TREND MICRO™

9.8 TREND MICRO™ Mobile Security™

Manuel de l'administrateur

(pour le mode de déploiement de l'analyse de sécurité)

Sécurité complète pour portables d'entreprise

Endpoint Security

Numéro de référence du document TSCM98148/180126

Date de publication : Novembre 2017

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

Chapitre 1: Introduction

Chapitre 2: Mise en route avec Mobile Security

Chapitre 3: Intégration à d'autres solutions MDM

Chapitre 4: Gestion des dispositifs mobiles

Chapitre 5: Affichage des utilisateurs

Chapitre 6: Protection des dispositifs à l'aide de stratégies

Chapitre 7: Affichage et gestion des détections

Chapitre 8: Mise à jour des composants

Chapitre 9: Affichage et maintenance des journaux

Chapitre 10: Utilisation des notifications et rapports

Chapitre 11: Dépannage et contact de l'assistance technique

Index

Préface

Préface

Bienvenue au Manuel de l'administrateur Trend Micro™ Mobile Security for Enterprise version 9.8. 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

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

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

Chapitre 1

Introduction

Trend Micro™ Mobile Security for Enterprise 9.8 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

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

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.

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 fonctions similaires, telles que le scan anti-programmes malveillants, risquent d'être incompatibles avec Mobile Security.

À propos de l'apprentissage automatique dans Trend Micro Mobile Security

L'apprentissage automatique prédictif de Trend Micro est une technologie avancée qui permet de mettre en corrélation les informations sur les menaces et d'effectuer une

analyse approfondie des fichiers pour détecter les risques de sécurité inconnus émergents via un système de reconnaissance de l'ADN numérique, des mappages d'API et d'autres fonctions de fichier. L'apprentissage automatique prédictif est un outil puissant qui vous aide à protéger votre environnement contre les menaces non identifiées et les attaques « jour zéro ».

Après la détection d'un fichier inconnu ou à faible prévalence, Mobile Security analyse le fichier à l'aide du moteur mobile de dernière génération pour extraire des fonctions de fichiers et envoie le rapport au moteur d'apprentissage automatique prédictif, hébergé sur le réseau Trend Micro Smart Protection Network. Grâce à l'utilisation de la modélisation de programmes malveillants, l'apprentissage automatique prédictif compare l'échantillon au modèle de programmes malveillants, attribue un score de probabilité et détermine le type du programme malveillant que contient probablement le fichier. Mobile Security peut empêcher l'installation du fichier concerné et rappeler à l'utilisateur de le désinstaller ou de le supprimer.

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.

TABLEAU 1-1. Composants du système Mobile Security

COMPOSANT	DESCRIPTION	REQUIS OU FACULTATIF
Serveur d'administration	Le serveur d'administration vous permet de gérer les agents de dispositif mobile à partir de la console Web d'administration. Une fois les dispositifs mobiles inscrits sur le serveur, vous pouvez configurer les stratégies des agents de dispositif mobile et effectuer des mises à jour.	Requis
Serveur de communication	Le serveur de communication gère les communications entre le serveur d'administration et les agents de dispositif mobile. Trend Micro Mobile Security fournit deux types de Communication Server : • Serveur de communication local (LCS)—il s'agit d'un Communication Server déployé localement sur votre réseau. • Cloud Communication Server(CCS)—il s'agit d'un Communication Server déployé sur le nuage ; vous n'aurez donc pas besoin de l'installer. Trend Micro gère le Cloud Communication Server et il vous suffit de vous-y connecter à partir du serveur d'administration. Voir la section *Comparaison entre le serveur local et le serveur de communication à la page 1-6*.	Requis
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

Composant	Description	Requis ou facultatif
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	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. 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. 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.	Facultatif

Composant	Description	Requis ou facultatif
Certificat SSL	(Modes de déploiement **Version complète** et **Analyse de sécurité** avec distributeur MDM non répertorié uniquement.) 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 pour gérer les dispositifs mobiles 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	Cloud Communication Server	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

Nouveautés de cette version (9.8)

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.8 :

Fonction	Description
Courriel d'invitation (Android uniquement)	Permet aux administrateurs d'envoyer un courriel d'invitation à tous les utilisateurs lors du déploiement de l'agent de dispositif mobile via AirWatch.
Plus d'analyses et de détections de sécurité :	Prise en charge de l'analyse des éléments suivants sur les dispositifs mobiles : • certificats SSL malveillants • profils iOS malveillants (iOS uniquement) • déchiffrement du trafic réseau • point d'accès dangereux (Wi-Fi) • options pour développeurs et débogage USB (Android uniquement) • applications modifiées
Nouveaux widgets, nouvelles notifications administrateur et nouveaux rapports	Introduction de nouveaux widgets, de nouvelles notifications administrateur et de nouveaux rapports sur les certificats SSL malveillants, les profils iOS malveillants, le déchiffrement du trafic réseau, les points d'accès dangereux (Wi-Fi), d'options pour développeurs, de débogage USB, d'applications modifiées et de dispositifs mobiles débridés.
Liste des applications approuvées	Introduction d'une liste approuvée qui permet aux administrateurs de certifier la fiabilité des applications considérées comme programmes malveillants, vulnérables, présentant un risque de confidentialité ou modifiées afin qu'elles puissent être installées sur des dispositifs mobiles.
Prise en charge de l'agent de dispositif mobile iOS	Prend en charge l'agent de dispositif mobile iOS en mode de déploiement Analyse de sécurité uniquement avec AirWatch et MobileIron.

Nouveautés de la version 9.7 Patch 3

Les fonctions suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.7 Patch 3 :

FONCTION	DESCRIPTION
Fourniture d'un code QR pour le déploiement rapide des agents (mode de déploiement Analyse de sécurité uniquement)	Fournit les informations d'inscription à l'aide du code QR sur l'écran des paramètres de déploiement de l'agent pour un déploiement rapide et simple de ce dernier. Cette fonction est uniquement disponible en mode de déploiement Analyse de sécurité avec intégration à AirWatch et à MobileIron.
Prise en charge de l'apprentissage automatique prédictif	Prend en charge l'apprentissage automatique prédictif de Trend Micro pour effectuer une analyse approfondie des fichiers afin de détecter les risques de sécurité connus émergents.

Nouveautés de la version 9.7 Patch 2

Les fonctions suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.7 Patch 2 :

FONCTION	DESCRIPTION
Intégration aux solutions de gestion de dispositifs mobiles MobileIron	Assure l'analyse de sécurité des dispositifs mobiles Android et iOS tout en assurant l'intégration aux solutions de gestion de dispositifs mobiles MobileIron suivantes : • MobileIron Core hébergé • MobileIron Core sur site
Intégration de l'aide en ligne	Relie tous les écrans d'interface utilisateur aux fichiers d'aide disponibles sur le centre d'aide en ligne de Trend Micro.

Fonction	Description
Prend en charge le verrouillage d'activation iOS (mode de déploiement Version complète uniquement)	Le verrouillage d'activation est une fonctionnalité de Find My iPhone intégrée dans les dispositifs mobiles disposant d'iOS 7 et versions ultérieures. Il empêche la réactivation d'un dispositif mobile perdu ou volé en exigeant l'ID Apple et le mot de passe de l'utilisateur avant que quiconque puisse désactiver Find My iPhone, effacer, ou réactiver et utiliser le dispositif mobile.

Nouveautés de la version 9.7

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.7 :

Fonction	Description
Modes de déploiement multiples	Permet de déployer Trend Micro Mobile Security dans : • Mode de déploiement **Version complète**, réunissant toutes les fonctions de Trend Micro Mobile Security. • Mode de déploiement **Sécurité uniquement**, assurant l'analyse de sécurité pour les dispositifs mobiles Android et iOS tout en s'intégrant avec les autres solutions de gestion des dispositifs mobiles (MDM).
Intégration avec AirWatch	Assure l'analyse de sécurité pour les dispositifs mobiles Android et iOS tout en garantissant l'intégration à la solution de gestion de dispositifs mobiles AirWatch.
Widget Actualités de la cybersécurité sur l'écran du tableau de bord	Inclut un widget sur l'écran **Tableau de bord** qui affiche les Actualités de la cybersécurité pour dispositifs mobiles, éditées par Trend Micro.
Vérification du certificat de serveur sur les dispositifs Android	Permet de vérifier le certificat de serveur sur les dispositifs mobiles Android.

Fonction	Description
Nouvelle API MARS pour l'analyse de la sécurité	S'intègre avec la dernière API MARS (Mobile Application Reputation Service), afin d'améliorer la détection et la description de la vulnérabilité.
Prise en charge pour les dernières versions d'Android et d'iOS	Ajoute la prise en charge d'Android 7 et iOS 10.

Nouveautés de la version 9.6 SP1

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.6 SP1 :

Fonction	Description
Widgets de détection de logiciels de rançon	Les nouveaux widgets du tableau de bord permettent aux administrateurs de consulter les statistiques de détection de logiciels de rançon.
Sélection de la version de l'application Android	Les administrateurs peuvent choisir de déployer la **Version complète** ou l'**Analyse de sécurité** uniquement de l'application pour les dispositifs Android et iOS.
Activation automatique de l'application sur les dispositifs Android	Cette version de Mobile Security inclut l'activation automatique sur les dispositifs Android pendant le déploiement de l'application.
Nettoyage de données Exchange Server (mode de déploiement Version complète uniquement)	Les administrateurs peuvent nettoyer les données avant tout transfert vers une autre instance d'Exchange Server. Ils peuvent ainsi supprimer les données de dispositifs de connecteur Exchange et Exchange ActiveSync sur Mobile Security.
Configuration de groupe pour plusieurs utilisateurs Active Directory	Les administrateurs peuvent appliquer la configuration de groupe à plusieurs utilisateurs Active Directory.

Fonction	Description
Génération de rapports par plate-forme de dispositif	Les améliorations apportées à la fonction de génération de rapports permettent aux administrateurs de générer des rapports pour les plates-formes de dispositifs sélectionnées.
Mise à jour des informations du dispositif	Les administrateurs peuvent mettre à jour les informations d'un dispositif mobile administré, avant la mise à jour programmée suivante.

Nouveautés de la version 9.6

Les fonctionnalités suivantes sont désormais disponibles dans Trend Micro Mobile Security 9.6 :

Fonction	Description
Gestion des utilisateurs	Permet aux administrateurs de gérer séparément les utilisateurs et les invitations.
Rapports à la demande	Les administrateurs peuvent désormais générer des rapports à tout moment.
Scan programmé	Permet aux administrateurs d'exécuter la recherche de programmes malveillants et l'analyse de sécurité de manière quotidienne, hebdomadaire ou mensuelle, selon le programme défini.
Analyse de sécurité pour Android	Outre l'analyse de confidentialité, Mobile Security prend désormais en charge l'analyse de vulnérabilité et l'analyse des applications modifiées pour une sécurité accrue.
Nouveaux widgets	Cinq nouveaux widgets font leur apparition dans cette version. Ils affichent des informations sur les analyses de sécurité sous Android et la recherche de programmes malveillants sous iOS.
Nouvelle version de iOS App	Les administrateurs peuvent déployer une nouvelle version de l'application iOS, qui prend uniquement en charge les analyses de sécurité et fonctionne avec les applications de gestion des dispositifs mobiles (MDM) tierces.

Principales fonctions de l'agent de dispositif mobile

Nom des fonctions	Description		Android	iOS
Analyse de la sécurité	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.	Recherche des programmes malveillants	●	●
		Analyse de la confidentialité	●	
		Analyse de la vulnérabilité	●	
		Analyse des applications modifiées	●	●
		Analyse du débogage USB	●	
		Analyse des options pour développeurs	●	
		Analyse du dispositif mobile débridé	●	
		Analyse du dispositif mobile débridé		●
		Analyse des profils iOS malveillants		●
		Analyse du déchiffrement du trafic réseau	●	●
		Analyse du certificat SSL malveillant	●	●
		Analyse du point d'accès dangereux (Wi-Fi)	●	

NOM DES FONCTIONS	DESCRIPTION	ANDROID	IOS
Authentification	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.	●	●
Mises à jour régulières	Pour vous protéger des menaces les plus récentes, vous pouvez mettre à jour Mobile Security manuellement ou le configurer pour qu'il se mette à jour automatiquement. Pour réduire les coûts, vous pouvez également définir une fréquence de mise à jour différente pour les appareils mobiles qui sont en « itinérance ». Les mises à jour incluent des mises à jour de composants et des correctifs pour le programme Mobile Security.	●	

NOM DES FONCTIONS	DESCRIPTION		ANDROID	IOS
Journaux de l'agent de dispositif mobile	Journaux de l'agent de dispositif mobile disponibles sur le serveur d'administration.	Journaux d'analyse de l'application	●	●
		Journaux de vulnérabilité du dispositif	●	●
		Journaux de protection du réseau	●	●
		Journaux de protection contre les menaces Internet	●	
	L'agent de dispositif mobile conserve les journaux utilisateur sur le dispositif mobile.	Historique de la recherche de programmes malveillants	●	
		Journaux d'analyse de la vulnérabilité	●	
		Journaux d'analyse des applications modifiées	●	
		Historique de l'analyse de la confidentialité	●	
		Historique du blocage Web	●	

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 9.8

STRATÉGIE	FONCTIONS	PARAMÈTRES		
Sécurité de dispositif	Paramètres de sécurité	Analyse en temps réel		●
		Analyse après mise à jour des signatures		●
		Analyse manuelle	●	●
Protection des données	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		●

Chapitre 2

Mise en route avec Mobile Security

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

Ce chapitre contient les sections suivantes :

Console Web d'administration

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

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

Vous pouvez utiliser la console Web pour effectuer les tâches suivantes :

- 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.

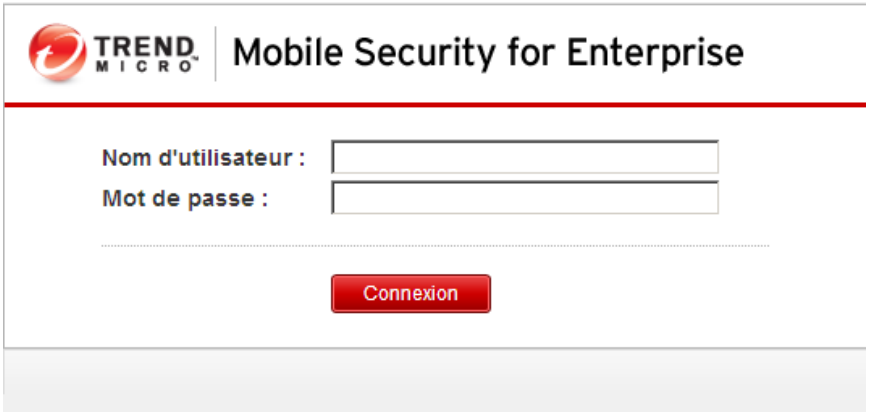


FIGURE 2-1. Écran de connexion de la console Web d'administration

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 **Afficher tous les sites Web dans Affichage de compatibilité** 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 dans Windows 2012 en utilisant Internet Explorer 10 en mode Metro, vérifiez que l'option **Mode protégé amélioré** 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** dans Internet Explorer. Si vous utilisez Internet Explorer pour accéder à la console Web 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 deux onglets :

- **Récapitulatif** : affiche les actualités relatives à la cybersécurité en relation avec les dispositifs mobiles, les états de santé et de sécurité du dispositif mobile et un récapitulatif de la version du système d'exploitation du dispositif mobile.
- **Sécurité** : affiche le récapitulatif de l'analyse des vulnérabilités des dispositifs Android et iOS, le récapitulatif de la protection des réseaux Android et iOS ainsi que le récapitulatif des risques relatifs aux applications Android et iOS. Cette catégorie affiche les widgets et les états suivants :
  - **Récapitulatif des vulnérabilités des dispositifs Android et iOS :**
    - **Débridé** : (Android uniquement) nombre de dispositifs mobiles débridés
    - **Débogage USB** : (Android uniquement) nombre de dispositifs mobiles avec le mode débogage USB activé
    - **Options pour développeurs** : (Android uniquement) nombre de dispositifs mobiles avec le mode Developer activé

- **Débridé** : (iOS uniquement) nombre de dispositifs mobiles débridés
- **Profils iOS malveillants** : (iOS uniquement) nombre de dispositifs mobiles sur lesquels des profils iOS malveillants sont installés

- **Récapitulatif de la protection du réseau Android/iOS** :
  - **Point d'accès dangereux (Wi-Fi)** : (Android uniquement) nombre de dispositifs mobiles connectés à des points d'accès suspects ou non sécurisés (Wi-Fi) sans mot de passe ou avec un mot de passe faible
  - **Déchiffrement du trafic réseau** : nombre de dispositifs mobiles détectés avec un trafic réseau chiffré
  - **Certificat SSL malveillant** : nombre de dispositifs mobiles sur lesquels des certificats SSL malveillants sont installés
- **Récapitulatif des risques relatifs à l'applications Android/iOS** :
  - **Programme malveillant** : nombre d'applications installées et considérées comme des programmes malveillants
  - **Application vulnérable** : (Android uniquement) nombre d'applications installées et considérées comme vulnérables
  - **Risques de confidentialité** : (Android uniquement) nombre d'applications installées et détectées comme présentant un risque de confidentialité
  - **Applications modifiées** : nombre d'applications installées avec le package de l'application modifiée

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.

Configuration des paramètres de déploiement

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

Basculer du mode de déploiement Version complète vers le mode Analyse de sécurité

Vous pouvez modifier le mode de déploiement de Mobile Security à tout moment.

Reportez-vous à l'article de base de connaissances suivant pour plus de détails sur le basculement du mode de déploiement **Version complète** vers le mode **Analyse de sécurité** :

https://success.trendmicro.com/solution/1115884

Configuration de l'intégration d'AirWatch à Trend Micro Mobile Security

Trend Micro Mobile Security permet l'intégration à la solution de gestion de dispositifs AirWatch.

Pour obtenir des informations détaillées, reportez-vous à la rubrique *Intégration avec AirWatch à la page 3-2*.

Configuration de l'intégration MobileIron avec Trend Micro Mobile Security

Trend Micro Mobile Security autorise l'intégration avec la solution MobileIron de gestion de dispositifs.

Pour obtenir des informations détaillées, reportez-vous à la rubrique *Intégration à MobileIron à la page 3-17*.

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 d'administrateur par défaut est « root » (mot de passe : « mobilesecurity »). Le compte racine ne peut pas être supprimé, il peut uniquement être modifié. Voir la section *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 la section *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

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

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

Composants du serveur	Autorisations	Super Administrateur	Administrateur de groupe
Notifications/ rapports	Requête des journaux	Tous les groupes	Groupes administrés uniquement
	Maintenance des journaux	Tous les groupes	Groupes administrés uniquement
	Notifications/rapports administrateur	Pris en charge	Non pris en charge
	Notifications utilisateur	Pris en charge	Non pris en charge
	Paramètres	Pris en charge	Non pris en charge
Applications		Pris en charge	Pris en charge pour les groupes administrés uniquement
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
Utilisateurs	Inviter des utilisateurs	Pris en charge	Pris en charge pour les groupes administrés uniquement

Ajout de comptes d'administrateur

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Administration** > **Gestion des comptes d'administrateur**.
2. Dans l'onglet **Comptes d'administrateur**, cliquez sur **Créer** pour ajouter un nouveau compte.

   L'écran **Créer un compte d'administrateur** apparaît.
3. 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.

4. 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

5. Cliquez sur **Enregistrer**.

Modification de compte d'administrateur

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Administration** > **Gestion des comptes d'administrateur**.

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

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

3. 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*.

4. Cliquez sur **Enregistrer**.

Suppression de comptes d'administrateur

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Administration** > **Gestion des comptes d'administrateur**.
2. Dans l'onglet **Comptes d'administrateur**, sélectionnez les comptes d'administrateur que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

   Un message de confirmation s'affiche.

Création d'un rôle d'administrateur

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Administration** > **Gestion des comptes d'administrateur**.
2. Dans l'onglet **Rôles d'administrateur**, cliquez sur **Créer**.

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

Modification d'un rôle d'administrateur

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Administration** > **Gestion des comptes d'administrateur**.
2. Dans l'onglet **Rôles d'administrateur**, cliquez sur **Créer**.

   L'écran **Créer un rôle d'administrateur** apparaît.
3. Modifiez les détails du rôle selon les besoins, puis cliquez sur **Enregistrer**.

Suppression d'un rôle d'administrateur

Procédure

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

   Un message de confirmation s'affiche.

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 dans la console Web et vous permet d'en annuler ou d'en renvoyer une, 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**, allez 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.

État de la commande	Description
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 de Mobile Security pour qu'elle les supprime automatiquement selon un programme défini 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**.

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 Web d'administration de Mobile Security.

2. Cliquez sur **Administration** > **Gestion des certificats**.

3. Cliquez sur **Ajouter**.

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

4. Cliquez sur **Choisir un fichier**, puis sélectionnez un fichier de certificat au format `.pfx`, `.p12`, `.cer`, `.crt` ou `.der`.

5. Entrez le mot de passe du certificat dans le champ **Mot de passe**.

6. Cliquez sur **Enregistrer**.

Suppression d'un certificat

Procédure

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

Chapitre 3

Intégration à d'autres solutions MDM

Trend MicroMobile Security vous permet d'intégrer d'autres solutions de gestion de dispositifs mobiles à Mobile Security.

Ce chapitre explique la procédure de configuration de l'intégration de Mobile Security à d'autres solutions de gestion de dispositifs mobiles.

Sujets traités dans ce chapitre :

Intégration avec AirWatch

Trend Micro Mobile Security vous permet d'intégrer la solution AirWatch MDM à Mobile Security.

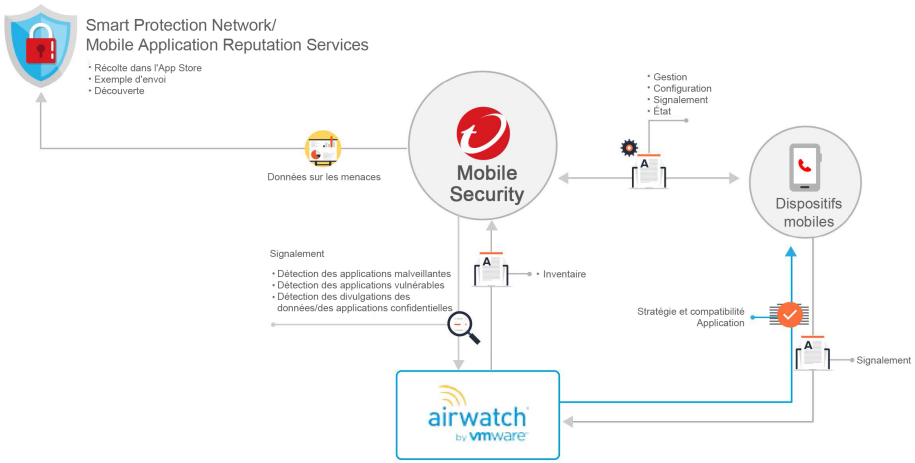
Conditions requises pour l'intégration

Pour intégrer d'autres solutions MDM à Trend MicroMobile Security, vous devez utiliser les éléments suivants :

- Mobile Security for Enterprise 9.7 ou version ultérieure
- Serveur de communication local ou Serveur de communication du nuage configuré dans Mobile Security
- AirWatch v9.1 ou version ultérieure
- Compte d'administrateur sur la console Web d'administration AirWatch

Architecture d'intégration à AirWatch

L'image suivante montre l'architecture de haut niveau d'intégration à AirWatch.



Mobile App Reputation est une technologie cloud qui identifie automatiquement les menaces mobiles sur la base du comportement des applications, collecte un grand nombre d'applications Android de divers marchés Android, identifie des programmes mobiles malveillants existants et récents, identifie les applications pouvant compromettre la confidentialité et utiliser de façon abusive les ressources des dispositifs. Il s'agit du premier service d'évaluation automatique d'applications mobiles au monde.

Trend Micro Smart Protection Network fournit des informations globales et interactives contre les menaces immédiates pour garantir une protection permanente. Trend Micro utilise ces informations pour instantanément contrer les attaques avant qu'elles puissent vous nuire. **Smart Protection Network** agit sur tous les produits et services Trend Micro.

Mobile Security utilise Smart Protection Network et Mobile Application Reputation Services pour détecter les problèmes de sécurité des dispositifs mobiles, et s'appuie sur la stratégie de conformité AirWatch pour gérer votre dispositif mobile.

Fonctionnalités d'intégration

Trend MicroMobile Security fournit les fonctionnalités suivantes avec l'intégration à AirWatch :

FONCTION	DESCRIPTION
Regroupement automatique de dispositifs mobiles	Mobile Security ajoute les préfixes Dangerous, Risky et No_TMMS pour baliser les dispositifs mobiles en fonction de leur niveau de risque. Voir *Regroupement automatique de dispositifs mobiles à la page 3-4* pour plus de détails.
Regroupement automatique d'applications	Mobile Security ajoute les préfixes Malware, Vulnerability et Privacy pour regrouper les applications mobiles en fonction de leur niveau de risque. Voir *Regroupement automatique pour applications mobiles à la page 3-5* pour plus de détails.

FONCTION	DESCRIPTION
Mise à jour automatique de la liste de blocage AirWatch pour les applications enfreignant la stratégie	Cette fonctionnalité vous permet de placer dans la liste de blocage les applications qui enfreignent la stratégie de conformité AirWatch (sur la base du résultat d'analyse de sécurité) et elle envoie un message d'alerte à l'utilisateur. Voir *Configuration de la stratégie de conformité à la liste de blocage AirWatch pour les applications à la page 3-5* pour plus de détails.
Déploiement automatique de l'application Mobile Security Client	Vous pouvez configurer AirWatch pour déployer automatiquement l'agent de dispositif mobile sur les dispositifs mobiles. • **Android** : Voir *Déploiement de l'agent Android au moyen du serveur Mobile Security à la page 3-12* pour la procédure. Vous pouvez également configurer des dispositifs mobiles Samsung pour lancer automatiquement l'agent de dispositif mobile sur des dispositifs mobiles. Voir *Configuration du lancement automatique de dispositifs mobiles Android à la page 3-13* pour les détails et la procédure. • **iOS** : Voir *Déploiement de l'agent iOS à la page 3-15* pour la procédure.

Regroupement automatique de dispositifs mobiles

Mobile Security utilise des préfixes pour créer trois (3) classes (Dangerous, Risky et NO_TMMS) et balise les dispositifs à risque de la façon suivante :

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

Mobile Security vous permet de définir des préfixes (PREDEFINEDPREFIX) dans la console Web d'administration. Lorsque Mobile Security détecte un dispositif mobile

avec différents niveaux de sécurité, il modifie automatiquement le groupe Smart du dispositif.

Par exemple, si Mobile Security détecte un programme malveillant sur un dispositif mobile, il transfère automatiquement le dispositif mobile vers le groupe PREDEFINEDPREFIX _Dangerous.

Regroupement automatique pour applications mobiles

Mobile Security regroupe automatiquement les applications à risque sous les groupes d'applications, en fonction du type de risque qu'elles impliquent.

- PREDEFINEDPREFIX _Malware_App_Android
- PREDEFINEDPREFIX _Privacy_App_Android
- PREDEFINEDPREFIX _Vulnerability_App_Android
- PREDEFINEDPREFIX _Malware_App_iOS

Mobile Security vous permet de définir des préfixes (PREDEFINEDPREFIX) dans la console Web d'administration.

Configuration de la stratégie de conformité à la liste de blocage AirWatch pour les applications

Après la configuration des paramètres d'intégration d'AirWatch, vous pouvez créer une stratégie de conformité sur la console Web d'administration AirWatch pour ajouter des applications malveillantes à la **liste de blocage** d'AirWatch.

Procédure

1. Ouvrez une session sur la console Web AirWatch, puis accédez à **Dispositifs** > **Stratégies de conformité** > **Affichage de la liste**.
2. Cliquez sur **Ajouter**, sélectionnez la plate-forme (Android ou Apple iOS), puis dans les listes déroulantes, sélectionnez **Liste d'applications**, puis **Contient une ou des applications en liste noire**.
3. Cliquez sur **Suivant**.

4. Dans l'onglet **Actions**, configurez des actions :

   a. Sélectionnez **Marquer comme non conforme**.

   b. Sélectionnez **Notifier** et **Envoyer un e-mail à l'utilisateur** à partir des listes déroulantes.

   c. Cliquez sur **Suivant**.

5. Dans l'onglet **Attribution**, configurez les éléments suivants :

   - **Géré par** : `Trend Micro`
   - **Groupes attribués**
   - **Exclusions**

6. Cliquez sur **Suivant**.

7. Dans l'onglet **Sommaire**, configurez le nom et la description.

8. Cliquez sur **Terminer et activer**.

Si un programme malveillant est détecté sur le dispositif mobile, Mobile Security place l'application dans la liste de blocage d'AirWatch, et le dispositif mobile sera marqué comme non conforme.

Autorisations du compte AirWatch requises pour l'intégration

Mobile Security prend en charge l'intégration à AirWatch. Pour intégrer Mobile Security à AirWatch, vous devez disposer d'un compte AirWatch avec les autorisations requises pour la communication entre le serveur Mobile Security et AirWatch.

Vous pouvez créer un compte sur AirWatch avec trois options d'autorisation différentes :

- **Option 1 : Créer un compte d'administrateur AirWatch pour communiquer avec toutes les autorisations**

Sur la console d'administration AirWatch, accédez à **Comptes** > **Administrateurs** > **Affichage de la liste** > **Ajouter** > **Ajouter un administrateur** et créez un compte avec les autorisations et le rôle suivants :

```
AirWatch Administrator AirWatch Admins (Internal or External) Access
```

- **Option 2 : Créer un utilisateur à l'aide de l'API ONLY avec toutes les autorisations de l'API REST**

  Sur la console d'administration AirWatch, accédez à **Comptes** > **Administrateurs** > **Affichage de la liste** > **Ajouter** > **Ajouter un administrateur** et créez un compte avec les autorisations et le rôle suivants :

  ```
  API Only Only provides access to REST APIs
  ```

- **Option 3 : Créer un utilisateur à l'aide de l'API ONLY avec toutes les autorisations personnalisées de l'API REST**

  Cette option vous permet de sélectionner les API REST spécifiques utilisées par Mobile Security.

  Effectuez les opérations suivantes :

  1. Sur la console d'administration AirWatch, accédez à **Comptes** > **Administrateurs** > **Rôles** et créez un rôle avec les autorisations spécifiques de l'API REST utilisée par Mobile Security, comme indiqué dans le tableau suivant :

Catégorie	Nom
Gestion des utilisateurs administrateurs	Rechercher un utilisateur administrateur

CATÉGORIE	NOM
Gestion WTag	Créer une balise
	Rechercher une balise
	Ajouter des dispositifs à la balise
	Supprimer les dispositifs de la balise
	Récupérer des dispositifs avec une balise spécifique
Gestion des groupes Smart	Créer un groupe Smart
	Rechercher des groupes Smart
	Supprimer les groupes Smart
Gestion des groupes d'applications	Créer un groupe d'applications
	Rechercher un groupe d'applications
	Récupérer les détails du groupe d'applications
	Ajouter une application à un groupe d'applications
	Supprimer l'application du groupe d'applications
Gestion des applications	Installation de l'application interne : Charger des blocs d'application (iOS et Android)
	Installation de l'application interne : Commencer l'installation de l'application interne
Gestion de dispositifs	Récupérer les informations sur le dispositif
	Recherche poussée de dispositif
	Informations sur le nombre de dispositifs

2. Accédez à **Comptes** > **Administrateurs** > **Affichage de la liste** > **Ajouter** > **Ajouter un administrateur** et ajoutez un compte avec le rôle récemment créé.

Remarque

La page des paramètres d'autorisation REST d'AirWatch n'a pas d'autorisation pour chaque API, mais fournit de nombreuses séries d'API telles que les API d'administration ou d'applications, par exemple. Contactez l'assistance technique d'AirWatch pour savoir quelles autorisations de l'API REST doivent être activées sur la page des paramètres.

Configuration de l'intégration d'AirWatch

Procédure

1. Connectez-vous à la console Web d'administration de Mobile Security.
2. Cliquez sur **Administration** > **Paramètres du serveur de communication** sur la barre de menu, puis assurez-vous que les paramètres du serveur de communication sont configurés. Si les paramètres ne sont pas configurés, reportez-vous à la rubrique *Configuration des paramètres du serveur de communication* du *Guide d'installation et de déploiement* pour les étapes de configuration.
3. Cliquez sur **Administration** > **Paramètres du déploiement**.
4. Dans la section **Serveur**, sélectionnez **Analyse de sécurité**, puis sélectionnez **AirWatch** MDM Solution dans la liste déroulante.
5. Dans la section **Enregistrer le service**, configurez les paramètres AirWatch suivants :
   - **URL de l'API**
   - **Clé de l'API**
   - **Compte**
   - **Mot de passe**
6. Cliquez sur **Vérifier les paramètres** pour vous assurer que Mobile Security peut se connecter au serveur AirWatch.
7. Dans la section **Paramètres de synchronisation de données**, configurez les éléments suivants :

- **Préfixe de catégorie de sécurité**

Remarque

Mobile Security utilise un préfixe pour créer trois (3) classes (Dangerous, Risky et NO_TMMS) et balise les dispositifs à risque de la façon suivante :

- XXXX_Dangerous
- XXXX_Risky
- XXXX_NO_TMMS

Les dispositifs et les applications à risque sont regroupés respectivement sous **Groupes Smart** et **Groupes d'applications**. Ils comprennent les applications dont la balise et la catégorie ont été ajoutées comme préfixe à leur nom.

- Groupes Smart : XXXX_Dangerous, XXXX_Risky, XXXX_NO_TMMS.
- Groupes d'application : XXXX_Malware_App_Android, XXXX_Privacy_App_Android, XXXX_Vulnerability_App_Android, XXXX_Malware_App_iOS

Déploiement d'agents

Trend Micro Mobile Security vous permet de déployer un agent client à partir de deux sources :

- **Google Play Store** : Vous devez configurer AirWatch pour déployer l'agent de dispositif mobile et fournir les informations d'inscription aux utilisateurs sous forme de texte ou de code QR. Les utilisateurs peuvent se servir des informations d'inscription ou scanner le code QR pour s'inscrire sur le serveur. Les informations d'inscription comprennent l'adresse IP et le numéro de port du serveur ainsi qu'une clé d'inscription disponible dans l'onglet **Agent Android** sur l'écran **Paramètres de déploiement**.

  Après l'installation de l'agent de dispositif mobile, les utilisateurs devront s'inscrire manuellement sur le serveur Mobile Security. Si vous déployez un agent de dispositif mobile depuis Google Play Store, les utilisateurs de dispositifs mobiles peuvent recevoir des mises à jour en temps réel via Google Play.

- **Serveur Mobile Security** : Demandez aux utilisateurs de télécharger l'agent de dispositif mobile portant le nom : **ENT Security**, à partir d'AirWatch App Store.

  Si vous utilisez cette option de déploiement, vous devrez fournir les informations d'inscription aux utilisateurs sous forme de texte ou de code QR. Les utilisateurs peuvent se servir des informations d'inscription ou scanner le code QR pour s'inscrire sur le serveur. Les informations d'inscription comprennent l'adresse IP et le numéro de port du serveur, ainsi qu'une clé d'inscription disponible dans l'onglet **Agent Android** sur l'écran **Paramètres de déploiement**. Chaque fois qu'un utilisateur lance l'agent de dispositif mobile, il doit inscrire l'application sur le serveur Mobile Security. Vous pouvez également configurer l'application pour l'inscrire automatiquement. Toutefois, chaque fois qu'une mise à jour est disponible, les utilisateurs de dispositifs mobiles devront mettre manuellement à jour leurs agents de dispositif mobile.

  Sur les dispositifs mobiles Samsung, la console d'administration AirWatch vous permet de déployer et de configurer l'agent de dispositif mobile automatiquement.

Déploiement de l'agent Android au moyen de Google Play Store

Procédure

1. Connectez-vous à la console Web AirWatch, puis accédez à **Applications et livres** > **Affichage de la liste** > **Public (onglet)** > **AJOUTER UNE APPLICATION**.
2. Dans l'écran **Ajouter une application**, configurez les champs suivants :
   - **Géré par** : Tapez `Trend Micro`.
   - **Plate-forme** : Sélectionnez **Android** dans la liste déroulante.
   - **Source** : Sélectionnez **Rechercher dans l'App Store**.
   - **Nom** : Tapez `ent security` pour effectuer une recherche dans l'App Store.
3. Cliquez sur **Suivant**.
4. Dans les résultats de recherche, sélectionnez **Enterprise Mobile Security**.

5. Dans l'écran **Ajouter une application**, cliquez sur l'onglet **Attribution**, puis sélectionnez les groupes attribués dans le champ **Groupes attribués**.

6. Cliquez sur **Enregistrer et publier**.

7. Cliquez sur **Charger**.

Mobile Security recompresse l'agent Android avec la clé d'inscription, puis le charge sur le serveur. Si aucune clé d'inscription prédéfinie n'a été configurée, Mobile Security génère une clé d'inscription avant de recompresser l'agent Android.

Remarque

Pour les dispositifs mobiles Samsung, vous pouvez également configurer la fonction de lancement automatique de l'agent Android Mobile Security sur la console Web AirWatch. Pour plus de détails, reportez-vous à l'article suivant :

https://success.trendmicro.com/solution/1115842

Que faire ensuite

Après le déploiement de l'agent Android, fournissez les informations d'inscription aux utilisateurs sous forme de texte ou de code QR. Les utilisateurs peuvent se servir des informations d'inscription ou scanner le code QR pour s'inscrire sur le serveur. Les informations d'inscription comprennent l'adresse IP et le numéro de port du serveur ainsi qu'une clé d'inscription disponible dans l'onglet **Agent Android** sur l'écran **Paramètres de déploiement**.

Déploiement de l'agent Android au moyen du serveur Mobile Security

Procédure

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

2. Cliquez sur **Administration** > **Paramètres d'inscription des dispositifs** dans la barre de menus.

3. Dans l'onglet **Authentification**, sélectionnez **Authentifier à l'aide de Clé d'inscription**, puis sélectionnez **Utilisez la clé d'inscription prédéfinie**.

4. Cliquez sur **Administration** > **Paramètres du déploiement** > **Agent Android (onglet)**.

5. Sélectionnez **Télécharger depuis le serveur TMMS**, puis sélectionnez **Inscription automatique**.

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

7. Cliquez sur **Charger**, puis sélectionnez le fichier modifié de l'agent Mobile Security à charger sur le serveur AirWatch.

   L'agent du dispositif mobile se charge et s'affiche sur la console Web d'administration d'AirWatch.

Que faire ensuite

Après le déploiement de l'agent Android, fournissez les informations d'inscription aux utilisateurs sous forme de texte ou de code QR. Les utilisateurs peuvent se servir des informations d'inscription ou scanner le code QR pour s'inscrire sur le serveur. Les informations d'inscription comprennent l'adresse IP et le numéro de port du serveur ainsi qu'une clé d'inscription disponible dans l'onglet **Agent Android** sur l'écran **Paramètres de déploiement**.

Configuration du lancement automatique de dispositifs mobiles Android

Avant de commencer

Avant d'effectuer la procédure, vous devez effectuer toutes les étapes expliquées dans la section *Déploiement de l'agent Android au moyen du serveur Mobile Security à la page 3-12*.

Procédure

1. Ouvrez une session sur la console Web AirWatch et accédez à **Dispositifs** > **Intermédiaire et mise en service** > **Composants** > **Fichiers/Actions**.

2. Configurez **Fichiers/Actions** depuis la console AirWatch. Effectuez les opérations suivantes :

   a. Accédez à **Dispositifs** > **Intermédiaire et mise en service** > **Composants** > **Fichiers/Actions**.

   b. • Cliquez sur **Ajouter** > **Android**.

   c. Dans l'onglet **Général**, renseignez les champs **Nom** et **Description**.

   d. Dans l'onglet **Manifeste**, cliquez sur **Ajouter une action**, sous la section **Installer le manifeste**.

   e. Dans les options **Ajouter un manifeste**, configurez les informations suivantes, puis cliquez sur **Enregistrer** :

      • **Action(s) à exécuter**: Exécuter Intent

      • **Ligne de commande et arguments à exécuter**:

      ```
      mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.trendmicro.tmmssuite.enterprise,class=com.trendmicro.tmmssuite.enterprise.ui.TmmsEnterpriseSplashScreen
      ```

      • Délai d'expiration : [toute durée correspondant à vos spécifications]

   f. Dans l'écran **Ajouter des fichiers/actions**, cliquez sur **Enregistrer**.

3. Configuration du produit. Effectuez les opérations suivantes :

   a. Accédez à **Dispositifs** > **Intermédiaire et mise en service** > **Affichage de la liste de produits**.

   b. • Cliquez sur **Ajouter un produit** > **Android**.

   c. Dans l'onglet **Général**, renseignez les champs **Nom**, **Description** et **Groupes attribués**.

   d. Dans l'onglet **Manifeste**, cliquez sur **Ajouter** pour ajouter le manifeste.

   e. Dans les options **Ajouter un manifeste**, configurez les informations suivantes, puis cliquez sur **Enregistrer** :

      • **Action(s) à exécuter**: Installer les fichiers/actions

- **Fichiers/Actions**:

  `TestLauncher`

f. Dans l'écran **Ajouter un produit**, cliquez sur **Enregistrer**.

4. Configuration de l'application. Effectuez les opérations suivantes :

   a. Attribuez l'agent TMMS à un groupe Smart.

   b. Définissez **Mode de Push** sur **Auto**.

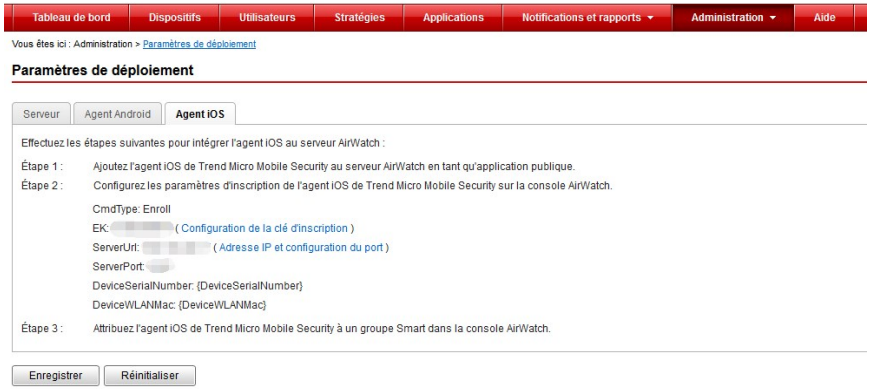
Déploiement de l'agent iOS

Procédure

1. Ouvrez une session sur la console Web AirWatch et accédez à **Applications et livres** > **Applications** > **Affichage de la liste**.
2. Dans l'onglet **Public**, cliquez sur **AJOUTER UNE APPLICATION**.
3. Dans l'écran **Ajouter une application**, configurez les champs suivants :
   - **Géré par** : Tapez `Trend Micro`.
   - **Plate-forme** : Sélectionnez **Apple iOS**.
   - **Source** : Sélectionnez **Rechercher dans l'App Store**.
   - **Nom** : Tapez **ENT Security**
4. Cliquez sur **Suivant**.
5. Dans les résultats de recherche, cliquez sur **Sélectionner** avant **Mobile Security for Enterprise Agent**.
6. Dans l'onglet **Déploiement**, sélectionnez **Envoyer la configuration de l'application**, puis configurez l'application sous le champ **Configuration de l'application**.

   Pour connaître les valeurs de configuration de l'application, reportez-vous à l'écran **Paramètres du déploiement** de la console Web d'administration de Mobile

Security présenté dans la figure ci-dessous. (**Administration** > **Paramètres du déploiement**)



Clé de configuration	Type de valeur	Valeur de configuration
CmdType	Chaîne	S'inscrire
EK	Chaîne	<Clé d'inscription>
ServerUrl	Chaîne	<URL réelle du serveur>
ServerPort	Chaîne	<Numéro de port réel du serveur>
DeviceSerialNumber	Chaîne	{DeviceSerialNumber}
DeviceWLANMac	Chaîne	{DeviceWLANMac}

7. Cliquez sur **Enregistrer et publier**.

8. Dans l'écran **Afficher l'attribution des dispositifs**, cliquez sur **Publier**.

Intégration à MobileIron

Trend Micro Mobile Security vous permet d'intégrer les solutions MobileIron MDM suivantes à Mobile Security :

- MobileIron Core hébergé
- MobileIron Core sur site

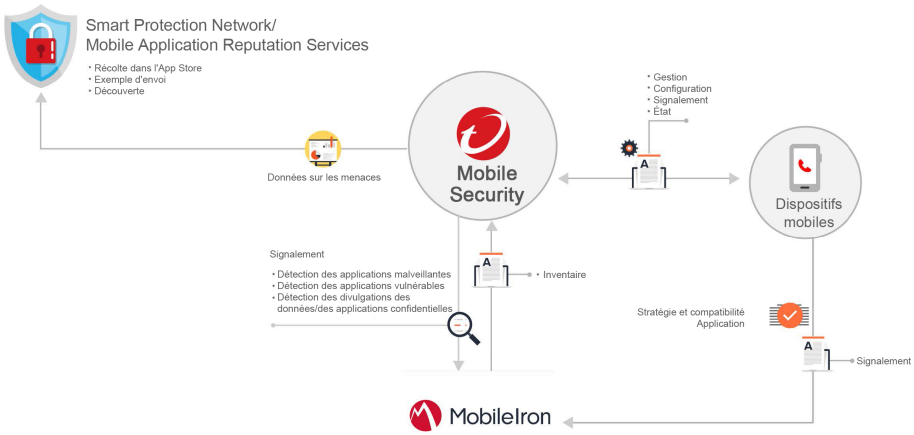
Conditions requises pour l'intégration

Pour intégrer d'autres solutions MDM à Trend MicroMobile Security, vous devez utiliser les éléments suivants :

- Mobile Security for Enterprise 9.7 ou version ultérieure
- Serveur de communication local ou Serveur de communication du nuage configuré dans Mobile Security
- MobileIron v9.3 ou version ultérieure
- Compte d'administrateur sur la console Web d'administration MobileIron

Architecture d'intégration à MobileIron

L'image suivante illustre l'architecture de haut niveau d'intégration à MobileIron.



Mobile App Reputation est une technologie cloud qui identifie automatiquement les menaces mobiles sur la base du comportement des applications, collecte un grand nombre d'applications Android de divers marchés Android, identifie des programmes mobiles malveillants existants et récents, identifie les applications pouvant compromettre la confidentialité et utiliser de façon abusive les ressources des dispositifs. Il s'agit du premier service d'évaluation automatique d'applications mobiles au monde.

Trend Micro Smart Protection Network fournit des informations globales et interactives contre les menaces immédiates pour garantir une protection permanente. Trend Micro utilise ces informations pour instantanément contrer les attaques avant qu'elles puissent vous nuire. **Smart Protection Network** agit sur tous les produits et services Trend Micro.

Mobile Security utilise Smart Protection Network et Mobile Application Reputation Services pour détecter des problèmes de sécurité de dispositif mobile et utilise la stratégie de conformité MobileIron pour gérer votre dispositif mobile.

Fonctionnalités d'intégration

Trend MicroMobile Security fournit les fonctionnalités suivantes avec l'intégration à AirWatch :

FONCTION	DESCRIPTION
Regroupement automatique de dispositifs mobiles	Mobile Security ajoute les préfixes Dangerous, Risky et NO_TMMS pour baliser les dispositifs mobiles en fonction de leur niveau de risque. Voir *Regroupement automatique de dispositifs mobiles à la page 3-19* pour plus de détails.
Déploiement automatique de l'application Mobile Security Client	Vous pouvez configurer MobileIron pour déployer automatiquement l'agent de dispositif mobile sur les dispositifs mobiles. • **Android** : Voir *Déploiement de l'agent Android au moyen du serveur Mobile Security à la page 3-23* pour la procédure. • **iOS** : Voir *Déploiement de l'agent iOS à la page 3-24* pour la procédure.

Regroupement automatique de dispositifs mobiles

Mobile Security utilise des préfixes pour créer trois (3) classes (Dangerous, Risky et NO_TMMS) et balise les dispositifs à risque de la façon suivante :

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

Mobile Security vous permet de définir des préfixes (PREDEFINEDPREFIX) dans la console Web d'administration. Lorsque Mobile Security détecte une application malveillante, il modifie automatiquement le groupe Smart du dispositif.

Par exemple, si Mobile Security détecte un programme malveillant sur un dispositif mobile, il transfère automatiquement le dispositif mobile vers le groupe PREDEFINEDPREFIX _Dangerous.

Configuration de l'intégration de MobileIron

Procédure

1. Connectez-vous à la console Web d'administration de Mobile Security.
2. Cliquez sur **Administration** > **Paramètres du serveur de communication** sur la barre de menu, puis assurez-vous que les paramètres du serveur de communication sont configurés. Si les paramètres ne sont pas configurés, reportez-vous à la rubrique *Configuration des paramètres du serveur de communication* du *Guide d'installation et de déploiement* pour les étapes de configuration.
3. Cliquez sur **Administration** > **Paramètres du déploiement**.
4. Sous la section **Serveur**, sélectionnez **Analyse de sécurité**, puis sélectionnez la solution MDM **MobileIron Core Hosted** ou **MobileIron Core On-Premise** dans la liste déroulante.
5. Dans la section **Enregistrement du service**, configurez les paramètres MobileIron suivants :
   - **URL de l'API**
   - **Nom du compte**
   - **Mot de passe**
6. Cliquez sur **Vérifier les paramètres** pour vous assurer que Mobile Security peut se connecter au serveur MobileIron.
7. Dans la section **Paramètres de synchronisation de données**, configurez les éléments suivants :
   - **Préfixe de catégorie de sécurité**

Remarque

Mobile Security utilise un préfixe pour créer trois (3) classes (Dangerous, Risky et NO_TMMS) et balise les dispositifs à risque de la façon suivante :

- XXXX_Dangerous
- XXXX_Risky
- XXXX_NO_TMMS

Déploiement d'agents

Trend Micro Mobile Security vous permet de déployer un agent client à partir de deux sources :

- **Google Play Store** : Vous devez configurer MobileIron pour déployer l'agent de dispositif mobile et fournir les informations d'inscription aux utilisateurs sous forme de texte ou de code QR. Les utilisateurs peuvent se servir des informations d'inscription ou scanner le code QR pour s'inscrire sur le serveur. Les informations d'inscription comprennent l'adresse IP et le numéro de port du serveur ainsi qu'une clé d'inscription disponible dans l'onglet **Agent Android** sur l'écran **Paramètres de déploiement**.

  Après l'installation de l'agent de dispositif mobile, les utilisateurs devront s'inscrire manuellement sur le serveur Mobile Security. Si vous déployez un agent de dispositif mobile depuis Google Play Store, les utilisateurs de dispositifs mobiles peuvent recevoir des mises à jour en temps réel via Google Play.

- **Serveur Mobile Security** : Demandez aux utilisateurs de télécharger l'agent de dispositif mobile portant le nom : **ENT Security**, à partir de MobileIron App Store.

  Si vous utilisez cette option de déploiement, vous devrez fournir les informations d'inscription aux utilisateurs sous forme de texte ou de code QR. Les utilisateurs peuvent se servir des informations d'inscription ou scanner le code QR pour s'inscrire sur le serveur. Les informations d'inscription comprennent l'adresse IP et le numéro de port du serveur, ainsi qu'une clé d'inscription disponible dans l'onglet **Agent Android** sur l'écran **Paramètres de déploiement**. Chaque fois qu'un utilisateur lance l'agent de dispositif mobile, il doit inscrire l'application sur le

serveur Mobile Security. Vous pouvez également configurer l'application pour l'inscrire automatiquement. Toutefois, chaque fois qu'une mise à jour est disponible, les utilisateurs de dispositifs mobiles devront mettre manuellement à jour leurs agents de dispositif mobile.

Déploiement de l'agent Android au moyen de Google Play Store

Procédure

1. Ouvrez une session dans la console Web MobileIron, puis cliquez sur **Catalogue d'applications** dans la barre de menus.
2. Cliquez sur **Ajouter+**, puis sélectionnez **Google Play**.
3. Dans le champ **Nom de l'application**, tapez `ENT Security` , puis cliquez sur **Rechercher**.
4. Dans les résultats de recherche, sélectionnez **Enterprise Mobile Security**, puis cliquez sur **Suivant**.
5. Ajoutez la description pour **Enterprise Mobile Security**, puis dans la liste déroulante **Catégorie**, sélectionnez la catégorie dans laquelle vous souhaitez placer cette application.
6. Cliquez sur **Terminer**.
7. Cliquez sur **Apps@Work** dans la barre de menus.
8. Dans la section **CATALOGUE APPS@WORK**, sélectionnez **Présenter cette application dans le catalogue Apps@Work**.
9. Cliquez sur **Enregistrer**.

Que faire ensuite

Après le déploiement de l'agent Android, fournissez les informations d'inscription aux utilisateurs sous forme de texte ou de code QR. Les utilisateurs peuvent se servir des informations d'inscription ou scanner le code QR pour s'inscrire sur le serveur. Les informations d'inscription comprennent l'adresse IP et le numéro de port du serveur

ainsi qu'une clé d'inscription disponible dans l'onglet **Agent Android** sur l'écran **Paramètres de déploiement**.

Déploiement de l'agent Android au moyen du serveur Mobile Security

Procédure

1. Connectez-vous à la console Web d'administration de Mobile Security.
2. Cliquez sur **Administration** > **Paramètres d'inscription des dispositifs** dans la barre de menus.
3. Dans l'onglet **Authentification**, sélectionnez **Authentifier à l'aide de Clé d'inscription**, puis sélectionnez **Utilisez la clé d'inscription prédéfinie**.
4. Cliquez sur **Administration** > **Paramètres du déploiement** > **Agent Android (onglet)**.
5. Sélectionnez **Télécharger depuis le serveur TMMS**, puis sélectionnez **Inscription automatique**.
6. Pour **enregistrer** les paramètres, cliquez sur Enregistrer.
7. Cliquez sur **Charger**, puis sélectionnez le fichier modifié de l'agent Mobile Security à charger sur le serveur AirWatch.

   L'agent du dispositif mobile se charge et s'affiche sur la console Web d'administration d'AirWatch.

Que faire ensuite

Après le déploiement de l'agent Android, fournissez les informations d'inscription aux utilisateurs sous forme de texte ou de code QR. Les utilisateurs peuvent se servir des informations d'inscription ou scanner le code QR pour s'inscrire sur le serveur. Les informations d'inscription comprennent l'adresse IP et le numéro de port du serveur ainsi qu'une clé d'inscription disponible dans l'onglet **Agent Android** sur l'écran **Paramètres de déploiement**.

Déploiement de l'agent iOS

Procédure

1. Ouvrez une session dans la console Web MobileIron, puis cliquez sur **Catalogue d'applications**.
2. Cliquez sur **Ajouter+** et sélectionnez **iTunes**.
3. Tapez `ENT Security` dans la zone de recherche, puis cliquez sur **Rechercher**.
4. Sélectionnez **Mobile Security for Enterprise Agent**, puis cliquez sur **Suivant**.
5. Sans modifier les informations, cliquez sur **Suivant**.
6. Dans la section **CATALOGUE APPS@WORK**, sélectionnez **Présenter cette application dans le catalogue Apps@Work**, puis cliquez sur **Suivant**.
7. Cliquez sur **Terminer**.
8. Connectez-vous à la console Web d'administration de Mobile Security.
9. Cliquez sur **Administration** > **Paramètres du déploiement** > **Agent iOS (onglet)**
10. Cliquez sur **Télécharger** pour télécharger le fichier de configuration.

Remarque

Si le bouton **Télécharger** est inactif, assurez-vous d'avoir correctement configuré tous les paramètres à l'étape précédente.

11. Dans la console Web d'administration de MobileIron, accédez à **Stratégies & Configure**.

12. Cliquez sur **Ajouter un nouveau** > **iOS et OS X** > **Configuration de l'application gérée**

13. Tapez les informations suivantes :

    - **Nom**
    - **Description**
    - **BundleId**

14. Cliquez sur **Télécharger** pour télécharger le fichier de configuration.

15. Sélectionnez le fichier de configuration récemment créé, puis cliquez sur **Plus d'actions** > **Appliquer à l'étiquette**.

16. Cliquez sur **Appliquer**.

    Mobile Security envoie la notification **Installation de l'application** aux dispositifs mobiles iOS.

Chapitre 4

Gestion des dispositifs mobiles

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

Le chapitre contient les sections suivantes :

Onglet Dispositifs administrés

L'onglet **Dispositifs administrés** de 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)
- configurer les informations 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, analyser un dispositif et mettre à jour la stratégie
- 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 les sous-groupes suivants :

- **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.

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 Web d'administration de 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 Web d'administration de 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 Web d'administration de Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.

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

Gestion des dispositifs mobiles

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

Réaffectation de dispositifs

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Dispositifs** > **Dispositifs administrés**.

   L'écran **Dispositifs** apparaît.
2. Dans l'arborescence des dispositifs, sélectionnez le dispositif que vous souhaitez réaffecter.

   Les informations sur le dispositif s'affichent.

3. Cliquez sur **Changer d'utilisateur**, puis modifiez le nom d'utilisateur dans le champ prévu à cet effet.

4. Cliquez sur **Enregistrer**.

Modification des informations d'un dispositif mobile

Procédure

1. Connectez-vous à la console Web d'administration de 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.
   - **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 4-6*
- *Suppression de plusieurs dispositifs mobiles à la page 4-6*

Suppression d'un seul dispositif mobile

Procédure

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

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

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

Suppression de plusieurs dispositifs mobiles

Procédure

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

2. Cliquez sur **Dispositifs** dans la barre de menu.

   L'écran **Dispositifs** apparaît.

3. Sur l'onglet **Dispositifs administrés**, cliquez sur le groupe contenant les dispositifs mobiles que vous souhaitez déplacer.

4. Sélectionnez les dispositifs mobiles de la liste dans le volet de droite, puis cliquez sur **Déplacer**.

   La boîte de dialogue **Déplacer les dispositifs** s'affiche.

5. Dans la liste déroulante, sélectionnez le groupe cible, puis cliquez sur **OK**.

État du dispositif mobile

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

- **Éléments de base**—inclut l'état d'enregistrement, le numéro de téléphone, le compte LDAP ainsi que les informations relatives à la plate-forme.
- **Matériel, système d'exploitation**— affiche les informations détaillées du dispositif mobile, dont le nom du dispositif et du modèle, la version du système d'exploitation, les informations relatives à la mémoire, la technologie cellulaire, les numéros IMEI et les numéros MEID ainsi que les informations relatives à la version du micrologiciel.
- **Sécurité** : affiche l'état du débridage, des options pour développeurs, de débogage USB et du déchiffrement du trafic réseau des dispositifs mobiles, le nombre de profils iOS malveillants, de certificats SSL malveillants, d'applications malveillantes, d'applications modifiées, d'applications vulnérables et d'applications présentant un risque de confidentialité ainsi que le point d'accès connecté (Wi-Fi).

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 les informations dans le champ de recherche de 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

- **Nom d'utilisateur** : nom d'utilisateur 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
- **Version de l'agent**—numéro de version des agents du dispositif mobile sur le dispositif mobile
- **Dernière connexion** : plage horaire pendant laquelle un dispositif mobile s'est connecté pour la dernière fois au serveur Mobile Security
- **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 infecté**—limite la recherche aux dispositifs mobiles avec le nombre spécifié de programmes malveillants détectés

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

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 Web d'administration de 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 8-2* pour de plus amples informations.

Mise à jour des informations sur le dispositif mobile

Le serveur Mobile Security obtient automatiquement les informations sur le dispositif depuis des dispositifs mobiles administrés à intervalles programmés et les affiche dans l'écran **Dispositifs**.

Vous pouvez mettre à jour les informations d'un dispositif administré dans l'onglet **Dispositifs administrés** avant la mise à jour automatique programmée suivante.

Procédure

1. Connectez-vous à la console Web d'administration de 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 dans l'arborescence.
4. Cliquez sur **Mise à jour**.

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 Web d'administration de 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.

Intégration avec Trend Micro Control Manager

Trend Micro Mobile Security assure l'intégration avec Trend Micro Control Manager (également dénommé Control Manager ou TMCM). 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 obtenir des informations détaillées sur Trend Micro Control Manager et la gestion des stratégies Mobile Security dans Control Manager, 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 5

Affichage des utilisateurs

Ce chapitre décrit comment afficher les utilisateurs enregistrés dans Mobile Security.

Le chapitre contient les sections suivantes :

Onglet Utilisateurs

Vous pouvez utiliser l'onglet **Utilisateurs** pour afficher tous les dispositifs mobiles enregistrés dans Mobile Security.

Affichage de la liste des utilisateurs

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Utilisateurs**.

   L'écran **Utilisateurs** s'affiche.

2. Pour trier la liste, cliquez sur l'en-tête de l'une des colonnes suivantes.

   - Nom d'utilisateur :
   - Messagerie électronique
   - Dispositifs
   - Invité le

3. Pour rechercher un utilisateur, saisissez son nom ou son adresse de messagerie dans la barre de **recherche**, puis appuyez sur Entrée.

   Si l'utilisateur figure dans la liste, Mobile Security affiche les informations qui s'y rapportent.

Chapitre 6

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

Vous pouvez configurer les stratégies d'un groupe Mobile Security sur le serveur d'administration ou sur tous les dispositifs mobiles inscrits sur Mobile Security.

TABLEAU 6-1. Stratégies de dispositif dans Mobile Security

STRATÉGIE	RÉFÉRENCE
Liste des éléments approuvés	Voir la section *Liste des applications approuvées à la page 6-2*.
Liste des certificats de déchiffrement du trafic réseau de confiance	Voir la section *Liste des certificats de déchiffrement du trafic réseau de confiance à la page 6-3*.

TABLEAU 6-2. Stratégies de groupe dans Mobile Security

GROUPE DE STRATÉGIE	STRATÉGIE	RÉFÉRENCE
Généralités	Stratégie courante	Voir la section *Stratégie courante à la page 6-6*.
Sécurité de dispositif	Stratégie de sécurité	Voir la section *Stratégie de sécurité à la page 6-7*.

Stratégies de tous les dispositifs

Cette section présente les stratégies disponibles dans Mobile Security pour tous les dispositifs mobiles.

Liste des applications approuvées

La **Liste des applications approuvées** comprend toutes les applications susceptibles de présenter un risque de sécurité (programmes malveillants, vulnérables, présentant un risque de confidentialité ou modifiés), mais dont l'installation sur des dispositifs mobiles a été approuvée par l'administrateur.

Pour gérer la **Liste des applications approuvées**, cliquez sur **Stratégies** > **Stratégies de tous les dispositifs**.

Liste des certificats de déchiffrement du trafic réseau de confiance

Si Mobile Security détecte un certificat SSL malveillant, il l'affiche sur l'écran **Détections** > **Certificats SSL malveillants**. Toutefois, vous pouvez ajouter ces certificats considérés comme malveillants à la **Liste des certificats de déchiffrement du trafic réseau de confiance** pour que Mobile Security les ignore lors de l'analyse et pour les masquer de l'écran **Certificats SSL malveillants**.

Pour gérer la **Liste des certificats de déchiffrement du trafic réseau de confiance**, cliquez sur **Stratégies** > **Stratégies de tous les dispositifs**.

Gestion des stratégies de tous les dispositifs

Mobile Security vous permet de gérer une liste des applications approuvées et une liste des certificats de déchiffrement du trafic réseau de confiance pour permettre aux utilisateurs d'utiliser ces applications et ces certificats de déchiffrement du réseau sans restriction ni avertissement.

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

Ajout d'applications à la liste approuvée

Procédure

1. Connectez-vous à la console Web d'administration de Mobile Security.
2. Effectuez l'une des actions suivantes :
   - Ajoutez une application déjà installée et analysée par Mobile Security dans la **Liste approuvée**.
     a. Cliquez sur **Détections** > **État de sécurité de l'application** dans la barre de menus.

b. Cliquez sur l'onglet **Android** ou **iOS**, et sélectionnez les applications de la liste des applications détectées que vous souhaitez ajouter à la **Liste approuvée**.

c. Cliquez sur **Ajouter à la liste approuvée**.

- Ajoutez des applications manuellement à la **Liste approuvée**.

  a. Cliquez sur **Stratégies** > **Stratégies de tous les dispositifs** dans la barre de menus.

  b. Dans la section **Liste des applications approuvées**, cliquez sur l'onglet **Android** ou **iOS**, puis sur **Ajouter à la liste approuvée**.

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

  c. Saisissez l'ID, le nom et la description de l'application dans le champ prévu à cet effet. Séparez les informations relatives à chaque application par un point-virgule (;).

  d. Cliquez sur **Enregistrer** dans l'écran **Importer une application**.

  e. Cliquez sur **Enregistrer** dans l'écran **Stratégie de tous les dispositifs**.

Suppression d'applications de la liste approuvée

Procédure

1. Connectez-vous à la console Web d'administration de Mobile Security.
2. Effectuez l'une des actions suivantes :

   - Supprimez les applications déjà installées et analysées par Mobile Security de la **Liste approuvée**.

     a. Cliquez sur **Détections** > **État de sécurité de l'application** dans la barre de menus.

     b. Cliquez sur l'onglet **Android** ou **iOS**, et sélectionnez les applications de la liste des applications détectées que vous souhaitez supprimer de la **Liste approuvée**.

c. Cliquez sur **Supprimer de la liste approuvée**.

- Supprimez directement une application de la **Liste approuvée**.

  a. Cliquez sur **Stratégies** > **Stratégies de tous les dispositifs** dans la barre de menus.

  b. Dans la section **Liste des applications approuvées**, cliquez sur l'onglet **Android** ou **iOS**, et sélectionnez les applications que vous souhaitez supprimer de la liste.

  c. Cliquez sur **Supprimer de la liste approuvée**.

  d. Cliquez sur **Enregistrer** dans l'écran **Stratégie de tous les dispositifs**.

Ajout d'un certificat de déchiffrement du trafic réseau de confiance

Procédure

1. Connectez-vous à la console Web d'administration de Mobile Security.
2. Cliquez sur **Stratégies** > **Stratégies de tous les dispositifs** dans la barre de menus.

   L'écran **Stratégie de tous les dispositifs** s'affiche.
3. Dans la section **Liste des certificats de déchiffrement du trafic réseau de confiance**, cliquez sur **Ajouter**.

   L'écran **Ajouter un certificat** s'affiche.
4. Sélectionnez un fichier de certificat sur votre disque dur local et saisissez sa description dans le champ **Description**.
5. Sélectionnez **OK**.
6. Cliquez sur **Enregistrer** dans l'écran **Stratégie de tous les dispositifs**.

Suppression d'un certificat de déchiffrement du trafic réseau de confiance

Procédure

1. Connectez-vous à la console Web d'administration de Mobile Security.
2. Cliquez sur **Stratégies** > **Stratégies de tous les dispositifs** dans la barre de menus.

   L'écran **Stratégie de tous les dispositifs** s'affiche.
3. Dans la section **Liste des certificats de déchiffrement du trafic réseau de confiance**, sélectionnez les fichiers de certificat que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
4. Cliquez sur **Enregistrer** dans l'écran **Stratégie de tous les dispositifs**.

Stratégies de tous les groupes

Cette section présente les stratégies disponibles dans Mobile Security pour tous les groupes.

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

  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 protection contre les menaces Internet** ne sont pas affectées lorsque cette option est sélectionnée. Pour plus d'informations, reportez-vous à *Stratégie de sécurité à la page 6-7*.

- Vous pouvez 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.

Stratégie de sécurité

Vous pouvez configurer les **paramètres de sécurité** depuis l'écran **Stratégie de sécurité**.

Remarque

La protection contre les menaces Internet de Mobile Security prend uniquement en charge le navigateur par défaut d'Android et Google Chrome sur les dispositifs mobiles.

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

Le tableau ci-dessous décrit les paramètres disponibles pour cette stratégie.

TABLEAU 6-3. Paramètres de stratégie de sécurité

SECTION	ÉLÉMENT	DESCRIPTION	SE DE DISPOSITIF MOBILE PRIS EN CHARGE
Paramètre de sécurité	**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 les autres fichiers stockés sur le dispositif mobile. Si vous sélectionnez cette option, indiquez si seuls les fichiers APK doivent être analysés, ou si tous les fichiers doivent l'être.	
	Analyse après mise à jour des signatures	Activez cette option si vous souhaitez que la recherche de programmes malveillants ait lieu après chaque mise à jour du fichier de signatures. Mobile Security lance automatiquement une analyse après une mise à jour réussie des signatures sur les dispositifs mobiles Android.	
	Analyse des applications	Activez cette option si vous souhaitez analyser les applications pour rechercher les programmes malveillants, les risques de confidentialité ou les applications vulnérables et modifiées (recompressées).	

SECTION	ÉLÉMENT	DESCRIPTION	SE DE DISPOSITIF MOBILE PRIS EN CHARGE
	Analyse de sécurité du réseau	Ces paramètres analysent le déchiffrement du trafic réseau, les points d'accès dangereux (Wi-Fi) ou les certificats SSL malveillants installés. Toutes les options de cette catégorie sont activées par défaut et ne peuvent pas être modifiées.	
	Analyse des applications vulnérables	Ces paramètres analysent la vulnérabilité du dispositif mobile en raison du débogage USB, des options pour développeurs, des profils malveillants et des dispositifs mobiles débridés.	
	Bloquer le réseau lors de la détection du déchiffrement du trafic réseau	Activez cette option pour arrêter le déchiffrement du trafic réseau lorsque Mobile Security détecte une fuite de données en cours de communication.	
	Bloquer le réseau lorsque le point d'accès suspect (Wi-Fi) semble présenter un risque élevé	Activez cette option pour déconnecter les dispositifs mobiles du réseau si la connexion réseau est soupçonnée d'être fictive.	
	Activer l'analyse programmée sous **Planification d'analyse**	Sélectionnez **Tous les jours**, **Toutes les semaines** ou **Tous les mois** pour exécuter l'analyse respectivement chaque jour, une fois par semaine ou une fois par mois.	
Paramètre de protection contre les	**Activer la stratégie de protection contre les menaces Internet**	Cette fonction vous offre un contrôle côté serveur des stratégies de protection contre les menaces Internet. Vous	

SECTION	ÉLÉMENT	DESCRIPTION	SE DE DISPOSITIF MOBILE PRIS EN CHARGE
menaces Internet	**contrôlée de manière centralisée**	pouvez configurer les niveaux de protection suivants en fonction de vos besoins : • **Faible** : Ce paramètre fournit la protection la plus faible contre la fraude en ligne et les autres activités malveillantes de sites web. • **Normal** : Ce paramètre assure une protection contre les menaces de sécurité en ligne sans bloquer la plupart des sites Web. Trend Micro recommande ce paramètre par défaut. • **Élevé** : Ce paramètre permet de définir la protection maximale contre la fraude en ligne et autres sites web. Il permet d'ouvrir les sites web jouissant d'une très bonne réputation et bloque tous les autres.	
	Filtrer les listes	Mobile Security bloque toutes les URL que vous ajoutez dans la **Liste bloquée** et autorise toutes les URL qui se trouvent dans la **Liste approuvée**.	
	Revérifier l'URL	Si vous repérez une URL susceptible d'avoir été placée dans la mauvaise catégorie, vous pouvez en informer Trend Micro sur le site Web suivant :	

SECTION	ÉLÉMENT	DESCRIPTION	SE DE DISPOSITIF MOBILE PRIS EN CHARGE
		http://sitesafety.trendmicro.com/	

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. Cette fonctionnalité permet également aux dispositifs mobiles de renvoyer au serveur le journal de protection contre les menaces Internet.

Remarque

La protection contre les menaces Internet de Mobile Security ne prend en charge que le navigateur par défaut d'Android et Google Chrome.

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**.

Gestion des stratégies de tous les groupes

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

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

Création d'une stratégie

Procédure

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

2. Cliquez sur **Stratégies** > **Stratégies des groupes** dans la barre de menus.

   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 6-13*.

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 Web d'administration de Mobile Security.
2. Cliquez sur **Stratégies** > **Stratégies des groupes** dans la barre de menus.

   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 Web d'administration de Mobile Security.
2. Cliquez sur **Stratégies** > **Stratégies des groupes** dans la barre de menus.

   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 Web d'administration de Mobile Security.
2. Cliquez sur **Stratégies** > **Stratégies des groupes** dans la barre de menus.

   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 6-13* pour la procédure.

Procédure

1. Connectez-vous à la console Web d'administration de Mobile Security.
2. Cliquez sur **Stratégies** > **Stratégies des groupes** dans la barre de menus.

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

Chapitre 7

Affichage et gestion des détections

Ce chapitre décrit comment gérer les applications malveillantes détectées sur les dispositifs mobiles iOS et Android, et comment afficher les certificats SSL et les profils iOS.

Le chapitre contient les sections suivantes :

À propos de l'écran Applications suspectes

L'écran **Applications suspectes** affiche le nom, la version, l'état de l'analyse de sécurité, le nombre d'installations et l'heure de la dernière analyse de toutes les applications installées sur les dispositifs mobiles.

Vous pouvez également ajouter les applications affichées sur cet écran à la **Liste approuvée** des applications si vous considérez que l'une d'elles est sûre. De la même manière, vous pouvez supprimer les applications que vous avez préalablement ajoutées à la **Liste approuvée**, mais dont vous doutez désormais de la sûreté.

Voir les sections *Ajout d'applications à la liste approuvée à la page 6-3* et *Suppression d'applications de la liste approuvée à la page 6-4* pour les procédures.

Cliquez sur le lien **Gérer la liste approuvée** en haut à droite du tableau pour accéder à l'écran **Liste approuvée** afin de gérer la liste.

Le tableau ci-dessous répertorie les informations disponibles pour les applications Android et iOS.

TABLEAU 7-1. État de sécurité des applications

INFORMATIONS	DESCRIPTION	ANDROID	IOS
Nom de l'application	Nom de l'application	●	●
Version	Numéro de version de l'application	●	●

INFORMATIONS	DESCRIPTION	ANDROID	IOS
Résultat de la recherche de programmes malveillants	La recherche de programmes malveillants peut donner les résultats suivants : • **Normal** : aucun programme malveillant détecté • **Logiciel PUA** : des applications potentiellement indésirables (Potentially Unwanted Applications, ou PUA) sont des applications de type grayware qui peuvent poser pour l'utilisateur un risque élevé en termes de sécurité et/ou de confidentialité. Pour plus d'informations, reportez-vous à http://about-threats.trendmicro.com/fr-fr/definition/potentially-unwanted-app. • **Programmes malveillants** : programmes malveillants connus • **Inconnu** : aucune information disponible	●	●
Résultat de l'analyse de vulnérabilité	L'analyse de la vulnérabilité peut donner les niveaux de risque suivants : • **Normal** • **Moyen** • **Élevé** • **Inconnu** : aucune information disponible	●	

INFORMATIONS	DESCRIPTION	ANDROID	iOS
Résultat de l'analyse de la confidentialité	L'analyse de la confidentialité peut donner les niveaux de risque suivants : • **Normal** • **Moyen** • **Élevé** • **Inconnu** : aucune information disponible	●	
Modifiée	L'analyse des applications modifiées peut donner les résultats suivants : • **Oui** : l'application d'origine a été modifiée ou recompressée, potentiellement à des fins malveillantes • **Non** : aucune modification n'a été apportée à l'application d'origine • **Inconnu** : aucune information disponible	●	●
Nombre d'installations	Nombre de dispositifs sur lesquels l'application est installée	●	●
Dernière analyse	Date et heure de la dernière analyse	●	●

Lorsque Mobile Security analyse les applications à la recherche de risques de sécurité, il prend les mesures suivantes en fonction des résultats de l'analyse de sécurité :

- Affichage de la détection sur le widget **Récapitulatif des risques relatifs à l'application Android/iOS** de l'écran **Tableau de bord**
- Affichage du nombre de risques de sécurité détectés pour le dispositif mobile sur l'écran **Dispositifs** dans la catégorie correspondante
- Génération d'une entrée de journal

Affichage des applications Android suspectes

Procédure

1. Sur la console Web Mobile Security, accédez à l'onglet **Détections** > **Applications suspectes** > **Android**.

   L'onglet **Android** s'affiche.

2. Pour afficher les détails de l'analyse d'une application, cliquez sur les résultats sous l'une des colonnes suivantes.

   - Résultat analyse vulnérab.
   - Résult. analyse confid.

   La page des détails de l'analyse des résultats sélectionnés s'affiche.

3. Pour afficher les dispositifs sur lesquels une application est installée, cliquez sur le nombre qui se trouve sous la colonne **Nombre d'installations**.

   L'écran **Dispositifs** s'affiche et présente la liste des dispositifs dans l'onglet **Dispositifs administrés**.

4. Pour afficher des informations sur une application en particulier, saisissez son nom dans la barre de **recherche**, puis appuyez sur Entrée.

   Si cette application figure dans la liste, les informations à son sujet s'affichent dans le tableau.

Affichage des applications iOS suspectes

Procédure

1. Sur la console Web Mobile Security, accédez à l'onglet **Détections** > **Applications suspectes** > **iOS**.

   L'onglet **iOS** s'affiche.

2. Pour afficher les dispositifs sur lesquels une application est installée, cliquez sur le nombre qui se trouve sous la colonne **Nombre d'installations**.

   L'écran **Dispositifs** s'affiche et présente la liste des dispositifs dans l'onglet **Dispositifs administrés**.

3. Pour afficher des informations sur une application en particulier, saisissez son nom dans la barre de **recherche**, puis appuyez sur Entrée.

   Si cette application figure dans la liste, les informations à son sujet s'affichent dans le tableau.

Affichage des certificats SSL malveillants

L'écran **Certificats SSL malveillants** affiche les certificats SSL considérés comme malveillants par Mobile Security et installés sur des dispositifs mobiles Android ou iOS. Si vous approuvez l'un des certificats répertoriés dans l'écran **Certificats SSL malveillants**, vous pouvez l'ajouter à la *Liste des certificats de déchiffrement du trafic réseau de confiance à la page 6-3* pour le masquer de l'écran **Certificats SSL malveillants**.

Lorsque Mobile Security détecte un certificat malveillant, il prend les mesures suivantes :

- Affichage du certificat SSL malveillant sur l'écran **Certificats SSL malveillants**
- Affichage de la détection sur le widget **Récapitulatif de la protection du réseau** de l'écran **Tableau de bord**
- Mise à jour de l'état de sécurité du dispositif sur **Dangereux**
- Envoi d'une notification par courriel à l'administrateur
- Génération d'une entrée de journal

Les détails du certificat affiché sur l'écran **Certificats SSL malveillants** comprennent le nom et les détails du certificat, le nombre de fois où il a été installé sur des dispositifs mobiles et l'heure de la dernière analyse.

Procédure

1. Sur la console Web Mobile Security, accédez à **Détections** > **Certificats SSL malveillants**.

   L'écran **Certificats SSL malveillants** s'affiche.

2. Cliquez sur l'onglet **Android** ou **iOS**.

3. Pour afficher des informations sur une application en particulier, saisissez son nom dans la barre de **recherche**, puis appuyez sur Entrée.

   Si cette application figure dans la liste, les informations à son sujet s'affichent dans le tableau.

Affichage des profils iOS malveillants

L'écran **Profils iOS malveillants** affiche les profils iOS considérés comme malveillants par Mobile Security et installés sur des dispositifs mobiles Android ou iOS.

Lorsque Mobile Security détecte un profil iOS malveillant, il prend les mesures suivantes :

- Affichage du profil iOS malveillant sur l'écran **Profils iOS malveillants**
- Affichage de la détection sur le widget **Récapitulatif de la protection du réseau iOS** de l'écran **Tableau de bord**
- Mise à jour de l'état du dispositif sur **Dangereux**
- Envoi d'une notification par courriel à l'administrateur
- Génération d'une entrée de journal

Les détails du profil affiché sur l'écran **Profils iOS malveillants** comprennent le nom, le type et le résultat de l'analyse du profil, le nombre de fois où il a été installé sur des dispositifs mobiles et l'heure de la dernière analyse.

Procédure

1. Sur la console Web Mobile Security, accédez à **Détections** > **Profils iOS malveillants**.

   L'écran **Profils iOS malveillants** s'affiche.

2. Pour afficher des informations sur un profil iOS particulier, saisissez le nom du certificat dans la barre de **recherche** et appuyez sur **Entrée**.

   Si cette application figure dans la liste, les informations à son sujet s'affichent dans le certificat.

Chapitre 8

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

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 8-4* pour plus d'informations).

Procédure

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

   L'écran **Mises à jour** s'affiche.
3. Cliquez sur l'onglet **Manuelles**.
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 8-2* 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 8-4* pour plus d'informations).

Procédure

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

   L'écran **Mises à jour** s'affiche.
3. Cliquez sur l'onglet **Programmées**.
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 ils ont 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 mises à jour hebdomadaires, indiquez le jour de la semaine (par exemple, dimanche, lundi, etc.)
   - Pour les mises à jour 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 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 Web d'administration de 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 8-2* ou pour la mise à jour programmée, consultez *Mise à jour programmée à la page 8-3*.

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

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** : saisissez le chemin d'accès de l'emplacement du fichier source.
     - **Nom d'utilisateur** et **Mot de passe** : saisissez le nom d'utilisateur et le 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 9

Affichage et maintenance des journaux

Ce chapitre décrit comment afficher les journaux 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

Mobile Security gère les types de journaux suivants :

- **Journaux d'administrateur** : Lorsqu'un administrateur effectue une configuration sur la console Web d'administration, Mobile Security génère un journal sur le serveur d'administration.
- **Journaux d'agent de dispositif mobile** : Lorsque les agents de dispositif mobile génèrent un journal d'analyse de l'application, de vulnérabilité du dispositif, de protection du réseau ou de protection contre les menaces Internet, 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.

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 :

- Journaux d'analyse de l'application : ces journaux sont générés lorsque l'agent de dispositif mobile détecte un programme malveillant, une menace pour la confidentialité, un risque de vulnérabilité ou une application modifiée sur un dispositif mobile.
- Journaux de vulnérabilité du dispositif : ces journaux sont générés en cas d'activation des options pour développeurs ou du mode débogage USB, ou en cas de détection d'un profil iOS malveillant sur un dispositif mobile ou d'un dispositif mobile débridé.
- Journaux de protection du réseau : ces journaux sont générés en cas de détection d'un déchiffrement du trafic réseau, d'un point d'accès dangereux (Wi-Fi) ou d'un certificat SSL malveillant sur un dispositif mobile.

- Journaux de protection contre les menaces Internet : l'agent de dispositif mobile génère un journal de protection contre les menaces Internet lorsqu'il bloque une page Web dangereuse ou contenant un programme malveillant et le charge sur le serveur.

Procédure

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

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

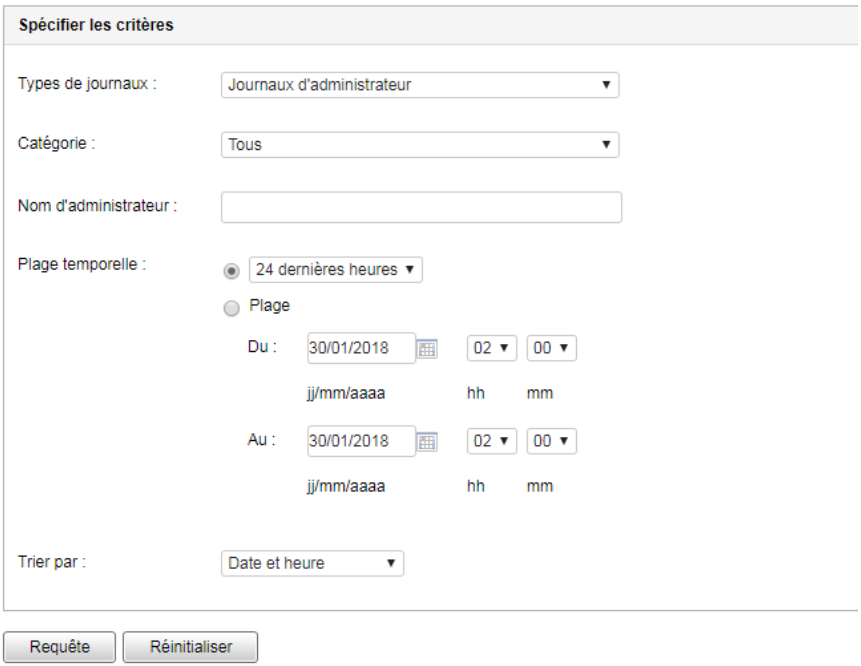


FIGURE 9-1. Écran Requête de journaux

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 d'administrateur** ou **Nom du dispositif** : saisissez le nom de l'administrateur ou du dispositif dont vous souhaitez rechercher les journaux.
- **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 selon un programme défini dans l'écran Maintenance des journaux.

Planification de suppression de journaux

Procédure

1. Connectez-vous à la console Web d'administration de 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.
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 Web d'administration de 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 10

Utilisation des notifications et rapports

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

Le chapitre contient les sections suivantes :

À propos des messages de notification et des rapports

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

- **Notifications administrateur**—envoie une notification par courriel à l'administrateur en cas d'anomalie du système.
- **Rapports**—envoie des rapports par courriel aux destinataires spécifiés.
- **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 Web d'administration de 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 administrateur

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

- **Avertissement de détection de programmes malveillants en temps réel** : envoie une notification par courriel à l'administrateur lorsque l'agent détecte un programme malveillant.
- **Avertissement de certificat malveillant** : envoie une notification par courriel à l'administrateur lorsque l'agent détecte un certificat malveillant.
- **Avertissement de profil iOS malveillant** : envoie une notification par courriel à l'administrateur lorsque l'agent détecte un profil iOS malveillant.
- **Erreur système**—envoie une notification par courriel à l'administrateur en cas d'anomalie du système. Les variables de jetons `<%PROBLEM%>`, `<%REASON%>` et `<%SUGGESTION%>` seront remplacées par le problème, la raison et la suggestion réels en vue de résoudre le problème.
- **Avertissement d'expiration du certificat APNs** : envoie une notification par courriel à l'administrateur un mois avant que le certificat APNs expire.

Activation des notifications administrateur

Procédure

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

   L'écran **Notifications 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 et rapports** > **Notifications administrateur**.

   L'écran **Notifications 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.

4. Cliquez sur **Enregistrer**.

Rapports

Mobile Security vous permet de générer et d'envoyer les rapports suivants :

- **Rapport de sécurité** : affiche des informations sur les programmes malveillants détectés, les applications modifiées, les risques de confidentialité, les applications vulnérables, le déchiffrement du trafic réseau, le point d'accès dangereux (Wi-Fi), le certificat SSL malveillant, le profil iOS malveillant, les options pour développeurs, l'état du débogage USB et du débridage ainsi que les dix (10) principaux sites Web bloqués.

- **Rapport d'inventaire des dispositifs**—affiche des informations complètes sur tous les dispositifs administrés.
- **Rapport d'enregistrement des dispositifs**—affiche des informations sur l'inscription du dispositif.

Vous pouvez effectuer les tâches suivantes depuis l'écran **Rapports**.

TABLEAU 10-1. Tâches liées aux rapports

TÂCHES	DESCRIPTION
Générer	Vous pouvez générer de nouveaux rapports lorsque vous en avez besoin. Pour plus d'informations, reportez-vous à *Génération de rapports à la page 10-5*.
Afficher	Vous pouvez afficher les derniers rapports générés depuis l'onglet À la demande. Pour plus d'informations, reportez-vous à *Affichage de rapports à la page 10-6*.
Envoyer	Vous pouvez envoyer des rapports par courriel à tout moment. Pour plus d'informations, reportez-vous à *Envoi de rapports à la page 10-7*.
Programmer	Vous pouvez spécifier un programme fixe pour l'envoi de rapports aux administrateurs et à d'autres utilisateurs. Pour plus d'informations, reportez-vous à *Programmation de rapports à la page 10-8*.

Génération de rapports

Remarque

Mobile Security ne conserve qu'une copie de chaque type de rapport sur le serveur.

Enregistrez une copie du dernier rapport en date avant d'en générer un nouveau.

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Notifications et rapports** > **Rapports** > **À la demande**.

   L'écran **À la demande** s'affiche.

2. Sélectionnez la période.

   - Aujourd\'hui
   - 7 derniers jours
   - 30 derniers jours

3. Sélectionnez toutes les plates-formes de dispositifs ou l'une d'entre elles.

   - Tous types
   - iOS
   - Android

4. Sélectionnez les informations utilisateur à inclure dans le rapport.

   - Tous
   - Spécifique

5. Sélectionnez les rapports à générer.

6. Cliquez sur **Générer**.

   Mobile Security génère les rapports sélectionnés et écrase toutes les versions précédentes.

Affichage de rapports

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Notifications et rapports** > **Rapports**.

2. Accédez au rapport que vous souhaitez afficher depuis l'un des onglets suivants.
   - **À la demande** : sélectionnez cet onglet pour afficher des rapports à la demande.
   - **Programmé** : sélectionnez cet onglet pour afficher des rapports programmés.
3. Cliquez sur **Afficher**.

Remarque

Si le lien n'apparaît pas, c'est que vous devez tout d'abord générer ce rapport.

Pour plus d'informations, reportez-vous à *Génération de rapports à la page 10-5*

Le rapport sélectionné s'ouvre dans un nouvel onglet ou une nouvelle fenêtre.

Envoi de rapports

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Notifications et rapports** > **Rapports** > **À la demande**.

   L'écran **À la demande** s'affiche.
2. Accédez au rapport que vous souhaitez envoyer dans le tableau **Rapport**.
3. Cliquez sur **Envoyer**.

Remarque

Si le lien n'apparaît pas, c'est que vous devez tout d'abord générer ce rapport.

Pour plus d'informations, reportez-vous à *Génération de rapports à la page 10-5*

L'écran **Envoyer le rapport** s'affiche.

4. Saisissez l'adresse de messagerie du destinataire.

5. Vous avez la possibilité de modifier l'objet et le corps du message.
6. Cliquez sur **Envoyer**.

   Un message de confirmation s'affiche.

Programmation de rapports

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Notifications et rapports** > **Rapports** > **Programmé**.

   L'écran **Programmé** s'affiche.
2. Sélectionnez la fréquence des rapports dans la liste déroulante.
   - **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.
3. Cliquez sur **Enregistrer**.

Modification du modèle de courriel

Procédure

1. Sur la console Web d'administration de Mobile Security, accédez à **Notifications et rapports** > **Rapports** > **Programmé**.

   L'écran **Programmé** s'affiche.
2. Cliquez sur le nom du rapport.

   L'écran **Paramètres de courriel** du rapport sélectionné 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 du sujet de l'e-mail contenant le rapport.
   - **Message** : Corps du message du rapport.

4. Cliquez sur **Enregistrer**.

   Un message de confirmation s'affiche.

Notifications 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.

Configuration des notifications utilisateur

Procédure

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

   L'écran **Notifications utilisateur** 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 11

Dépannage et contact de l'assistance technique

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

Le chapitre contient les sections suivantes :

Dépannage

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

- **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.

- **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**.

- **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. Accédez 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

Contacter 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	http://www.trendmicro.fr
Adresse de messagerie	support@trendmicro.com

- 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℠ 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 logicielles

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**—Un correctif constitue un contournement ou une solution à un problème unique signalé par un client. Les correctifs résolvent un problème précis et ne sont donc pas proposés à tous les clients. Contrairement aux autres, les correctifs Windows contiennent un programme d'installation (vous devez généralement arrêter les démons, copier le fichier pour remplacer le fichier correspondant dans votre installation et redémarrer les démons).
- **Patch de sécurité**—Un patch de sécurité est un correctif relatif à des problèmes de sécurité, qui peut être déployé chez tous les clients. Les patchs de sécurité

Windows contiennent un programme d'installation alors que les patchs non-Windows incluent en général un script d'installation.

- **Patch**—Un patch est un groupe de correctifs et de patchs de sécurité qui résolvent plusieurs problèmes logiciels. Trend Micro publie régulièrement des patchs. Les patchs Windows contiennent un programme d'installation alors que les patchs non-Windows incluent en général un script d'installation.
- **Service Pack**—Un service pack est une consolidation de correctifs à chaud, de patchs et d'améliorations suffisamment significative pour être considérée comme une mise à niveau du produit. Les services packs Windows et non-Windows contiennent un programme d'installation et un script d'installation.

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

http://esupport.trendmicro.com

Consultez le site Web de Micro Trend régulièrement pour télécharger des patchs et des 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, de patch ou de 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

TREND MICRO INCORPORATED
Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France
Tél. : +33 (0) 1 76 68 65 00 info@trendmicro.com

www.trendmicro.com
Item Code: TSCM98148/180126