mobile Security assure l'intégration avec le gestionnaire de contrôle Trend MicroControl Manager. Cette intégration permet aux administrateurs du gestionnaire de contrôle de remettre des stratégies d'entreprise aux dispositifs mobiles et leur permet de visualiser l'écran <b>Tableau de bord</b> de Mobile Security dans le gestionnaire de contrôle.

## Nouveautés de la version 8.0 SP1

Le tableau suivant décrit les fonctionnalités supplémentaires qui ont été introduites dans Trend Micro™ Mobile Security for Enterprise 8.0 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 géré pour Android et iOS	Introduit un groupe "non géré" 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.



NOM DES FONCTIONS	DESCRIPTION
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 fonctionnalités supplémentaires qui ont été introduites dans Trend Micro™ Mobile Security for Enterprise 8.0.

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 d'administration 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.

NOM DES FONCTIONS	DESCRIPTION
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'application	Maintient la liste des applications installées sur les dispositifs mobiles et l'affiche sur l'écran d'état du dispositif.
Contrôle de l'application	Vous permet d'autoriser ou de bloquer l'installation de certaines applications sur les dispositifs mobiles disposant de listes bloquées ou approuvées.
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 du tableau de bord	Introduit l'écran du <b>tableau de bord</b> pour remplacer l'ancien écran <b>résumé</b> 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 <b>Configuration et vérification de la configuration de Mobile Security</b> 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.

NOM DES FONCTIONS	DESCRIPTION
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 fonctionnalités supplémentaires qui ont été introduites dans Trend Micro™ Mobile Security for Enterprise 7.1.

NOM DES FONCTIONS	DESCRIPTION
Prise en charge des dispositifs mobiles BlackBerry et iOS	Ajout de la prise en charge par Mobile Security 7.1 des dispositifs mobiles iOS et BlackBerry.
Intégré avec Active Directory	Mobile Security 7.1 tire profit de l'Active Directory (AD) d'entreprise pour importer des utilisateurs et les authentifier.
Architecture mise à jour	Dans Mobile Security 7.1, des modèles de déploiement sur un ou deux serveurs sont introduits. La passerelle SMS est également supprimée dans la version 7.1.
Stratégie de mise en service	Cette version introduit la stratégie de mise en service des dispositifs mobiles.


## Nouveautés de la version 7.0


Cette section décrit les fonctionnalités supplémentaires qui ont été introduites dans Trend Micro™ Mobile Security for Enterprise 7.0.

NOM DES FONCTIONS	DESCRIPTION
Prise en charge des dispositifs mobiles Android	Ajout de la prise en charge par Mobile Security 7.0 des dispositifs mobiles Android 2.1 ou ultérieurs.
Stratégies de filtrage des appels	Permet à l'administrateur de contrôler les appels entrants ou sortants sur les dispositifs mobiles Android.
Fonction de 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.
Localisation d'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 7.0, 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
Analyse contre les 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.

NOM DES FONCTIONS	DESCRIPTION
Sécurité Web	<p>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.</p>
Anti-spam pour SMS	<p>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.</p> <hr/> <p> <b>Remarque</b></p> <p>La fonction Anti-spam SMS n'est pas disponible sur les dispositifs mobiles non équipés de fonctionnalités téléphoniques.</p>




NOM DES FONCTIONS	DESCRIPTION
Filtrage des appels	<p>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.</p> <hr/> <p> <b>Remarque</b></p> <p>La fonction de filtrage des appels n'est pas disponible sur les dispositifs mobiles non équipés de fonctionnalités téléphoniques.</p>
Protection WAP Push	<p>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.</p> <p>Il s'avère que des utilisateurs malveillants envoient des messages WAP-Push erronés ou contenant de fausses informations qui trompent les utilisateurs pour qu'ils acceptent un contenu susceptible d'abriter des applications et des paramètres système indésirables, 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.</p> <p>La fonction de protection WAP Push n'est pas disponible sur les dispositifs mobiles non équipés de fonctionnalités téléphoniques.</p>
Authentification	<p>Après l'installation de l'agent de dispositif mobile, l'utilisateur du dispositif mobile doit fournir les informations d'authentification pour inscrire les dispositifs mobiles sur le serveur d'administration Mobile Security.</p>

NOM DES FONCTIONS	DESCRIPTION
Mises à jour régulières	<p>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.</p>
Journaux	<p>Les journaux de l'agent de dispositif mobile suivants sont disponibles sur le serveur d'administration :</p> <ul style="list-style-type: none"> <li>• journal de protection contre les programmes malveillants</li> <li>• journal de protection contre les menaces Internet</li> <li>• journal d'événements</li> <li>• journal des violations</li> </ul> <p>Vous pouvez afficher les journaux suivants sur les dispositifs mobiles :</p> <ul style="list-style-type: none"> <li>• Android : <ul style="list-style-type: none"> <li>• historique de la recherche de programmes malveillants</li> <li>• historique de l'analyse de la confidentialité</li> <li>• historique du blocage web</li> <li>• historique des appels bloqués</li> <li>• historique des SMS bloqués</li> <li>• historique des mises à jour</li> </ul> </li> </ul>




## Fonctions des dispositifs mobiles OS prises en charge




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




**TABLEAU 1-3. Matrice des fonctionnalités Trend Micro Mobile Security 9.5**




STRATÉGIE	FONCTIONS	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	●		
	Réseau cellulaire	Configuration d'un réseau cellulaire	●		
	AirPlay/AirPrint	Configuration AirPlay/AirPrint	●		
	Thèmes (pour le mode supervisé uniquement)	Configuration du papier-peint	●		
		Configuration de la police	●		
	Domaines gérés	Domaines de messagerie non marqués	●		
		Domaines Web Safari gérés	●		
Sécurité de dispositif	Protection contre les programmes malveillants	Analyse en temps réel		●	
		Analyse après mise à jour des signatures		●	
		Analyse manuelle	●	●	
	Protection de la confidentialité	Analyse de la confidentialité		●	









STRATÉGIE	FONCTIONS	PARAMÈTRES			
		Chargement de journal d'analyse de confidentialité		●	
		Analyse de Facebook	●	●	
Protection des données	Prévention anti-spam par SMS	Contrôle côté serveur		●	
		Utiliser liste bloquée		●	
		Utiliser liste approuvée		●	
	Prévention anti-spam WAP Push	Contrôle côté serveur		●	
		Utiliser liste approuvée		●	
	Filtrage des appels	Contrôle côté serveur		●	
		Utiliser liste bloquée		●	
		Utiliser liste approuvée		●	
	Protection contre les menaces Internet	Contrôle côté serveur		●	
		Utiliser liste bloquée		●	
		Utiliser liste approuvée		●	
		Autoriser des sites Web spécifiques uniquement	●		
Autoriser le contenu réservé aux adultes		●			
Protection des données	Paramètres de mot de passe	Ouverture de session à l'aide d'un mot de passe	●	●	●
		Autoriser un mot de passe simple	●	●	●
		Nécessiter un mot de passe alphanumérique	●	●	●




STRATÉGIE	FONCTIONS	PARAMÈTRES			
		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	●	●	●
	Verrou de fonction	Caméra	●	●	
		Temps en vis-à-vis	●		
		Capture d'écran	●		
		Installation d'applications	●		
		Synchronisation en itinérance	●		
		Composition vocale	●		
		Achat d'applications intégré	●		
		Jeu multi-joueurs	●		
		Ajouter des amis au Game center	●		
		Game Center (uniquement pour le mode surveillé)	●		
		Forcer les sauvegardes chiffrées	●		
		Musique, podcast et iTunes U explicites	●		
		Carnet de banque en mode verrouillé	●		




STRATÉGIE	FONCTIONS	PARAMÈTRES			
		Bluetooth et Bluetooth discovery		●	
		WLAN/Wi-Fi		●	
		Réseau de données 3G		●	
		Mode modem		●	
		Mode développeur		●	
		Haut-parleur/téléphone à haut-parleur/microphone			
		Restriction des cartes mémoire		●	
		Siri	●		
		Siri lorsque le dispositif est en mode verrouillé	●		
		Activer le filtre d'obscénités	●		
		Activer l'accès aux services iCloud	●		
		Sauvegarde Cloud	●		
		Synchronisation de documents Cloud	●		
		Galerie de photos	●		
		Galerias de photos partagées	●		
		Données de diagnostic	●		
		Accepter les TLS (Transport Layer Security) non approuvés	●		

STRATÉGIE	FONCTIONS	PARAMÈTRES			
		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 Internet 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)	●		
		Érotique (uniquement pour le mode surveillé)	●		
		Installation de profil de configuration (uniquement pour le mode surveillé)	●		




STRATÉGIE	FONCTIONS	PARAMÈTRES			
		iMessage (uniquement pour le mode surveillé)	●		
		Évaluations de la région	●		
		Films	●		
		Évaluation des émissions	●		
		Applications	●		
		Modification de compte (dispositifs supervisés uniquement)	●		
		AirDrop (dispositifs supervisés uniquement)	●		
		Modification de l'utilisation de données cellulaires des applications (dispositifs supervisés uniquement)	●		
		Contenu de l'assistant (Siri) généré par les utilisateurs (dispositifs supervisés uniquement)	●		
		Synchronisation du trousseau iCloud	●		
		Modification de l'application Localiser mes amis (dispositifs supervisés uniquement)	●		
		Déverrouillage du dispositif par empreinte digitale	●		
		Jumelage de l'hôte (dispositifs supervisés uniquement)	●		




STRATÉGIE	FONCTIONS	PARAMÈTRES			
		Centre de contrôle sur l'écran de verrouillage	●		
		Affichage des notifications sur l'écran de verrouillage	●		
		Affichage du jour sur l'écran de verrouillage	●		
		Mises à jour de l'infrastructure à clés publiques en mode OTA (OTAPKI)	●		
		Forçage du suivi publicitaire limité	●		
		Forçage des demandes sortantes AirPlay de mot de passe de jumelage	●		
		Autoriser les applications gérées à stocker des données dans l'iCloud	●		
		Autoriser la sauvegarde des livres d'entreprise	●		
		Autoriser les restrictions de configuration	●		
		Autoriser l'effacement de tout le contenu et des paramètres	●		
		Autoriser le transfert	●		
		Autoriser les résultats Internet dans les actualités	●		
		Autoriser la synchronisation des remarques et des recommandations dans les livres d'entreprise	●		

STRATÉGIE	FONCTIONS	PARAMÈTRES			
		Autoriser le partage des documents gérés en utilisant AirDrop	●		
		Autoriser la bibliothèque de photos iCloud	●		
		Autoriser l'installation d'applications du dispositif	●		
		Autoriser les raccourcis clavier	●		
		Autoriser le couplage avec Apple Watch	●		
		Autoriser la modification du code secret	●		
		Autoriser la modification du nom du dispositif	●		
		Autoriser la modification du papier peint	●		
		Autoriser le téléchargement automatique des applications	●		
		Autoriser les applications de confiance	●		
	Paramètres de conformité	Débridé	●	●	
		Non chiffré	●	●	
		Vérification de la version du système d'exploitation	●	●	
Gestion des applications	Surveillance et contrôle des applications	Applications requises	●	●	
		Applications autorisées	●	●	

STRATÉGIE	FONCTIONS	PARAMÈTRES				
		Verrouillage pour application (uniquement pour le mode Surveillé)	●			
	Programme d'achats en grande quantité	Programme d'achats en grande quantité	●			
Contrôle à distance	Enregistrer		●	●		
	Mise à jour		●	●		
	Protection antivol	Localisation à distance			●	
		Verrouillage à distance		●	●	
		Effacement à distance		●	●	●
		Réinitialiser le mot de passe		●	●	
	Samsung KNOX Workspace	Créer un conteneur			●	
		Supprimer le conteneur			●	
		Verrouiller le conteneur			●	
		Déverrouiller le conteneur			●	
Réinitialiser le mot de passe du conteneur			●			
Stratégie Samsung KNOX Workspace	Configuration de compte de conteneur	Liste bloquée		●		
		Liste approuvée		●		
	Paramètres de restriction	Autoriser les utilisateurs à utiliser la caméra			●	
		Autoriser l'affichage du partage via la liste des applications			●	



STRATÉGIE	FONCTIONS	PARAMÈTRES			
	Paramètres du navigateur	Paramètre Activer le remplissage automatique		●	
		Paramètre Activer les cookies		●	
		Paramètre Activer les messages contextuels		●	
		Paramètre Activer l'avertissement forcé de fraude		●	
		Paramètre Activer JavaScript		●	
		Activer le proxy Web		●	
Stratégie Samsung KNOX Workspace	Paramètres de mot de passe du conteneur	Activer la visibilité du mot de passe		●	
		Longueur minimale de modification de mot de passe		●	
		Longueur minimale du mot de passe		●	
		Délai d'inactivité maximal		●	
		Nombre maximal de tentatives infructueuses		●	
		Historique des mots de passe		●	
		Âge maximal du mot de passe		●	
		Nombre minimal de caractères spéciaux requis dans un mot de passe		●	
	Complexité du mot de passe		●		
	Paramètres de l'application	Installation de la liste approuvée		●	

STRATÉGIE	FONCTIONS	PARAMÈTRES			
		Installation de la liste bloquée		<input checked="" type="checkbox"/>	
		Applications requises		<input checked="" type="checkbox"/>	
		Applications désactivées		<input checked="" type="checkbox"/>	
		Programme d'inscription des appareils	<input checked="" type="checkbox"/>		

# 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 :

- *Accès à la console Web d'administration à la page 2-2*
- *Informations relatives au tableau de bord : à la page 2-5*
- *Paramètres d'administration à la page 2-10*
- *Gestion de la file de commandes à la page 2-19*
- *Intégration d'Exchange Server à la page 2-21*
- *Gestion des certificats à la page 2-22*

## 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 actuelle, et <HTTPS\_port> avec le numéro de port actuel 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 Web d'administration est « root » 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. Les composants anti-programmes malveillants sont donc vulnérables face aux risques de sécurité les plus récents.

Si votre licence expire, vous devrez enregistrer le serveur d'administration 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 d'administration 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** de 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 :
  - Afficher l'état des dispositifs mobiles :
    - **Sain**—indique que le dispositif est inscrit sur le serveur d'administration Mobile Security et que les composants et stratégies sur le dispositif mobile sont à jour.
    - **Non conforme**—indique que le dispositif est inscrit sur le serveur d'administration Mobile Security, mais qu'il n'est pas compatible avec les stratégies du serveur.
    - **Désynchronisé**—indique que le dispositif est inscrit sur le serveur d'administration Mobile Security, mais que les composants ou les stratégies sont obsolètes.

- **Inactif**—indique que le dispositif n'est pas encore inscrit sur le serveur d'administration Mobile Security.
- Afficher le nombre total de dispositifs mobiles inscrits et non inscrits gérés par Mobile Security.

Si la connexion au serveur de communication n'est pas établie, il est possible qu'un dispositif mobile ne soit pas enregistré.
- Afficher le programme correctif du dispositif mobile et l'état de la mise à jour des composants :
  - **Versión actuelle**—le numéro de la version actuelle de l'agent de dispositif mobile ou des composants sur le Mobile Security serveur d'administration
  - **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
  - **Versión actuelle**—le numéro de la version actuelle des modules du serveur d'administration 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 du débridage du dispositif mobile :
    - **Débridé**— le nombre de dispositifs mobiles débridés
    - **Non débridé**—le nombre de dispositifs mobiles non débridés
  - Afficher l'état du 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 **Activer** ou **Désactiver** 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.

---

## Modification de la 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 utilisateurs

Trend Micro Mobile Security vous permet de configurer l'authentification des utilisateurs basée sur Active Directory (AD) ou par le biais d'une clé d'inscription.

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

**TABEAU 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

<b>COMPOSANTS DU SERVEUR</b>	<b>AUTORISATIONS</b>	<b>SUPER ADMINISTRATEUR</b>	<b>ADMINISTRATEUR DE GROUPE</b>
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 de 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 et prénom** : nom complet de l'utilisateur.

- **Mot de passe** (et **Confirmez le mot de passe**).
- **Adresse de messagerie** : 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 dans la liste de gauche, puis cliquez sur **>** pour le déplacer vers la liste **Utilisateurs sélectionnés** sur la droite.



#### **Remarque**

Pour supprimer l'utilisateur de la liste **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 le rôle dans **Choisir le rôle d'administrateur : 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 de 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 et prénom** : nom complet de l'utilisateur.
    - **Adresse de messagerie** : 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 modifier le mot de passe du compte utilisateur, saisissez le nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**, puis cliquez sur **Enregistrer**.
  - **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 de 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 de 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 d'administration 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 d'administration 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.

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

## Configuration de la programmation de la suppression d'anciennes commandes

### Procédure

1. Cliquez sur **Administration > Gestion de la file de commandes**.  
L'écran **Gestion de la file de commandes** s'affiche.
2. Dans l'onglet **Maintenance de la file de commandes**, sélectionnez **Activer la suppression programmée des commandes**.
3. Indiquez le nombre d'anciennes commandes à supprimer.
4. Indiquez la fréquence et l'heure de suppression de la file de commandes.

5. Cliquez sur **Enregistrer**.
- 

## Suppression manuelle d'anciennes commandes

---

### Procédure

1. Cliquez sur **Administration > Gestion de la file de commandes**.  
L'écran **Gestion de la file de commandes** s'affiche.
  2. Dans l'onglet **Maintenance de la file de commandes**, sélectionnez **Activer la suppression programmée des commandes**.
  3. Indiquez le nombre d'anciennes commandes à supprimer.
  4. Cliquez sur **Supprimer maintenant**.
- 

## 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 d'administration Mobile Security.
  - **Port HTTPS**—numéro de port HTTPS du serveur d'administration Mobile Security pour la console Web d'administration.
- 

## Gestion des certificats

Utilisez l'écran **Gestion des certificats** pour charger les certificats .pfx, .p12, .cer, .crt, .der sur le serveur d'administration 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 à la page 3-3*
- *Gestion des groupes à la page 3-4*
- *Gestion des dispositifs mobiles à la page 3-6*
- *État du dispositif mobile à la page 3-11*
- *Tâches de l'agent de dispositif mobile à la page 3-14*
- *Mise à jour des agents de dispositif mobile à la page 3-14*
- *Protection contre la perte du dispositif à la page 3-15*
- *Réinitialisation du mot de passe à distance à la page 3-19*
- *Onglet Dispositifs invités à la page 3-23*
- *Onglet Dispositifs Exchange ActiveSync à la page 3-26*
- *Onglet Programme d'inscription des appareils à la page 3-29*

- *Intégration avec Trend Micro Control Manager à la page 3-33*

## 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 d'administration 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 d'administration Mobile Security crée automatiquement ce groupe si **Authentification du périphérique** 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 ».
- **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 d'administration 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. Configurez ce qui suit :
  - **Groupe parent** : sélectionnez le groupe pour lequel vous voulez créer un sous-groupe.
  - **Nom de groupe** : saisissez le nom du groupe.
  - **Stratégie** : sélectionnez la stratégie dans la liste déroulante que vous voulez appliquer au groupe.

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 boîte 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 :
      - **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 :

adresse\_messagerie, nom\_dispositif, nom\_groupe, numéro\_actif  
(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 courriel d'invitation aux utilisateurs des dispositifs invités.

## Modification du nom d'utilisateur d'un dispositif mobile

Contexte de la tâche en cours

---

### 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 **Changer d'utilisateur**, puis modifiez le nom d'utilisateur dans le champ prévu à cet effet.
  5. Cliquez sur **Enregistrer**.
- 

## 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.
  - **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 3-9*
- *Suppression de plusieurs dispositifs mobiles à la page 3-10*

### 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 boîte de dialogue de confirmation.
- 

Le dispositif mobile est supprimé de l'arborescence des dispositifs mobiles, et n'est plus inscrit sur le serveur d'administration 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 d'administration 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 MEID, les informations relatives à la version du micrologiciel ainsi que la dernière sauvegarde iCloud.
- **Sécurité** : affiche l'état de chiffrement du dispositif mobile, le compte iTunes actif 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 Wi-Fi, les informations détaillées relatives au réseau, comprenant le nom du réseau du fournisseur, la version des paramètres, le statut d'itinérance, les informations relatives aux indicatifs de pays pour les mobiles (MCC) et codes de réseau mobile (MNC) ainsi que l'état du partage de connexion.
- **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.
- **Informations sur Samsung KNOX** : affiche des informations supplémentaires sur les dispositifs mobiles qui prennent en charge Samsung KNOX.

## 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
  - **IMEI** : numéro IMEI d'un dispositif mobile.
  - **Numéro de série** : numéro de série d'un dispositif mobile
  - **Adresse Wi-Fi MAC** : adresse Wi-Fi MAC d'un dispositif mobile
  - **Description** —description d'un dispositif mobile
  - **Système d'exploitation** : limite la recherche au système d'exploitation spécifique sur lequel le dispositif mobile est exécuté ou au numéro de version pour Android et iOS.
  - **Groupe**—groupe auquel appartient le dispositif mobile
  - **Versión 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
  - **Nom d'application** : application installée sur les dispositifs mobiles
  - **Agent de dispositif mobile désinstallé par l'utilisateur** : limite la recherche aux dispositifs mobiles desquels l'agent de dispositif mobile est désinstallé par l'utilisateur
  - **Dispositif mobile associé à une racine** : limite la recherche aux dispositifs mobiles associés à une racine
  - **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.



## 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 d'administration affiche la localisation du dispositif mobile sur Google Maps.



#### Remarque

Cette fonctionnalité est uniquement disponible pour les dispositifs mobiles Android et 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. 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 boîte de dialogue de confirmation.

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

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 fonctionnalité est prise en charge uniquement sur les dispositifs mobiles Android et 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. Dans l'onglet **Dispositifs administrés**, cliquez sur le dispositif mobile que vous souhaitez verrouiller dans l'arborescence des dispositifs.
4. Effectuez l'une des actions suivantes :

Pour un dispositif mobile Android, cliquez sur **Verrouillage à distance**, puis sur **OK** dans la boîte de dialogue de confirmation.

Pour un dispositif mobile iOS, cliquez sur **Verrouillage à distance**, puis saisissez le message que vous voulez envoyer à l'utilisateur, le numéro de téléphone de l'utilisateur et enfin cliquez sur **Verrouiller**.

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



### AVERTISSEMENT!

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

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



### Remarque

Cette fonctionnalité est prise en charge uniquement sur les dispositifs mobiles Android, iOS et Windows Phone.

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 3-28](#).

### 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.**—Également connu comme "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.**
- Pour les dispositifs mobiles Windows Phone, sélectionnez les 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.)

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 mobiles Android et iOS.

---

## 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.
- 

## Gestion de Samsung KNOX Workspace à distance

Vous pouvez envoyer des commandes pour gérer des espaces de travail Samsung KNOX à partir de la console Web d'administration Mobile Security. Ces commandes incluent la création d'un conteneur, la suppression d'un conteneur, le verrouillage d'un conteneur, le déverrouillage d'un conteneur et la réinitialisation du mot de passe d'un conteneur. Cette fonction est disponible pour les dispositifs mobiles Samsung 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**, sélectionnez un dispositif mobile Samsung que vous souhaitez gérer dans l'arborescence des dispositifs.
4. Effectuez l'une des actions suivantes :
  - Pour créer un espace de travail KNOX sur le dispositif mobile, cliquez sur **Opérations KNOX > Créer un conteneur**.
  - Pour supprimer l'espace de travail sur le dispositif mobile, cliquez sur **Opérations KNOX > Supprimer le conteneur**.
  - Pour permettre à un utilisateur de réinitialiser le mot de passe de l'espace de travail, cliquez sur **Opérations KNOX > Réinitialiser le mot de passe**.
  - Pour verrouiller l'espace de travail sur le dispositif mobile, cliquez sur **Opérations KNOX > Verrouiller le conteneur**.

- Pour déverrouiller l'espace de travail sur le dispositif mobile, cliquez sur **Opérations KNOX > Déverrouiller le conteneur.**
- 

## Modification des paramètres iOS à distance

Vous pouvez modifier les paramètres du dispositif mobile iOS à distance à partir de la console Web d'administration. Ces paramètres incluent l'itinérance données, l'itinérance voix et le partage de connexion.

---

### 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**, sélectionnez un dispositif mobile iOS que vous souhaitez gérer dans l'arborescence des dispositifs.
4. Effectuez l'une des actions suivantes :
  - Pour activer l'itinérance des données, cliquez sur **Opérations iOS > Activer l'itinérance des données.**
  - Pour désactiver l'itinérance données, cliquez sur **Opérations iOS > Désactiver l'itinérance données.**
  - Pour activer l'itinérance voix, cliquez sur **Opérations iOS > Activer l'itinérance voix.**
  - Pour désactiver l'itinérance voix, cliquez sur **Opérations iOS > Désactiver l'itinérance voix.**
  - Pour activer le partage de connexion, cliquez sur **Opérations iOS > Activer le partage de connexion.**
  - Pour désactiver le partage de connexion, cliquez sur **Opérations iOS > Désactiver le partage de connexion.**

- Pour démarrer la mise en miroir AirPlay, cliquez sur **Opérations iOS > Demander la mise en miroir AirPlay**.
  - Pour arrêter la mise en miroir AirPlay, cliquez sur **Opérations iOS > Arrêter la mise en miroir AirPlay**.
- 

## Exportation de données

Vous pouvez exporter les données pour une analyse approfondie ou une sauvegarde à partir de l'onglet **Dispositifs gérés** de 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. Sélectionnez dans l'arborescence des dispositifs le groupe de dispositifs mobiles dont vous souhaitez exporter les données.
  4. Cliquez sur **Exporter**.
  5. En cas de besoin, cliquez sur **Enregistrer** dans la fenêtre contextuelle qui apparaît pour enregistrer le fichier .zip sur votre ordinateur.
  6. Faites une extraction du contenu du fichier téléchargé .zip et ouvrez le fichier .csv pour afficher les informations du dispositif mobile.
- 

## Envoi de messages aux dispositifs mobiles

Vous pouvez envoyer un SMS à un utilisateur ou à un groupe à partir de l'onglet **Dispositifs gérés** de l'écran **Dispositifs**.

---

### Procédure

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



2. Cliquez sur **Dispositifs** dans la barre de menu.  
L'écran **Dispositifs** apparaît.
  3. Dans l'arborescence du dispositif, sélectionnez le dispositif mobile ou le groupe de dispositifs auquel vous voulez envoyer un SMS.
  4. Cliquez sur **Envoyer un message**.  
L'écran **Envoyer un SMS** s'ouvre.
  5. Saisissez votre message dans le champ fourni, puis cliquez sur **Envoyer**.
- 

## Onglet Dispositifs invités

L'onglet **Dispositifs invités** de l'écran **Dispositifs** enregistre les invitations d'inscription envoyées par Mobile Security aux dispositifs mobiles.

Par défaut, le courriel d'invitation comprend 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.
Utilisée	<p>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.</p> <hr/> <p> <b>Remarque</b> Ce état ne s'affiche que lorsque l'<b>option de limitation d'utilisation de clé d'inscription</b> est définie à <b>Utiliser une seule fois</b> dans les paramètres d'inscription de dispositifs.</p>
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 de serveur Exchange sur le serveur d'administration 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 des e-mails à l'utilisateur du dispositif mobile invité. Une fois le dispositif mobile inscrit sur le serveur d'administration 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 boîte 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

---



### **AVERTISSEMENT!**

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

---

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.

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 3-17*.

---

### **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.

- 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 d'administration Mobile Security ne sera plus en mesure d'accéder au serveur Exchange. 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 d'administration Mobile Security.

---

### Procédure

- Connectez-vous à la console d'administration Mobile Security.
  - Cliquez sur **Dispositifs** dans la barre de menu.  
L'écran **Dispositifs** apparaît.
  - Cliquez sur l'onglet **Dispositifs Exchange ActiveSync**.
  - Sélectionnez les dispositifs mobiles que vous souhaitez supprimer de la liste.
  - Cliquez sur **Supprimer**, puis cliquez sur **OK** sur l'écran de confirmation.
- 

## Onglet Programme d'inscription des appareils

Le Programme d'inscription des appareils (DEP) offre une manière rapide et simple de déployer les dispositifs mobiles iOS appartenant à l'entreprise. Vous pouvez inscrire votre entreprise au programme DEP.

Trend Micro Mobile Security s'intègre au Programme d'inscription des appareils d'Apple afin de simplifier l'enregistrement des dispositifs mobiles iOS 7 et iOS 8 professionnels

achetés directement auprès d'Apple. Si vous avez configuré l'intégration au Programme d'inscription des appareils, les utilisateurs qui se voient remettre des dispositifs mobiles iOS appartenant à l'entreprise sont invités à s'enregistrer auprès de Mobile Security lorsqu'ils configurent le dispositif mobile à l'aide du processus d'activation iOS.

L'intégration de Mobile Security au Programme d'inscription des appareils vous permet d'éviter d'avoir à communiquer les instructions d'inscription aux utilisateurs tout en garantissant que tous les dispositifs mobiles sont enregistrés lors de leur première utilisation. En outre, cette intégration supprime les frais de prise en charge associés.

## Expérience utilisateur du Programme d'inscription des appareils

Si vous configurez l'intégration de Mobile Security au Programme d'inscription des appareils Apple, la marche à suivre pour les utilisateurs sera la suivante :

- Un utilisateur reçoit un nouveau dispositif mobile iOS de son entreprise, le déballe et l'allume.
- Le dispositif mobile se connecte à Apple.
- Grâce à l'identifiant du dispositif mobile, les serveurs Apple détectent que l'appareil a été ajouté à votre compte Programme d'inscription des appareils et envoient les paramètres de l'appareil et les informations de connexion pour le déploiement de Mobile Security.
- L'utilisateur fait alors appel à l'assistant d'installation iOS pour terminer l'activation initiale du dispositif mobile, notamment l'inscription à Mobile Security.

Vous pouvez déterminer les écrans qui apparaissent dans l'assistant d'installation iOS lorsque vous configurez l'intégration au Programme d'inscription des appareils. Ceci vous permet de simplifier le processus d'activation en ignorant les écrans consacrés aux paramètres que vous avez configurés via la gestion des dispositifs. Par exemple, si vous comptez configurer l'activation des services de localisation sur les dispositifs comme partie de la configuration de géorepérage, vous pouvez configurer l'assistant d'installation iOS pour qu'il ignore l'écran permettant aux utilisateurs d'activer ou non ces services de localisation.

Dans le cadre du processus d'activation du dispositif, l'utilisateur est invité à s'inscrire à Mobile Security. Il n'est pas nécessaire que l'utilisateur saisisse ses informations



d'authentification ou son adresse e-mail, ni qu'il connaisse les détails de la connexion à Mobile Security. Un profil spécifique de Programme d'inscription des appareils créé automatiquement par l'administrateur lorsque vous configurez l'intégration au DEP est déployé sur le dispositif.

## Configuration de Mobile Security pour le Programme d'inscription des appareils

Avant de pouvoir configurer Mobile Security pour le Programme d'inscription des appareils (DEP), assurez-vous d'avoir inscrit préalablement votre organisation au programme DEP sur le site Web Apple suivant :

<http://deploy.apple.com/>

---

### Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.  
L'écran **Dispositifs** s'ouvre.
3. Cliquez sur l'onglet **Programme d'inscription des appareils**.
4. Cliquez sur **Paramètres**.
5. Cliquez sur le lien **Télécharger** devant **Clé publique** afin de télécharger la clé publique sur l'ordinateur local à partir du serveur d'administration Mobile Security.
6. Cliquez sur le lien **Programmes de déploiement Apple** devant **Déploiement**.  
Le portail Web **Programmes de déploiement Apple** s'ouvre dans le navigateur Internet.
7. Connectez-vous à votre compte **Programme d'inscription des appareils** et créez un nouveau serveur MDM à l'aide de la clé publique téléchargée depuis le serveur d'administration Mobile Security. Consultez le document suivant pour obtenir les étapes détaillées de l'inscription au Programme d'inscription des appareils.

[https://www.apple.com/iphone/business/docs/DEP\\_Business\\_Guide\\_EN\\_Feb14.pdf](https://www.apple.com/iphone/business/docs/DEP_Business_Guide_EN_Feb14.pdf)

8. Sur le serveur MDM, générez un jeton d'accès et enregistrez le fichier de jeton sur un emplacement adéquat. Ensuite attribuez les dispositifs mobiles pour l'inscription sur le serveur MDM.
9. Chargez le fichier de jeton généré via le portail Web **Programmes de déploiement d'Apple** sur le serveur d'administration Mobile Security. Patientez jusqu'à la fin du chargement.

Lorsque le chargement est terminé, l'écran **Paramètres du Programme d'inscription des appareils** s'ouvre.

10. Sous la section **Détails du Programme d'inscription des appareils**, configurez les paramètres suivants du profil d'installation pour les dispositifs mobiles.
  - **Nom de profil** : nom du profil d'installation affiché sur le dispositif mobile.
  - **Supervision requise** : pour placer les dispositifs mobiles inscrits via le Programme d'inscription des appareils en mode supervisé.
  - **Configuration amovible** : permet aux utilisateurs de supprimer la configuration de gestion du dispositif des dispositifs inscrits via le Programme d'inscription des appareils.
  - **Autoriser le couplage** : permet que les dispositifs inscrits via le Programme d'inscription des appareils soient gérés via les outils Apple tels qu'iTunes et Apple Configurator.
  - **Configuration obligatoire** : permet d'empêcher que les utilisateurs ignorent l'étape d'inscription de Mobile Security lors du processus d'activation du dispositif.
  - **Unité commerciale** : nom du département auquel le dispositif mobile est attribué.
  - **Identifiant de service unique** : si vous devez effectuer plusieurs déploiements de Mobile Security, dans la case Identifiant de service unique, saisissez un nom qui identifie de façon unique le déploiement que vous êtes en train de configurer.
  - **Numéro de téléphone de l'assistance** : numéro de téléphone que les utilisateurs peuvent appeler pour obtenir de l'aide.

- **Éléments de configuration requis** : éléments devant être configurés par les utilisateurs. Par défaut, tous les éléments de configuration sont requis. Si vous désactivez l'un de ces éléments, les utilisateurs pourront l'ignorer au cours de la configuration.

#### 11. Cliquez sur **Enregistrer**.

Le serveur d'administration Mobile Security synchronise la liste des dispositifs mobiles avec le serveur des Programmes de d'inscription des appareils d'Apple et affiche les dispositifs mobiles sur l'onglet **Programme d'inscription des appareils** de l'écran **Dispositifs**.

---

## Intégration avec Trend Micro Control Manager

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

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

Pour des informations détaillées sur le gestionnaire de contrôle Trend Micro Control Manager et la gestion des stratégies de Mobile Security dans 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 Control Manager

La console Web de Trend Micro Control Manager 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 de Control Manager peut modifier une stratégie à tout moment et la stratégie sera déployée sur les dispositifs mobiles immédiatement.

Trend Micro Control Manager 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 de Control Manager, la stratégie sera renvoyée aux paramètres d'origine ou créée à nouveau après la synchronisation.

## États des stratégies de sécurité dans Control Manager

Sur la console Web de Trend Micro Control Manager, les états suivants relatifs aux stratégies de sécurité sont affichés :

- **En attente** : la stratégie est créée sur la console Web de Control Manager 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 les stratégies de sécurité sur les dispositifs mobiles d'un groupe Mobile Security. Vous pouvez utiliser les stratégies relatives à la mise en service, à la sécurité des dispositifs et à la protection des données.

Le chapitre contient les sections suivantes :

- *À propos des stratégies de sécurité à la page 4-3*
- *Gestion des stratégies à la page 4-6*
- *Stratégie courante à la page 4-10*
- *Stratégie WiFi à la page 4-11*
- *Stratégie Exchange ActiveSync à la page 4-11*
- *Stratégie VPN à la page 4-12*
- *Stratégie du proxy HTTP global à la page 4-12*
- *Stratégie des certificats à la page 4-12*
- *Stratégie d'authentification unique à la page 4-12*
- *Stratégie AirPlay/AirPrint à la page 4-13*

- *Stratégie de réseau cellulaire à la page 4-14*
- *Stratégie de thème à la page 4-14*
- *Stratégie de domaine géré à la page 4-14*
- *Stratégie de protection contre les programmes malveillants à la page 4-15*
- *Stratégie de prévention anti-spam à la page 4-16*
- *Stratégie de filtrage des appels à la page 4-19*
- *Stratégie de protection contre les menaces Internet à la page 4-21*
- *Stratégie de protection de la confidentialité à la page 4-22*
- *Stratégie de mot de passe à la page 4-22*
- *Stratégie de verrouillage des fonctions à la page 4-23*
- *Stratégie de compatibilité à la page 4-23*
- *Stratégie de surveillance et de contrôle des applications à la page 4-24*
- *Stratégie du programme d'achats en volume à la page 4-26*
- *Stratégie de conteneur à la page 4-27*

## À propos des stratégies de sécurité

Vous pouvez configurer les stratégies de sécurité d'un groupe Mobile Security sur le serveur d'administration. Ces stratégies s'appliquent à tous les dispositifs mobiles du groupe. Vous pouvez appliquer les stratégies de sécurité à tous les groupes Mobile Security en sélectionnant le groupe **Dispositifs mobiles** (le 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 STRATÉGIE	STRATÉGIE	RÉFÉRENCE
Généralités	Stratégie courante	Voir la section <a href="#">Stratégie courante à la page 4-10</a> .

<b>GROUPE DE STRATÉGIE</b>	<b>STRATÉGIE</b>	<b>RÉFÉRENCE</b>
Mise en service	Stratégie WiFi	Voir la section <a href="#">Stratégie WiFi à la page 4-11</a> .
	Stratégie Exchange ActiveSync	Voir la section <a href="#">Stratégie Exchange ActiveSync à la page 4-11</a> .
	Stratégie VPN	Voir la section <a href="#">Stratégie VPN à la page 4-12</a> .
	Stratégie du proxy HTTP global	Voir la section <a href="#">Stratégie du proxy HTTP global à la page 4-12</a> .
	Stratégie des certificats	Voir la section <a href="#">Stratégie des certificats à la page 4-12</a> .
	Stratégie d'authentification unique	Voir la section <a href="#">Stratégie d'authentification unique à la page 4-12</a> .
	Stratégie AirPlay/AirPrint	Voir la section <a href="#">Stratégie AirPlay/AirPrint à la page 4-13</a> .
	Stratégie de réseau cellulaire	Voir la section <a href="#">Stratégie de réseau cellulaire à la page 4-14</a> .
	Stratégie de thème	Voir la section <a href="#">Stratégie de thème à la page 4-14</a> .



GROUPE DE STRATÉGIE	STRATÉGIE	RÉFÉRENCE
Sécurité de dispositif	Stratégie de protection contre les programmes malveillants	Voir la section <i>Stratégie de protection contre les programmes malveillants à la page 4-15.</i>
	Stratégie de prévention anti-spam	Voir la section <i>Stratégie de prévention anti-spam à la page 4-16.</i>
	Stratégie de filtrage des appels	Voir la section <i>Stratégie de filtrage des appels à la page 4-19.</i>
	Stratégie de protection contre les menaces Internet	Voir la section <i>Stratégie de protection contre les menaces Internet à la page 4-21.</i>
Dispositifs	Voir la section <i>Stratégie de mot de passe à la page 4-22.</i>	Voir la section <i>Stratégie de mot de passe à la page 4-22.</i>
	Stratégie de verrouillage des fonctions	Voir la section <i>Stratégie de verrouillage des fonctions à la page 4-23.</i>
	Stratégie de compatibilité	Voir la section <i>Stratégie de compatibilité à la page 4-23.</i>
Gestion des applications	Stratégie de surveillance et de contrôle des applications	Voir la section <i>Stratégie de surveillance et de contrôle des applications à la page 4-24.</i>
	Stratégie du programme d'achats en volume :	Voir la section <i>Stratégie du programme d'achats en volume à la page 4-26.</i>
Samsung KNOX	Stratégie de conteneur	Voir la section <i>Stratégie de conteneur à la page 4-27.</i>

## 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 4-7*.

5. (Super-administrateur uniquement) Si vous voulez utiliser cette stratégie comme modèle, cliquez sur la flèche sous la colonne **Type** de l'écran **Stratégie**. Les administrateurs de groupes peuvent utiliser les modèles créés par le super-administrateur pour créer des stratégies pour les groupes qui leur sont attribués.

**Remarque**

- Vous pouvez attribuer un modèle à n'importe quel groupe.
  - Vous pouvez également convertir un modèle en stratégie. Toutefois, vous ne pouvez le faire que si le modèle n'est pas déjà attribué à un groupe.
- 

## 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 : dans la liste **Groupes disponibles** 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 : dans 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 4-7* 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**.
- 

## Configuration de la disponibilité des applications

Mobile Security vous permet de configurer les applications que vous souhaitez rendre disponibles sur des dispositifs mobiles iOS et Android pour une stratégie en particulier.

---

### 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 le nombre d'applications requises pour la stratégie, sous la colonne **Applications disponibles**.  
L'écran **Applications disponibles** s'affiche.
  4. Cliquez sur l'onglet **Applications iOS** ou **Applications Android**.
  5. Effectuez l'une des actions suivantes :
    - Pour activer ou désactiver une application, cliquez sur le bouton sous la colonne **Autorisation** pour l'application à changer.
    - Pour activer ou désactiver toutes les applications, cliquez sur **Activer tous** ou **Désactiver tous**.
  6. Changez la disponibilité d'une application dans la colonne **Autorisation**.
- 

## Stratégies de sécurité de Mobile Security

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

À l'aide du compte de super-utilisateur, vous pouvez spécifier une stratégie pour qu'elle serve de modèle aux administrateurs de groupes lors de la création d'autres stratégies de

sécurité dans Mobile Security. Cependant, une fois qu'une stratégie de sécurité est définie comme modèle, vous ne pouvez plus l'attribuer à un groupe.

## 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**.

- **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 4-16*, *Stratégie de prévention anti-spam WAP Push à la page 4-18* et *Stratégie de protection contre les menaces Internet à la page 4-21*.

- **Paramètres de mise à jour** : Vous pouvez configurer le serveur d'administration 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 d'administration Mobile Security.

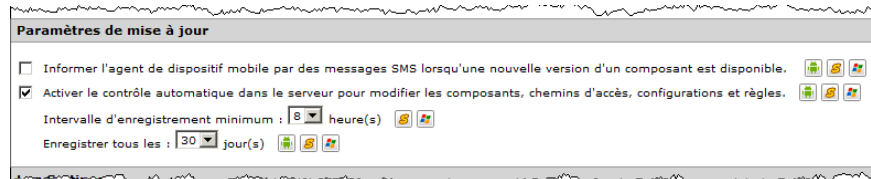


FIGURE 4-1. Stratégie courante, section des paramètres de mise à jour

- **Paramètres des journaux** : Lorsque les agents de dispositif mobile détectent un risque de sécurité, par exemple un programme malveillant sur un système d'exploitation Android, un journal est généré sur le dispositif mobile.

## Stratégie Wi-Fi

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

Les paramètres de stratégie VPN vous permettent 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'identification sur un ensemble d'applications, y compris Mobile 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 AirPlay/AirPrint

La stratégie AirPlay/AirPrint vous permet de créer des stratégies AirPlay/AirPrint pour votre organisation et de les distribuer aux dispositifs mobiles iOS.

Pour configurer les paramètres de stratégie AirPlay et/ou AirPrint, cliquez sur **Stratégies**, puis cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie AirPlay/AirPrint**.

## Stratégie de réseau cellulaire

La stratégie de réseau cellulaire vous permet de configurer des paramètres de réseau cellulaire pour votre organisation et de les distribuer aux dispositifs mobiles iOS.

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

## Stratégie de thème

Les paramètres de la stratégie de thème vous permettent de pousser une police et de définir un papier peint pour l'écran d'accueil des dispositifs mobiles iOS. Cette stratégie s'applique aux dispositifs mobiles iOS qui sont en mode surveillé.

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

## Stratégie de domaine géré

Une stratégie de domaine géré vous permet de configurer les domaines de messagerie et/ou Web gérés par votre organisation.

- Domaines de messagerie non marqués : Lorsqu'un utilisateur rédige un courriel à l'aide du client de messagerie du système, toute adresse de messagerie saisie ne correspondant pas aux domaines configurés est mise en surbrillance (marquée) en rouge. Les administrateurs doivent envisager l'utilisation de cette fonctionnalité afin d'avertir les utilisateurs susceptibles, par manque d'attention, d'envoyer des informations sensibles à des adresses de messagerie non fiables.
- Domaines Web Safari gérés : Vous pouvez indiquer la possibilité que des fichiers téléchargés depuis des domaines spécifiques utilisant Safari puissent seulement s'ouvrir à l'aide d'applications gérées. Par exemple, il est possible qu'un PDF téléchargé depuis interne.exemple.com puisse s'ouvrir avec Adobe Reader (application gérée) mais pas avec Dropbox (application non gérée). Cela permet d'améliorer la nature de conteneur de Safari et d'élargir son utilisation en tant que navigateur d'entreprise.

**Important**

Dans Stratégie de verrouillage des fonctions, vous devez désactiver les fonctionnalités iOS suivantes. Dans le cas contraire, les paramètres de domaines Web Safari gérés seront sans effet, car les fichiers téléchargés peuvent être ouverts à l'aide d'autres applications (non gérées) :

- Ouverture de documents issus d'applications gérées dans d'autres applications (version 7.0 ou supérieure)
- Ouverture de documents issus d'autres applications dans des applications gérées (version 7.0 ou supérieure)

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

## 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.

- **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**
  - **Analyser uniquement les applications installées**: Sélectionnez cette option si vous souhaitez analyser uniquement les applications installées.
  - **Analyser les applications installées et les fichiers**: Sélectionnez cette option si vous souhaitez analyser les applications installées et d'autres fichiers sur le stockage du dispositif mobile, puis choisissez si vous voulez analyser tous les fichiers ou uniquement les fichiers APK.

## 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	<p>L'utilisateur peut modifier la liste approuvée/ bloquée sur l'agent de dispositif mobile.</p> <p>Mobile Security autorise ou bloque les messages selon l'ordre de priorité suivant :</p> <ol style="list-style-type: none"> <li>1. Liste approuvée sur l'agent de dispositif mobile</li> <li>2. Liste bloquée sur l'agent de dispositif mobile</li> </ol>
Activé	Désactivé	<p>L'utilisateur peut uniquement modifier la liste approuvée/bloquée sur l'agent de dispositif mobile.</p> <p>Mobile Security autorise ou bloque les messages selon l'ordre de priorité suivant :</p> <ol style="list-style-type: none"> <li>1. Liste approuvée ou liste bloquée sur le serveur</li> <li>2. Liste approuvée sur l'agent de dispositif mobile</li> <li>3. Liste bloquée sur l'agent de dispositif mobile</li> </ol>

CONTRÔLE CENTRAL	CONTRÔLE UTILISATEUR	DESCRIPTION
Activé	Activé	<p>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.</p> <p>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.</p> <p>Mobile Security autorise ou bloque les messages selon l'ordre de priorité suivant :</p> <ol style="list-style-type: none"> <li>1. Liste approuvée sur l'agent de dispositif mobile</li> <li>2. Liste bloquée sur l'agent de dispositif mobile</li> <li>3. Liste approuvée ou liste bloquée sur le serveur</li> </ol>



#### 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.

## Stratégie de prévention anti-spam WAP Push

Cette fonction vous offre un contrôle côté serveur de prévention WAP Push. Si elle est activée, vous pouvez choisir d'utiliser ou non une liste approuvée de WAP.

**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 contenir entre 4 et 20 caractères constitués des éléments suivants : 0 à 9, +, -, #, (, ) et espaces. Le nombre d'entrées ne doit pas dépasser un maximum de 200.

La liste suivante présente les fonctions disponibles lors de la configuration des stratégies de prévention WAP Push :

- activer ou désactiver la prévention WAP Push pour le dispositif mobile
- configurer le dispositif mobile de manière à utiliser une liste approuvée ou désactiver la prévention 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 prévention 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 prévention WAP Push configurée par l'administrateur ; mais il pourra modifier la liste personnelle de prévention WAP Push du côté du dispositif mobile

**Remarque**

Les paramètres personnels de l'utilisateur relatifs aux messages de spams seront effacés une fois la stratégie de prévention anti-spam 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	<p>L'utilisateur peut modifier la liste approuvée/bloquée sur l'agent de dispositif mobile.</p> <p>Mobile Security autorise ou bloque les URL selon l'ordre de priorité suivant :</p> <ol style="list-style-type: none"> <li>1. Liste approuvée sur l'agent de dispositif mobile</li> <li>2. Liste bloquée sur l'agent de dispositif mobile</li> </ol>
Activé	Désactivé	<p>L'utilisateur peut uniquement modifier la liste approuvée/bloquée sur l'agent de dispositif mobile.</p> <p>Mobile Security autorise ou bloque les appels entrants selon l'ordre de priorité suivant :</p> <ol style="list-style-type: none"> <li>1. Liste bloquée sur le serveur</li> <li>2. Liste approuvée sur l'agent de dispositif mobile</li> <li>3. Liste bloquée sur l'agent de dispositif mobile</li> </ol> <p>Vous pouvez également configurer le contrôle côté serveur pour les appels sortants sur les dispositifs mobiles Android.</p>



CONTRÔLE CENTRAL	CONTRÔLE UTILISATEUR	DESCRIPTION
Activé	Activé	<p>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.</p> <p>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.</p> <p>Mobile Security autorise ou bloque les appels entrants selon l'ordre de priorité suivant :</p> <ol style="list-style-type: none"> <li>1. Liste approuvée sur l'agent de dispositif mobile</li> <li>2. Liste bloquée sur l'agent de dispositif mobile</li> <li>3. Liste bloquée sur le serveur</li> </ol> <p>Vous pouvez également configurer le contrôle côté serveur pour les appels sortants sur les dispositifs mobiles Android.</p>



### 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 protection contre les menaces Internet


Vous permet de gérer la stratégie de protection contre les menaces Internet depuis le serveur d'administration Mobile Security et la déploie sur les dispositifs mobiles Android et iOS. Cette fonctionnalité permet également aux dispositifs mobiles 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 cliquez sur le nom de la stratégie, et enfin cliquez sur **Stratégie protection contre les menaces Internet**.

## Stratégie de protection de la confidentialité

Vous pouvez activer les paramètres de protection de la confidentialité afin que les utilisateurs puissent effectuer les tâches suivantes sur leurs dispositifs :

**TABLEAU 4-4. Paramètres de la stratégie de protection de la confidentialité**

TÂCHES	ANDROID	iOS
Effectuer manuellement une analyse de la confidentialité	●	
Charger automatiquement les journaux d'analyse de la confidentialité sur le serveur d'administration Mobile Security	●	
Configurer les paramètres de confidentialité Facebook	●	●
 <b>Remarque</b> Activer l' <b>analyse Facebook</b> permet aux utilisateurs de protéger leurs informations et de vérifier qu'ils ne partagent des données qu'avec des personnes de confiance.		

Pour configurer la stratégie de protection de la confidentialité, accédez à **Stratégies** > <Nom de stratégie> > **Stratégie de protection de la confidentialité**.

## Stratégie de mot de passe

La stratégie de mot de passe empêche tout accès non autorisé aux données contenues sur les dispositifs mobiles.

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

## 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 *Fonctions des dispositifs mobiles OS prises en charge à la page 1-25* pour la liste des fonctions/composants pris en charge.



### 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.

## 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 cliquez sur le nom de la stratégie, et enfin cliquez 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 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 autorisera toutes les autres.

- **Activer le blocage des applications du système** (Android uniquement):  
si ce paramètre est sélectionné, Mobile Security bloquera 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 utiliser l'exception en ajoutant à la liste approuvée ou bloquée les applications qui appartiennent à ces catégories. Par exemple, si vous avez désactivé une catégorie de type Jeux, Mobile Security bloquera toutes les applications qui appartiennent à cette catégorie, en dehors de celles qui figurent dans la liste approuvée.

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

1. **Liste approuvée**—Mobile Security autorise les applications figurant sur la liste approuvée, même si elles appartiennent à la catégorie que vous avez désactivée.
  2. **Liste bloquée**—Mobile Security bloque les applications figurant sur la liste bloquée, même si elles appartiennent à la catégorie que vous avez activée.
  3. **Permissions d'applications**—Mobile Security autorise ou bloque les applications en fonction de l'état de permission que vous avez sélectionné pour la catégorie à laquelle elles appartiennent.
- **Activer Autorisations d'applications** (pour Android uniquement) : sélectionnez les services d'applications que vous souhaitez activer ou désactiver sur les dispositifs mobiles Android. Vous pouvez aussi utiliser l'exception en ajoutant les applications qui utilisent ces services à la liste approuvée ou bloquée. Par exemple, si vous avez désactivé un service du type **Lire les données**, Mobile Security bloquera toutes les applications qui utilisent le service Lire les données, en dehors des application qui figurent dans la liste approuvée.

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

1. **Liste approuvée**—Mobile Security autorise les applications qui figurent sur la liste approuvée, même si elles utilisent les services que vous avez désactivés.
  2. **Liste bloquée**—Mobile Security bloque les applications qui figurent sur la liste bloquée, même si elles utilisent les services que vous avez activés.
  3. **Permissions d'applications**—Mobile Security autorise ou bloque les applications en fonction de l'état de permission 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 contextuel sur les dispositifs mobiles Android si des applications qui ne figurent pas sur la liste approuvée sont détectées.
- Sur les dispositifs mobiles iOS, si Mobile Security détecte une application qui ne figure pas dans la liste approuvée, 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 contextuel sur les dispositifs mobiles Android si des applications qui figurent sur la liste bloquée sont détectées.
  - Sur les dispositifs mobiles iOS, si Mobile Security détecte une application qui figure dans la liste bloquée, Mobile Security envoie une notification par e-mail à l'utilisateur.
- **Verrouiller à l'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 collecte des informations** dans **Administration > Paramètres de serveur de communication > Paramètres courants (onglet)**, ou
- lors de la mise à jour des paramètres de **Fréquence de collecte des informations** dans **Administration > Paramètres de serveur de communication > Paramètres courants (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.

## Stratégie de conteneur

Cette stratégie vous permet de gérer les paramètres de sécurité d'un conteneur Samsung KNOX. Vous pouvez configurer une liste approuvée ou une liste bloquée pour des comptes, appliquer des restrictions et configurer des paramètres de navigateur, de mot de passe ou d'application.



### Remarque

Vous devez configurer une licence KNOX dans Mobile Security avant d'activer cette stratégie. Pour configurer la licence KNOX, accédez à **Administration > Licence du produit** sur la console Web d'administration.

---

- **Paramètres du compte** : Indiquez les comptes qui peuvent être ajoutés ou restreints sur les conteneurs Samsung KNOX à l'aide de listes approuvées et/ou bloquées.
- **Paramètres de restriction** : Désactivez la caméra ou le partage de fichiers sur les conteneurs Samsung KNOX.
- **Paramètres du navigateur** : Configurez les paramètres de sécurité pour le navigateur Web natif Android sur les conteneurs Samsung KNOX.
- **Paramètres de mot de passe** : Configurez les paramètres de sécurité par mot de passe pour un conteneur Samsung KNOX.

- **Paramètres de l'application** : Configurez les listes suivantes :
  - **Filtrer les listes d'applications** : Configurez les listes approuvées ou bloquées pour limiter l'installation d'applications sur un conteneur Samsung KNOX.
  - **Applications requises** : Configurez la liste des applications requises pour indiquer les applications qui doivent être installées sur Samsung KNOX.
  - **Désactiver les applications** : Configurez la liste des applications à désactiver pour désactiver certaines applications sur le dispositif mobile. Si les applications de cette liste sont installées sur le dispositif mobile, elles ne seront pas supprimées, mais elles ne pourront pas être utilisées.

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



# 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 à la page 5-2*
- *Gestion des applications d'entreprise à la page 5-2*
- *Gestion des catégories d'applications à la page 5-5*
- *Gestion des applications achetées via le Programme d'achats en volume à la page 5-7*

# 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) **Veillez 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 4-26](#) 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 boîte 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.
-

## Gestion des applications achetées via le Programme d'achats en volume

Apple utilise des codes de téléchargement et les licences du Programme d'achats en volume (VPP) pour l'achat en volume d'applications. Étant donné que vous ne pouvez pas convertir les codes de téléchargement en licences VPP, Mobile Security prend en charge ces deux options.

Le programme d'achats en grande quantité vous permet de distribuer des licences VPP aux utilisateurs ou aux dispositifs pour les applications iOS.

Vous pouvez gérer les applications VPP en surveillant le nombre de licences restantes et en récupérant des licences. Les utilisateurs peuvent employer les applications VPP, même s'ils n'ont pas encore installé l'application cliente Mobile Security sur leurs dispositifs mobiles.



### Remarque

Mobile Security n'enverra pas les applications VPP sur les dispositifs mobiles. Les utilisateurs doivent les télécharger manuellement sur leurs dispositifs mobiles depuis l'App Store d'Apple à l'emplacement suivant : **App Store** > **Mise à jour** > **Achetée**.

---



### Important

VPP n'est disponible que dans certaines régions. Assurez-vous que votre entreprise en fait partie. Consultez le lien suivant pour obtenir plus de détails :

<http://www.apple.com/business/vpp/>

---

## Configuration des licences du Programme d'achats en volume (VPP)

---

### Procédure

1. Accédez à l'URL suivante :

<http://www.apple.com/business/vpp/>

2. Connectez-vous à l'aide de votre compte Apple et téléchargez le fichier de jeton de service depuis le portail Web du Programme d'achats en volume (VPP) d'Apple.
  3. Connectez-vous à la console d'administration Mobile Security.
  4. Cliquez sur **Banque d'applications** dans la barre de menu.  
L'écran **Banque d'applications d'entreprise** s'affiche.
  5. Cliquez sur l'onglet **Applications iOS > Gestion du programme d'achats en volume (VPP) > Paramètre VPP**.
  6. Chargez le fichier de jeton que vous avez téléchargé du portail Internet d'Apple dans le champ adéquat, puis patientez jusqu'à la fin du chargement.
  7. Cliquez sur **Synchroniser maintenant**.
- 

## Attribution ou récupération de licences VPP

Mobile Security vous permet d'attribuer ou de récupérer des licences d'applications achetées via le programme d'achats en grande quantité aux utilisateurs ou aux dispositifs.



### Important

Avant de pouvoir attribuer ou récupérer des applications, assurez-vous que les licences du programme d'achats en grande quantité sont prêtes.

Pour plus d'informations, reportez-vous à [Configuration des licences du Programme d'achats en volume \(VPP\) à la page 5-7](#).

---

### Procédure

1. Accédez à **App Store > Application iOS > Gestion du VPP (programme d'achats en grande quantité)**.
2. Dans la **Liste d'applications**, identifiez l'application puis cliquez sur **Attribuer/récupérer**.  
L'écran **Attribuer/récupérer des licences** s'affiche.
3. Pour attribuer une licence, suivez la procédure suivante :



- Attribution d'une licence à un dispositif :
  - a. Dans l'onglet **Dispositifs**, sélectionnez un ou plusieurs dispositifs dans l'état **Non attribué**.
  - b. Cliquez sur **Attribuer**.

**Remarque**

Le programme d'achats en grande quantité impose les limitations suivantes lors de l'attribution d'applications aux dispositifs :

- Vous ne pouvez attribuer que des applications VPP à des dispositifs fonctionnant sous iOS 9 ou une version ultérieure.
- Les développeurs d'applications doivent activer l'attribution de dispositif.

- 
- Attribution d'une licence à un utilisateur :
    - a. Dans l'onglet **Utilisateurs**, sélectionnez un ou plusieurs utilisateurs dans l'état **Non attribué**.
    - b. Cliquez sur **Attribuer**.

**Remarque**

Mobile Security envoie une notification aux utilisateurs lorsqu'une licence VPP est attribuée.

Pour modifier les paramètres de notification utilisateur, accédez à **Notification & rapports > Notifications utilisateur > Notification utilisateur du VPP**.

---

Les licences sont bien attribuées.

4. Pour récupérer une licence, suivez la procédure suivante :
  - Récupération d'une licence à partir d'un dispositif :
    - a. Dans l'onglet **Dispositifs**, sélectionnez un ou plusieurs dispositifs dans l'état **Attribué**.
    - b. Cliquez sur **Récupérer**.
  - Récupération d'une licence à partir d'un utilisateur :

- a. Dans l'onglet **Utilisateurs**, sélectionnez un ou plusieurs utilisateurs dans l'état **Attribué**.
- b. Cliquez sur **Récupérer**.

Les licences sont bien récupérées.

---

## Vérification de l'état des utilisateurs VPP

---

### 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**.
  4. Cliquez sur l'onglet **Applications iOS > Gestion du programme d'achats en volume (VPP) > Liste des utilisateurs VPP**.
  5. Dans la colonne **État**, vous pouvez voir l'état des utilisateurs. La colonne **État** peut afficher l'un des états suivants :
    - - : vous n'avez pas encore attribué d'application à cet utilisateur.
    - **Enregistré** : vous avez attribué au moins une application à l'utilisateur, mais celui-ci n'a pas encore associé l'identifiant Apple à l'adresse de messagerie.
    - **Associé** : vous avez attribué au moins une application à l'utilisateur et celui-ci a déjà associé l'identifiant Apple à l'adresse de messagerie.
    - **Retiré** : vous avez récupéré toutes les licences attribuées à cet utilisateur.
- 

## Récupération de toutes les licences d'un utilisateur

Mobile Security vous permet de récupérer toutes les licences d'un utilisateur.

---

### 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**.
  4. Cliquez sur l'onglet **Applications iOS > Gestion du programme d'achats en volume (VPP) > Liste des utilisateurs VPP**.
  5. Sélectionnez les utilisateurs dans la liste, puis cliquez sur **Retirer**.
  6. Cliquez sur **Fermer** dans l'écran **Liste des utilisateurs**.
-



# Chapitre 6

## Mise à jour des composants

Ce chapitre vous indique comment mettre à jour les composants de Mobile Security

Le chapitre contient les sections suivantes :

- *À propos des mises à jour de composants à la page 6-2*
- *Mise à jour des composants de Mobile Security à la page 6-2*
- *Mise à jour manuelle d'un serveur AutoUpdate local à la page 6-7*

## 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 de communication Mobile Security.
- Signatures de programmes malveillants—fichier contenant des milliers de signatures de programmes malveillants et déterminant la capacité de Mobile Security à détecter ces fichiers dangereux. Trend Micro met régulièrement à jour les fichiers de signatures pour assurer la protection contre les toutes dernières menaces.
- Programme d'installation des agents de dispositif mobile — pack d'installation de programme pour les agents de dispositif mobile.

## Mise à jour des composants de Mobile Security

Vous pouvez configurer des mises à jour manuelles ou programmées de composants sur le serveur d'administration 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 d'administration 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 **Manuel** de 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 6-5* 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**.

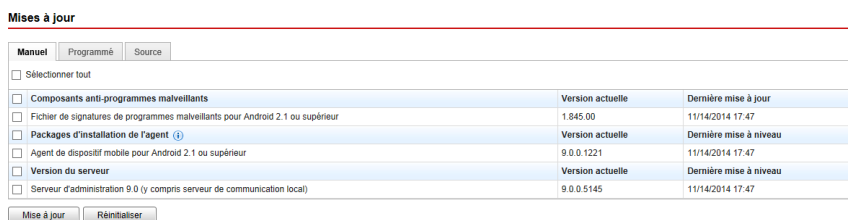


FIGURE 6-1. L'onglet Manuelles sur l'écran Mises à jour

4. Sélectionnez la case à cocher du composant à mettre à jour. Sélectionnez les cases à cocher **Composants anti-programmes malveillants**, **Packages de mise à jour 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. 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 6-5](#) 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**.

**Mises à jour**

Manuel Programmé Source

Activer la mise à jour programmée du module de gestion de Mobile Security.

<input checked="" type="checkbox"/> Composants anti-programmes malveillants	Version actuelle	Dernière mise à jour
<input checked="" type="checkbox"/> Fichier de signatures de programmes malveillants pour Android 2.1 ou supérieur	1.845.00	11/14/2014 17:47
<input checked="" type="checkbox"/> Packages d'installation de l'agent (i)	Version actuelle	Dernière mise à niveau
<input checked="" type="checkbox"/> Agent de dispositif mobile pour Android 2.1 ou supérieur	9.0.0.1221	11/14/2014 17:47
<input checked="" type="checkbox"/> Version du serveur	Version actuelle	Dernière mise à niveau
<input checked="" type="checkbox"/> Serveur d'administration 9.0 (y compris serveur de communication local)	9.0.0.5145	11/14/2014 17:47

**Programmation de mise à jour**

Toutes les heures  
 **Tous les jours**  
 Toutes les semaines, le   
 Tous les mois, le

Heure de début :   (hh:mm)

**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** 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 6-2](#) ou pour la mise à jour programmée, consultez [Mise à jour programmée à la page 6-3](#).

3. Cliquez sur l'onglet **Source**.

Vous êtes ici : Administration > [Mises à jour](#)

## Mises à jour

The screenshot shows the 'Mises à jour' (Updates) configuration page with the 'Source' tab selected. It features three radio button options for selecting the update source. The first option, 'Serveur ActiveUpdate de Trend Micro', is selected and includes a text field with the URL 'http://mobilesecurity.activeupdate.trendmicro.com/Activeupdate/'. The second option, 'Autre source de mise à jour', includes a single text input field. The third option, 'Emplacement sur intranet contenant une copie du fichier actuel', includes three text input fields labeled 'Chemin UNC', 'Nom d'utilisateur', and 'Mot de passe'. An 'Enregistrer' (Save) button is located at the bottom left of the form area.

**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 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 ne peut pas se connecter à Internet, il est nécessaire de mettre à jour manuellement le serveur AutoUpdate local 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 à la page 7-2*
- *Affichage des journaux de l'agent de dispositif mobile à la page 7-2*
- *Maintenance des journaux à la page 7-4*

## 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 violation de la stratégie ou d'événements, ce journal est envoyé au serveur d'administration 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 de l'agent 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 d'administration Mobile Security. Sur le serveur d'administration, vous pouvez afficher les journaux de l'agent de dispositif mobile suivants :

- 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—Mobile Security Agent génère un journal lorsqu'il bloque une page Web dangereuse ou contenant un programme malveillant et le charge sur le serveur.
- Journal d'événements : ces journaux sont générés lorsque certaines actions sont entreprises par le serveur et par l'agent de dispositif mobile.

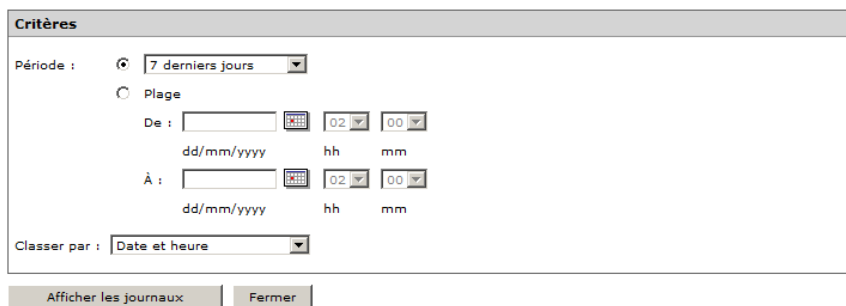
- Journal de violation de stratégies : ces journaux contiennent des informations relatives à l'état de conformité de la stratégie des agents de dispositif mobile.
- Journal de confidentialité—Mobile Security Agent génère un journal lorsqu'il détecte une menace pour la confidentialité et le charge sur le serveur.

---

## 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.
  - **Trier 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, 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 à la page 8-2*
- *Configuration des paramètres de notification à la page 8-2*
- *Configuration des notifications par courriel à la page 8-2*
- *Notifications et Rapports administrateur programmés à la page 8-3*
- *Notification utilisateur à la page 8-7*

## À propos des messages de notification et des rapports

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

- **Notifications & rapports administrateur**—envoie des notifications et rapports par e-mail 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 des 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**.
-

## 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 de jetons <%PROBLEME%>, <%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 de jeton <%DEVICE%> sera remplacée par le nom du dispositif mobile dans l'e-mail.
  - **Avertissement d'expiration du certificat APNs** : envoie une notification par courriel à l'administrateur un mois avant que le certificat APNs expire.
  - **Journal en temps réel de la recherche des programmes malveillants** : envoie une notification par courriel à l'administrateur lorsque l'agent détecte un programme malveillant.
  - **Avertissement d'expiration du jeton VPP** : envoie une notification par courriel à l'administrateur 15 jours avant l'expiration du jeton VPP.
  - **Avertissement d'expiration du jeton DEP** : envoie une notification par courriel à l'administrateur 15 jours avant l'expiration du jeton DEP.
- Rapports :
  - **Rapport d'inventaire des dispositifs**—affiche des informations complètes sur tous les dispositifs administrés.
  - **Rapport de violation de conformité**—affiche des informations de violation de conformité.

- **Rapport de détection de programmes malveillants**—affiche des informations sur les logiciels malveillants détectés.
- **Rapport de protection contre les menaces Internet**—affiche des informations sur les URL bloquées.
- **Rapport d'inventaire d'applications**—affiche des informations sur les applications principales installées sur les dispositifs Android et iOS.
- **Rapport d'enregistrement des dispositifs**—affiche des informations sur l'inscription du dispositif.
- **Rapport d'annulation d'enregistrement des dispositifs**—affiche des informations sur l'annulation d'enregistrement du dispositif.



**Remarque**

Pour consulter les rapports, accédez à **Notifications & rapports > Notifications administrateur & Rapports > Paramètres des rapports programmés**, puis cliquez sur **Consultez le dernier rapport** sous le nom du rapport.

---

## Activation des notifications et rapports administrateur

---

### Procédure

1. Accédez à **Notifications & rapports > Notifications & rapports administrateur**.

L'écran **Notifications & rapports administrateur** s'affiche.

2. Sélectionnez les notifications et les rapports que vous souhaitez recevoir par e-mail
  3. Cliquez sur **Enregistrer**.
-

## Configuration des paramètres de notification administrateur

---

### Procédure

1. Accédez à **Notifications & rapports > Notifications & rapports administrateur**.

L'écran **Notifications & rapports administrateur** s'affiche.

2. Dans **Paramètres des notifications**, cliquez sur un nom de notification.

L'écran **Paramètres des e-mails** de la notification sélectionnée s'affiche.

3. Mettez les informations suivantes à jour :

- **À** : adresse e-mail de l'administrateur.



#### Remarque

Utilisez un point-virgule « ; » pour séparer plusieurs adresses e-mail.

---

- **Sujet** : Ligne de sujet de l'e-mail de notification.
- **Message** : Corps du message de notification.



#### Important

Inclure les variables jetons fournies dans le modèle d'e-mail par défaut lorsque vous modifiez un message de notification.

---

4. Cliquez sur **Enregistrer**.
-

## Configuration des paramètres des rapports administrateur

---

### Procédure

1. Accédez à **Notifications & rapports > Notifications & rapports administrateur > Paramètres des rapports programmés**.

L'écran **Notifications & rapports administrateur** s'affiche.

2. Modifiez la fréquence du rapport.
  - a. Utilisez la liste déroulante située à côté de chaque rapport pour spécifier sa fréquence.
  - b. Choisissez l'une des options suivantes pour chaque rapport :
    - **Tous les jours**
    - **Toutes les semaines** : Spécifiez le jour de la semaine pour l'envoi du rapport dans la liste déroulante.
    - **Tous les mois** : Spécifiez le jour du mois pour l'envoi du rapport dans la liste déroulante.
  - c. Cliquez sur **Enregistrer**.
3. Modifiez les paramètres d'e-mail.

- a. Cliquez sur le nom du rapport.

L'écran **Paramètres de courriel** du rapport sélectionné s'affiche.

- b. Mettez les informations suivantes à jour :
  - **À** : adresse e-mail de l'administrateur.



#### Remarque

Utilisez un point-virgule « ; » pour séparer plusieurs adresses e-mail.

---

- **Sujet** : Ligne du sujet de l'e-mail contenant le rapport.



- **Message** : Corps du message du rapport.
- c. Cliquez sur **Enregistrer**.
- L'écran **Notifications & rapports administrateur** s'affiche.
- 

## Notification utilisateur

Utilisez l'écran **Notifications utilisateur** pour configurer la notification par courriel 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 de 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 de jetons <%DEVICE%> et <%VIOLATION%> seront remplacées par le nom du dispositif mobile dans le courriel et les stratégies qu'il viole.
- **Notification utilisateur VPP**—envoie une notification par courriel à un dispositif mobile lorsque l'administrateur attribue une application VPP à un utilisateur.

## 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 des 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.
  - Pour configurer les SMS de notification, il faut mettre à jour le corps du message dans le champ **Message**.
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 à la page 9-2*
- *Avant de contacter l'assistance technique à la page 9-5*
- *Envoi de contenu suspect à Trend Micro à la page 9-6*
- *TrendLabs à la page 9-6*
- *À propos des mises à jour de logiciel à la page 9-7*
- *Autres ressources utiles à la page 9-9*
- *À propos de Trend Micro à la page 9-9*

## 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 biométrique 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 cette liste, l'administrateur peut s'en servir pour définir le mot de passe de protection contre les désinstallations depuis la console d'administration.

- **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 obtenu par Trend Micro Mobile Security. Assurez-vous que l'heure de l'horloge système du serveur SCEP est correcte. Si le problème persiste, suivez cette 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**.

- **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 : `<adresse IP de SQL Server Express>\sqlexpress.`

**Remarque**

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

---

- **Impossible de se connecter au serveur SQL.**

Ce problème peut survenir lorsque le serveur SQL n'est pas configuré pour accepter des connexions à distance. Par défaut, les éditions SQL Server Express et SQL Server Developer n'autorisent pas les connexions à distance. Pour configurer le serveur SQL afin 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, procédez comme suit :

1. Accédez au <dossier d'installation de Visual Studio>\Microsoft Visual Studio 9.0\Common7\IDE, localisez et copiez le fichier devenv.exe.config, puis collez-le dans le dossier suivant (vous devrez peut-être 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.**

Ce problème se produit si votre Internet Explorer est configuré pour 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 d'administration 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 d'administration 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, consultez :

<http://esupport.trendmicro.com>

## Contacteur Trend Micro

Vous pouvez contacter les représentants Trend Micro par téléphone :

Adresse	Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France
Téléphone	Téléphone :+33 (0) 1 76 68 65 00

Site Internet	<a href="http://www.trendmicro.fr">www.trendmicro.fr</a>
Adresse de messagerie	<a href="mailto:support@trendmicro.com">support@trendmicro.com</a>

- Bureaux d'assistance dans le monde :  
<http://www.trendmicro.fr/apropos/contact/index.html>
- Documentation sur les produits Trend Micro :  
<http://docs.trendmicro.com/fr-fr/home.aspx>

## Envoi de contenu suspect à Trend Micro

Plusieurs options sont disponibles pour envoyer du contenu suspect à Trend Micro pour analyse.

### Services de File Reputation

Rassemblez les informations du système et envoyez les contenus de fichiers suspects à Trend Micro :

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

Conservez le numéro de dossier pour le suivi.

## TrendLabs

Trend Micro TrendLabs<sup>SM</sup> 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, d'ajouter des fonctionnalités ou de 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 patches de sécurité Windows contiennent un programme d'installation alors que les patches non-Windows incluent en général un script d'installation.
- **Patch**—Un patch est un groupe de correctifs à chaud et de patches de sécurité qui résolvent plusieurs problèmes du logiciel. Trend Micro publie régulièrement des patches. Les patches Windows contiennent un programme d'installation alors que les patches non-Windows incluent en général un script d'installation.
- **Service Pack**—Un service pack est une consolidation de correctifs à chaud, de patches 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 patches et les service packs :

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

Toutes les publications contiennent un fichier Lisez-moi contenant 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 concernent les fonctions de Mobile Security qui pourraient provisoirement nécessiter 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 comprennent :

- 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

Trend Micro, 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

## A

Affichage de compatibilité, 2-4  
Amélioration de la sécurité des données, 1-15  
amélioration de la stratégie de verrouillage,  
1-17  
analyse après mise à jour des signatures, 1-19  
analyse contre les programmes malveillants,  
1-22  
Analyse de Facebook, 1-8  
analyse de la confidentialité, 1-9  
Analyse depuis le nuage, 1-9  
analyse de sécurité, 1-8  
Anti-spam pour SMS, 1-23  
application push, 1-20  
arborescence de dispositif, 1-12  
architecture mise à jour, 1-21, 1-22  
authentification basée sur l'identité du  
dispositif, 1-18  
authentification de dispositif mobile, 1-24  
Authentification facultative, 1-20  
authentification unique, 1-15

## B

banque d'applications d'entreprise, 1-12, 1-14,  
1-21  
    À propos, 5-2  
Base de connaissances, 9-5  
BlackBerry, 1-11

## C

certificats d'entreprise, 1-14, 1-15, 1-17  
client iOS simple, 1-19  
code QR, 1-17  
comptes administrateurs multiples, 1-16  
confirmation de commande du serveur, 1-17

Connecteur Exchange, 1-16  
conseils de dépannage, 9-2, 9-3  
    certificat SCEP, 9-2  
    Désynchronisé, 9-4  
    fichier de configuration  
    automatique .pac, 9-4  
    fichier de configuration  
    devenv.exe.config, 9-3  
    horloge système, 9-2  
    liste de dispositifs client, 9-4  
    Serveur de communication, 9-2  
    SQL Server 2008 R2, 9-3  
    SQL Server Express, 9-3  
console Web d'administration, 2-2, 2-4  
    nom d'utilisateur et mot de passe, 2-3  
    opérations, 2-2  
    URL, 2-2  
contrôle des applications, 1-17, 1-20

## D

détails du compte utilisateur, 2-15  
Dispositifs invités  
    états d'invitation, 3-24

## E

Écran de vérification de configuration  
rapide, 1-20  
effacement des données d'entreprise sur les  
dispositifs mobiles, 3-17  
envoyer une alerte par e-mail, 4-26  
état de la commande, 2-19  
état du dispositif, 1-14  
états des dispositifs mis à jour, 1-16  
évaluation des risques, 1-9  
exportation de journal, 1-12

**F**

- file de commandes, 1-14
- filtrage des appels, 1-24
  - configuration de la liste de filtrage, 4-20
  - format de la liste de filtrage, 4-21
  - stratégies, 1-22
- fonction de verrouillage mise à jour, 1-22

**G**

- gestion des dispositifs en mode surveillé, 1-17
- gestion iOS, 1-11, 1-13, 1-14
- questionnaire de contrôle, 1-15
- Google Play, 1-8
- Groupe non géré pour Android et iOS, 1-18

**I**

- informations sur le dispositif, 1-12
- inscription d'un dispositif mobile, 1-17
- inscription du dispositif, 1-12
- Intégration de Control Manager, 1-15
- intégration de serveur Exchange, 1-16
- intégré avec Active Directory, 1-21
- interface MDA mise à jour, 1-17
- inventaire d'application, 1-20

**J**

- journal d'événements, 1-12
- Journal de violation de la stratégie, 1-18
- journaux d'événements améliorés, 1-18
- journaux MDA
  - à propos de, 7-2
  - critères de requête, 7-3
  - Journal d'événements, 7-2
  - Journal de confidentialité, 7-3
  - Journal de protection contre les menaces Internet, 7-2
  - Journal de protection contre les programmes malveillants, 7-2

- Journal de violation de la stratégie, 7-3
- types de journaux, 7-2

## Journaux MDA

- suppression manuelle, 7-5
- suppression planifiée, 7-4

**L**

- liste de vérification
  - stratégie de compatibilité, 4-23
- localisation d'un dispositif à distance, 1-22
- localisation de dispositifs mobiles iOS, 1-9

**M**

- MARS, 1-9, 1-17
- menaces mobiles, 1-2
  - messages de spam, 1-2
- mise à jour du logiciel
  - à propos de, 9-7
  - éléments de version, 9-7
  - Fichier Lisez-moi, 9-8
- mise en service des dispositifs iOS, 1-15, 1-17
- mise en service simplifiée, 1-19
- mises à jour de composants
  - à propos de, 6-2
  - manuel, 6-2
  - programmé, 6-3
  - Serveur local AutoUpdate, 6-7
  - sources de téléchargement, 6-6
- mises à jour régulières, 1-25
- Mobile Security
  - Active Directory, 1-5
  - Agent de dispositif mobile, 1-5
  - à propos de, 1-2
  - architecture, 1-3
  - certificat
    - autorité, 1-5

- Certificat APNs (Apple Push Notification service), 1-6
  - Certificat SSL, 1-6
    - clés publiques et privées, 1-5
    - gestion, 2-22
    - informations d'identification de la sécurité, 1-5
    - SCEP, 1-5
  - communications réseau indésirables, 1-2
  - compatibilité avec le logiciel de chiffrement, 1-2
  - composants, 1-3
  - Connecteur Exchange, 1-4
  - méthodes de communication, 1-3
  - Microsoft SQL Server, 1-5
  - Modèle de sécurité amélioré
    - Serveur de communication du nuage, 1-3
    - Serveur de communication local, 1-3
  - Modèle de sécurité de base, 1-3
  - modèles de déploiement, 1-3
  - OfficeScan, 1-2
  - Serveur d'administration, 1-3
  - Serveur de communication, 1-4
  - Serveur de communication du nuage, 1-4
  - Serveur de communication local, 1-4
  - Serveur SMTP, 1-6
  - sous-groupes, 3-3
  - Types de serveur de communication, 1-4
  - modèle, 1-9
  - mot de passe
    - protection contre la désinstallation, 9-2
    - réinitialiser le mot de passe, 1-21, 3-19
- N**
- notifications et rapports
    - à propos de, 8-2
    - configuration par courriel, 8-7
    - notifications, 8-3
    - rapports, 8-3
    - variables de jeton, 8-7
  - Nouveautés
    - 7.0, 1-21
    - 7.1, 1-21
    - 8.0, 1-19
    - 8.0 SP1, 1-18
    - 9.0, 1-16
    - 9.0 SP1, 1-14
    - 9.0 SP2, 1-12
    - 9.1, 1-11
    - 9.2, 1-9
    - 9.3, 1-8
    - v9.5, 1-7
- O**
- OfficeScan, 1-16
  - onglet Dispositifs administrés, 3-3
  - Onglet Dispositifs Exchange ActiveSync, 3-26
  - Onglet Dispositifs invités, 3-23
    - informations du courriel d'invitation, 3-23
- P**
- Paramètres des notifications push HTTP(S), 1-19
  - personnalisation d'agent, 1-19
  - Point d'accès WiFi, 1-15
  - prise en charge des dispositifs mobiles
    - Android, 1-22

prise en charge des dispositifs mobiles  
 BlackBerry, 1-21  
 prise en charge des dispositifs mobiles iOS,  
 1-21  
 Prise en charge du proxy Web, 1-19  
 Prise en charge IPv6, 1-15  
 problèmes connus, 9-8  
 programme d'achats en grande quantité, 1-17  
 propriétés du compte racine, 2-11  
 propriétés du rôle Super administrateur, 2-12  
 Protection contre les menaces Internet, 1-15  
 protection par mot de passe, 1-12  
 Protection WAP Push, 1-24

## R

rapports programmés, 1-20  
 recherche avancée, 1-12  
 ressources  
     Outils et services basés sur Internet :,  
     9-9  
 Restriction de carte SD, 1-20

## S

Samsung KNOX, 1-13  
 Sécurité Web, 1-23  
 sensibilisation sur l'emplacement, 1-9  
 serveur d'administration autonome, 1-16  
 serveur de communication du nuage  
 facultatif, 1-16  
 Site Web d'assistance technique, 9-5  
 SMS sender, 1-9, 1-11  
 spam  
     SMS, 4-16  
         configuration de la liste de filtrage,  
         4-17  
         format de la liste de filtrage, 4-18  
     WAP Push, 4-18

format de liste approuvée, 4-19  
 stratégie de mise en service, 1-21  
 Stratégie de protection contre les menaces  
 Internet, 1-19  
 Stratégie de protection contre les  
 programmes malveillants  
     Options d'analyse, 4-16  
     types d'analyse, 4-15  
 Stratégie générale  
     désinstallation des fonctions de  
     protection, 4-10  
     paramètres de mise à jour, 4-10  
     paramètres des journaux, 4-11  
 stratégies basées sur des modèles, 1-16  
 suppression sélective, 1-20  
 Symbian, 1-13

## T

Tableau de bord  
     écran, 1-20  
     état de la mise à jour du serveur, 2-6  
     état du chiffrement, 2-7  
     état du contrôle d'application, 2-7  
     état du débridage, 2-7  
     état du dispositif mobile, 2-5  
     gestion des informations, 1-17  
     programme correctif et état de la mise à  
     jour des composants, 2-6  
 téléchargement de rapports administrateur,  
 1-18  
 TrendLabs, 9-6  
 Trend Micro  
     à propos de, 9-9

## U

URL d'inscription personnalisable, 1-18



**V**

- vérification de la compatibilité, 1-20
- verrouillage d'un dispositif mobile, 3-16
- Version complète de la licence, 2-4
- VPN par application, 1-15

**W**

- widgets, 1-16, 1-17
- Windows Mobile, 1-13
- Windows Phone, 1-13





**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](http://www.trendmicro.com)

Item Code: TSFM97238/151028