



9.0 TREND MICRO™ Mobile Security™ SP2

Manuel d'installation et de déploiement

Sécurité complète pour portables d'entreprise



Endpoint Security

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

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

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

Copyright © 2014. Trend Micro Incorporated. Tous droits réservés.

Référence document TFSM96395/140410

Date de publication : Septembre 2014

La documentation utilisateur de Trend Micro™ Mobile Security 9.0 SP2 for Enterprise présente les fonctions principales du produit et fournit les instructions d'installation pour votre environnement de production. Lisez entièrement la documentation avant d'installer ou d'utiliser le produit.

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

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

Vous pouvez évaluer cette documentation sur le site Web suivant :

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

Table des matières

Préface

Préface	v
Public ciblé	vi
Documentation de Mobile Security	vi
Conventions typographiques du document	vii

Chapitre 1: Préparation de l'installation du serveur

Architecture du système Mobile Security	1-2
Modèle de sécurité renforcée (installation de deux serveurs) avec le serveur de communication du nuage	1-3
Modèle de sécurité renforcée (installation de deux serveurs) avec Serveur de communication local	1-4
Modèle de sécurité de base (installation sur un serveur)	1-4
Composants du système Mobile Security	1-5
Comparaison entre le serveur de communication local et le serveur du nuage	1-8
Configuration minimale requise	1-9

Chapitre 2: Configuration de l'environnement

Configuration de l'environnement pour l'installation de Mobile Security	2-2
Configuration de l'environnement pour les dispositifs mobiles iOS (Facultatif)	2-4
Configuration de l'environnement pour les dispositifs mobiles BlackBerry (Facultatif)	2-7
Installation du serveur Internet Microsoft IIS	2-9
Installation de SQL Server (facultatif)	2-10

Configuration des droits d'accès du compte Active Directory (facultatif)	2-11
Application des règles d'accès au réseau pour Mobile Security	2-11
Installation des outils d'administration de Microsoft Exchange Server (facultatif)	2-12
Installation de l'outil BES d'administration des utilisateurs (facultatif)	2-13

Chapitre 3: Installation et suppression des composants du serveur

Installation des composants du serveur	3-3
Avant l'installation	3-3
Procédure d'installation de Trend Micro Mobile Security	3-3
Installation du serveur d'administration	3-4
Installation du Serveur de communication local	3-14
Expéditeur de SMS	3-17
Configuration de l'intégration d'Exchange Server	3-18
Mise à niveau de Mobile Security	3-24
Suppression de composants du serveur	3-25

Chapitre 4: Configuration des composants du serveur

Configuration initiale du serveur	4-3
Configuration des paramètres de base de données	4-5
Configuration des paramètres du serveur de communication	4-6
Configuration des paramètres d'inscription des dispositifs.	4-14
Personnalisation des Conditions d'utilisation de Mobile Security	4-16
Configuration des paramètres Active Directory (AD)	4-17
Configuration des paramètres de serveur d'administration	4-18
Configuration de l'intégration d'Exchange Server	4-19
Configuration des paramètres de notifications/rapports	4-20
Configuration des notifications administrateur	4-21
Vérification de la configuration de Mobile Security	4-22

Chapitre 5: Gestion de l'Agent de dispositif mobile

Plates-formes et dispositifs mobiles pris en charge	5-3
Stockage et mémoire du dispositif	5-3
Configuration Agent de dispositif mobile	5-4
Configuration du serveur pour l'envoi de messages d'invitation (Facultatif)	5-5
Installation du MDA sur les dispositifs mobiles	5-10
Inscription du MDA sur le serveur Mobile Security	5-13

Annexe A: Configurations des ports de réseau

Configuration des ports de réseau pour le modèle de sécurité renforcée avec le serveur de communication du nuage	A-2
Configuration des ports de réseau pour le modèle de sécurité renforcée avec serveur de communication local	A-5
Configuration des ports de réseau pour le modèle de sécurité de base	A-10

Annexe B: Configurations facultatives

Utilisation de l'authentification Windows pour SQL Server	B-2
Configuration des ports du serveur de communication	B-5
Augmentation de l'extensibilité du serveur	B-6
Configuration de SCEP	B-7

Annexe C: Génération et configuration d'un certificat APNs (Apple Push Notification service)

Introduction au certificat APNs	C-3
Génération d'un certificat APNs (Apple Push Notification service)	C-3
Génération d'un certificat APNs (Apple Push Notification service) à partir d'un Windows Server	C-5
Génération d'un certificat APNs (Apple Push Notification service) à partir d'un poste de travail Mac	C-20
Téléchargement du certificat APNs (Apple Push Notification service) vers le serveur Mobile Security	C-26

Génération et configuration d'un certificat APNs dans Windows Server 2003 à l'aide d'IIS 6.0	C-28
Renouvellement d'un certificat APNs	C-29

Index

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

Préface

Préface

Bienvenue dans le *Manuel d'installation et de déploiement* de Trend Micro™ Mobile Security for Enterprise 9.0 SP2. Ce manuel aide les administrateurs à déployer et à gérer Trend Micro™ Mobile Security for Enterprise 9.0 SP2. Il décrit les différents composants de Mobile Security et les diverses méthodes de déploiement d'agents de dispositif mobile.

Pour obtenir les informations les plus récentes sur Mobile Security, en particulier la prise en charge des dispositifs mobiles et les dernières compilations, visitez la page <http://www.trendmicro.fr/produits/mobile-security/index.html>.



Remarque

Ce *Manuel d'installation et de déploiement* s'applique uniquement à Mobile Security version 9.0 SP2. Il ne s'applique pas à d'autres versions de Mobile Security. L'assistance de Trend Micro se limite à l'utilisation de Mobile Security. Pour recevoir de l'assistance sur les applications tierces mentionnées dans ce manuel, contactez les fournisseurs correspondants.

Cette préface aborde les sujets suivants :

- *Public ciblé à la page vi*
- *Documentation de Mobile Security à la page vi*
- *Conventions typographiques du document à la page vii*

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
<i>Italique</i>	Références à des documents annexes
Monospace	Exemples de lignes de commande, de code de programme, adresses Internet, noms de fichier et sortie de programme
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

Préparation de l'installation du serveur

Ce chapitre aide les administrateurs à planifier les composants du serveur pour Trend Micro™ Mobile Security for Enterprise 9.0 SP2.

Ce chapitre contient les sections suivantes :

- *Architecture du système Mobile Security à la page 1-2*
- *Modèle de sécurité renforcée (installation de deux serveurs) avec le serveur de communication du nuage à la page 1-3*
- *Modèle de sécurité renforcée (installation de deux serveurs) avec Serveur de communication local à la page 1-4*
- *Modèle de sécurité de base (installation sur un serveur) à la page 1-4*
- *Composants du système Mobile Security à la page 1-5*
- *Configuration minimale requise à la page 1-9*

Architecture du système Mobile Security

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

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

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

Modèle de sécurité renforcée (installation de deux serveurs) avec le serveur de communication du nuage

Le modèle de sécurité renforcée prend en charge le déploiement du serveur de communication du nuage. La figure suivante indique l'emplacement de chaque composant de Mobile Security dans un modèle de sécurité renforcée.

TMMS 9.0 – Modèle de sécurité recommandé (serveur de communication du nuage)

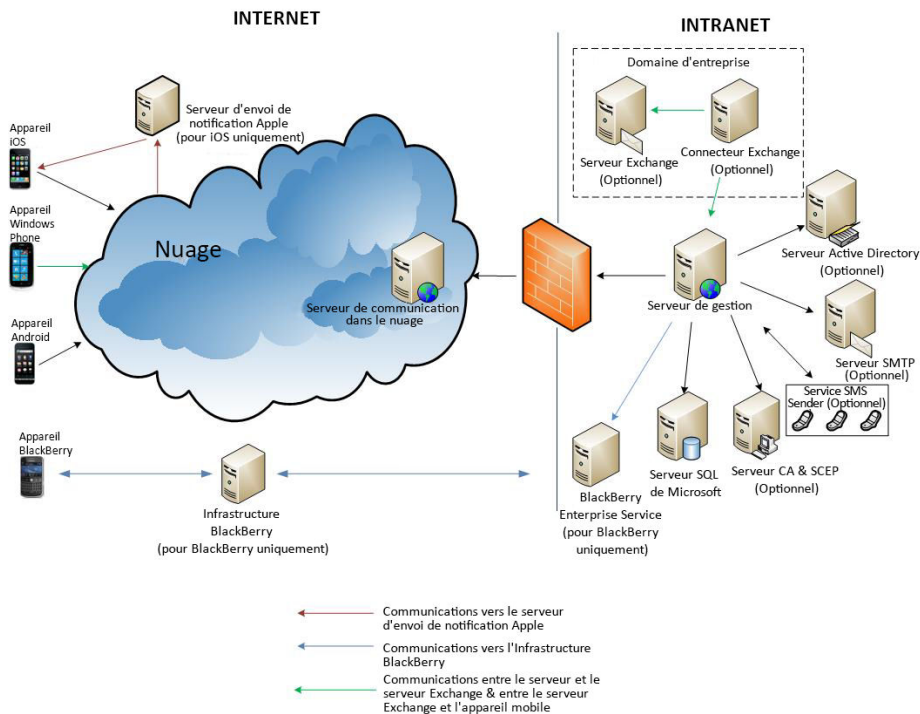


FIGURE 1-1. Modèle de sécurité renforcée avec le serveur de communication du nuage

Modèle de sécurité renforcée (installation de deux serveurs) avec Serveur de communication local

Le modèle de sécurité renforcée prend en charge l'installation du serveur de communication et du serveur d'administration sur le même ordinateur. La figure suivante indique l'emplacement de chaque composant de Mobile Security dans un modèle de sécurité renforcée.

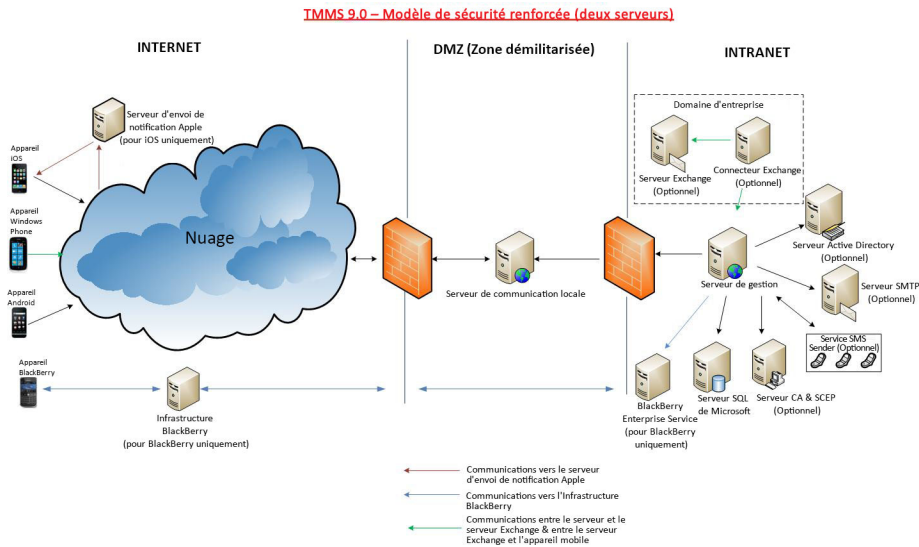


FIGURE 1-2. Modèle de sécurité renforcée avec Serveur de communication local

Modèle de sécurité de base (installation sur un serveur)

Le modèle de sécurité de base prend en charge l'installation du serveur de communication et du serveur d'administration sur le même ordinateur. La figure

suivante indique l'emplacement de chaque composant de Mobile Security dans un modèle de sécurité de base.

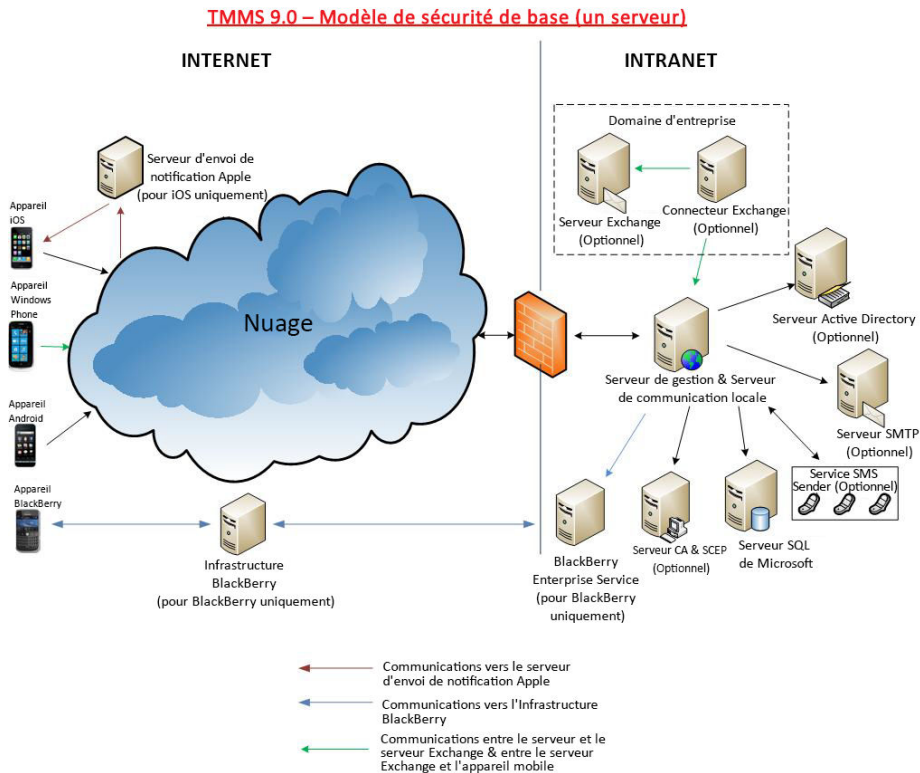


FIGURE 1-3. Modèle de sécurité de base

Composants du système Mobile Security

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

TABLEAU 1-1. Composants du système Mobile Security

COMPOSANT	DESCRIPTION	REQUIS OU FACULTATIF
Serveur d'administration	Le serveur d'administration vous permet de gérer les agents de dispositif mobile à partir de la console Web d'administration. Une fois les dispositifs mobiles inscrits sur le serveur, vous pouvez configurer les stratégies des agents de dispositif mobile et effectuer des mises à jour.	Requis
Serveur de communication	<p>Le serveur de communication gère les communications entre le serveur d'administration et les agents de dispositif mobile.</p> <p>Trend Micro Mobile Security fournit deux types de serveurs de communication :</p> <ul style="list-style-type: none"> • Serveur de communication local (LCS)—il s'agit d'un serveur de communication déployé localement sur votre réseau. • Serveur de communication du nuage CCS), —il s'agit d'un serveur de communication déployé sur le nuage et vous n'aurez pas besoin d'installer ce serveur. Trend Micro gère le serveur de communication du nuage et il vous suffit de vous-y connecter à partir du serveur d'administration. <p>Voir la section Comparaison entre le serveur de communication local et le serveur du nuage à la page 1-8.</p>	Requis
Expéditeur de SMS	Vous pouvez utiliser l'expéditeur de SMS pour envoyer des messages SMS aux utilisateurs.	Facultatif
Connecteur Exchange	Trend Micro Mobile Security utilise le connecteur Exchange pour communiquer avec Microsoft Exchange Server, et détecte les dispositifs qui utilisent le service Exchange ActiveSync.	Facultatif

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

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

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

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

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




FONCTIONS	SERVEUR DE COMMUNICATION DU NUAGE	SERVEUR DE COMMUNICATION LOCAL
Installation requise	Non	Oui
Méthode d'authentification utilisateur prise en charge	Clé d'inscription	Active Directory ou clé d'inscription
Personnalisation d'agent pour Android	Non pris en charge	Pris en charge
Gestion de Windows Phone	Non pris en charge	Pris en charge

Configuration minimale requise

Consultez les configurations minimales requises suivantes avant d'installer chaque composant Mobile Security sur votre réseau.

TABLEAU 1-3. Configuration minimale requise

COMPOSANT	CONFIGURATION
Serveur d'administration et serveur de communication	<p>Plate-formes recommandées</p> <ul style="list-style-type: none"> • Windows Server 2008 R2 Enterprise Edition • Windows Server 2008 Enterprise Edition SP1 • Windows Server 2003 R2 Enterprise Edition • Windows Server 2003 Enterprise Edition • Windows Server 2008 Standard Edition • Windows Web Server 2008 Edition SP1 <p>Autres plate-formes</p> <ul style="list-style-type: none"> • Famille des systèmes d'exploitation Windows 2003 Server • Famille des systèmes d'exploitation Windows 2003 R2 Server • Famille des systèmes d'exploitation Windows 2008 Server • Famille des systèmes d'exploitation Windows 2008 R2 Server • Famille des systèmes d'exploitation Windows 2012 Server • Famille des systèmes d'exploitation Windows Server 2012 R2
	<p>Matériel</p> <ul style="list-style-type: none"> • Processeur 1 GHz Intel™ Pentium™ ou équivalent • Au minimum 1 Go de RAM • Au moins 400 Mo d'espace disque disponible • Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum

COMPOSANT	CONFIGURATION
Serveur Internet IIS pour le serveur d'administration	<p>Microsoft Internet Information Server (IIS) 6.0/7.0/7.5/8.0</p> <hr/> <p> Remarque</p> <ul style="list-style-type: none"> • IIS fait intégralement partie de Microsoft Windows et les numéros de version IIS correspondent à la version Windows installée. • Conserver les paramètres par défaut et sélectionner <p>Lorsque vous utilisez IIS 7.0 ou une version supérieure pour le serveur d'administration, conservez les paramètres par défaut et activez et installez CGI et les extensions ISAPI dans le développement d'applications, Redirection HTTP dans les fonctions courantes HTTP, et la compatibilité de gestion IIS6 dans les outils de gestion.</p> <hr/> <p> Remarque</p> <p>Trend Micro Mobile Security ne prend PAS en charge le serveur Internet Apache.</p>
Expéditeur de SMS	Android 2.1 ou version supérieure
Microsoft Exchange Server	<ul style="list-style-type: none"> • Microsoft Exchange Server 2007 • Microsoft Exchange Server 2010 • Microsoft Exchange Server 2013
Navigateur Web	<ul style="list-style-type: none"> • Internet Explorer 8.0 ou version supérieure • Chrome 17 ou version supérieure • Firefox 14 ou version supérieure • Safari 6 ou version supérieure sur Mac <hr/> <p> Remarque</p> <p>Adobe Flash Player est nécessaire pour la console Web d'administration de Mobile Security.</p>

COMPOSANT	CONFIGURATION
SQL Server	<ul style="list-style-type: none">• Microsoft SQL Server 2005• Microsoft SQL Server 2005 Express Edition• Microsoft SQL Server 2008• Microsoft SQL Server 2008 Express Edition• Microsoft SQL Server 2008 R2• Microsoft SQL Server 2008 R2 Express Edition• Microsoft SQL Server 2012• Microsoft SQL Server 2012 Express Edition
Connecteur Exchange de Mobile Security	<p>Plate-forme</p> <ul style="list-style-type: none">• Windows Server 2008 R2 (64-bit)• Windows Server 2012 (64 bits)• Windows Server 2012 R2 (64 bits) <p>Matériel</p> <ul style="list-style-type: none">• Processeur 1 GHz Intel™ Pentium™ ou équivalent• Au minimum 1 Go de RAM• Au moins 200 Mo d'espace disque disponible <p>Autre</p> <ul style="list-style-type: none">• Microsoft .Net Framework 3.5

Chapitre 2

Configuration de l'environnement

Ce chapitre fournit les informations dont vous aurez besoin pour configurer votre environnement avant d'installer Trend Micro™ Mobile Security for Enterprise 9.0 SP2.

Ce chapitre contient les sections suivantes :

- *Configuration de l'environnement pour l'installation de Mobile Security à la page 2-2*
- *Configuration de l'environnement pour les dispositifs mobiles iOS (Facultatif) à la page 2-4*
- *Configuration de l'environnement pour les dispositifs mobiles BlackBerry (Facultatif) à la page 2-7*
- *Installation du serveur Internet Microsoft IIS à la page 2-9*
- *Installation de SQL Server (facultatif) à la page 2-10*
- *Configuration des droits d'accès du compte Active Directory (facultatif) à la page 2-11*
- *Application des règles d'accès au réseau pour Mobile Security à la page 2-11*
- *Installation des outils d'administration de Microsoft Exchange Server (facultatif) à la page 2-12*
- *Installation de l'outil BES d'administration des utilisateurs (facultatif) à la page 2-13*

Configuration de l'environnement pour l'installation de Mobile Security

Le tableau suivant décrit la procédure d'installation de l'environnement pour l'installation de Mobile Security.

TABLEAU 2-1. Procédure de configuration de l'environnement pour l'installation de Mobile Security

ÉTAPE	ACTION	DESCRIPTION
Étape 1	Installer le serveur Internet Microsoft IIS sur l'ordinateur où vous envisagez d'installer le serveur d'administration.	Voir Installation du serveur Internet Microsoft IIS à la page 2-9 pour plus de détails.
Étape 2	(Facultatif) Installer la base de données.	Si vous sauter cette étape maintenant, Mobile Security installera automatiquement Microsoft SQL Server 2005 Express Edition lors de l'installation. Voir Installation de SQL Server (facultatif) à la page 2-10 pour plus de détails.
Étape 3	(Facultatif) Configurer les droits d'accès au compte Active Directory.	Effectuez cette étape si vous souhaitez importer des utilisateurs depuis le serveur d'entreprise Active Directory. Voir Configuration des droits d'accès du compte Active Directory (facultatif) à la page 2-11 pour plus de détails.

ÉTAPE	ACTION	DESCRIPTION
Étape 4	(Facultatif) Installer les outils du serveur d'administration Microsoft Exchange Server.	Cela permet d'intégrer Exchange Server avec le serveur Mobile Security pour gérer les dispositifs mobiles Windows Phone, Android, iOS. Voir Installation des outils d'administration de Microsoft Exchange Server (facultatif) à la page 2-12 pour plus de détails.
Étape 5	Appliquer les règles d'accès au réseau.	Voir Application des règles d'accès au réseau pour Mobile Security à la page 2-11 pour plus de détails. Voir Configurations des ports de réseau à la page A-1 pour la configuration de ports réseau complète.
Étape 6	(Facultatif) Configurer l'environnement pour gérer les dispositifs mobiles iOS.	Si vous souhaitez gérer les dispositifs mobiles iOS, cette étape est obligatoire. Voir la section Configuration de l'environnement pour les dispositifs mobiles iOS (Facultatif) à la page 2-4.
Étape 7	(Facultatif) Configurer l'environnement pour gérer les dispositifs mobiles BlackBerry.	Si vous souhaitez gérer les dispositifs mobiles BlackBerry, cette étape est obligatoire. Voir la section Configuration de l'environnement pour les dispositifs mobiles BlackBerry (Facultatif) à la page 2-7.

Configuration de l'environnement pour les dispositifs mobiles iOS (Facultatif)



AVERTISSEMENT!


Avant de configurer l'environnement pour gérer les dispositifs mobiles iOS, assurez-vous que vous avez effectué toutes les étapes mentionnées dans le tableau suivant.

Le tableau suivant décrit la procédure de configuration de l'environnement pour gérer les dispositifs mobiles iOS.

TABLEAU 2-2. Procédure de configuration de l'environnement pour les dispositifs mobiles iOS

ÉTAPE	ACTION	DESCRIPTION
Étape 1	Configurer le certificat de notifications Push Apple (APNs).	Pour gérer des dispositifs mobiles iOS4 ou version ultérieure, vous devez configurer le certificat APNs (Apple Push Notification service). Voir la section Génération et configuration d'un certificat APNs (Apple Push Notification service) à la page C-1 pour la procédure complète.

ÉTAPE	ACTION	DESCRIPTION
Étape 2	(Facultatif) Obtenir un certificat de serveur SSL d'une autorité de certification publique reconnue.	<p>Le certificat SSL fournit une communication sécurisée entre les dispositifs mobiles et le serveur de communication.</p> <p>Si vous voulez gérer des dispositifs mobiles Windows Phone ou iOS 5.x ou version ultérieure, ou si vous prévoyez d'utiliser le serveur de communication local, alors cette étape est obligatoire. Vous devrez importer un certificat SSL public lors de l'installation du serveur de communication local.</p> <p>Vous pouvez sauter cette étape :</p> <ul style="list-style-type: none">• Si vous souhaitez utiliser un certificat SSL privé. Mobile Security le créera pendant l'installation du serveur de communication local.• Si vous envisagez d'utiliser le serveur de communication du nuage.

ÉTAPE	ACTION	DESCRIPTION
Étape 3	(Facultatif) Configurer l'Extension du protocole d'inscription du certificat simple (SCEP) pour plus de sécurité	<p>Il permet une communication sécurisée entre les dispositifs mobiles et le serveur de communication.</p> <p>Voir Configuration de SCEP à la page B-7 pour plus de détails.</p> <p>Si SCEP est déjà configurée dans votre environnement, vous pouvez sauter cette étape.</p> <hr/> <p> Remarque</p> <p>Si vous ne souhaitez pas utiliser SCEP pour les dispositifs mobiles iOS, vous devrez le désactiver dans Paramètres du serveur de stratégie après avoir installé le serveur d'administration et le serveur de communication. Consultez la section Configuration des paramètres du serveur de communication iOS à la page 4-10 pour la procédure.</p>

ÉTAPE	ACTION	DESCRIPTION
Étape 4	Configurer les ports réseau 2195 (TCP) sur le serveur de communication local et 5223 sur le réseau Wi-Fi	<p>Le port TCP 2195 permet une connexion sortante du serveur de communication vers le service de notifications Push Apple au port TCP 2195. Le nom d'hôte du service de notifications Push Apple est gateway.push.apple.com.</p> <p>Le port 5223 permet de recevoir une notification push du serveur Apple pour les dispositifs iOS, en particulier lors d'une connexion par le biais d'un réseau Wi-Fi où le port 5223 est bloqué. Cependant, si les dispositifs mobiles se trouvent sur un réseau 3G, il n'est pas nécessaire de configurer ce port.</p> <p>Voir Configurations des ports de réseau à la page A-1 pour la configuration de ports réseau complète.</p>

Configuration de l'environnement pour les dispositifs mobiles BlackBerry (Facultatif)




AVERTISSEMENT!

Avant de configurer l'environnement pour gérer les dispositifs mobiles BlackBerry, assurez-vous que vous avez effectué toutes les étapes mentionnées dans le tableau suivant.

Le tableau suivant décrit la procédure de configuration de l'environnement pour gérer les dispositifs mobiles BlackBerry.

TABLEAU 2-3. Procédure de configuration de l'environnement pour les dispositifs mobiles BlackBerry

ÉTAPE	ACTION	DESCRIPTION
Étape 1	Installer le serveur BlackBerry Enterprise BlackBerry (BES).	<p>Consulter les URL suivantes pour de plus amples renseignements concernant BlackBerry Enterprise Server (BES) 5.x :</p> <p>http://us.blackberry.com/apps-software/server/5/</p> <p>et</p> <p>http://docs.blackberry.com</p> <hr/> <p> Remarque</p> <p>Trend Micro Mobile Security prend uniquement en charge la version 5.x de BlackBerry Enterprise Server (BES).</p>
Étape 2	Activer le dispositif mobile BlackBerry	<p>Vous devez activer les dispositifs mobiles BlackBerry pour pouvoir les gérer depuis Mobile Security.</p> <p>Consultez l'URL suivante pour plus de détails :</p> <p>http://docs.blackberry.com</p>
Étape 3	Installer l'outil d'administration des utilisateurs BES sur le serveur d'administration	<p>Permet à Mobile Security de gérer les dispositifs mobiles BlackBerry.</p> <p>Voir <i>Installation de l'outil BES d'administration des utilisateurs (facultatif)</i> à la page 2-13 pour plus de détails.</p>

Installation du serveur Internet Microsoft IIS

Cette tâche est une étape de la procédure de configuration de l'environnement pour l'installation de Mobile Security.

Voir la section *Configuration de l'environnement pour l'installation de Mobile Security à la page 2-2.*

Procédure

- Accédez à l'une des URL suivantes pour la procédure d'installation du serveur Internet Microsoft IIS :
 - Pour Windows 2003 (IIS 6.0) :
<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/750d3137-462c-491d-b6c7-5f370d7f26cd.msp?mfr=true>
 - Pour Windows 2008 ou Windows Server 2008 R2 (IIS 7.0 ou 7.5)
<http://www.iis.net/learn/install/installing-iis-7>
 - Pour Windows 2012 (IIS 8.0)
<http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012>



Remarque

Lorsque vous utilisez la version IIS 7.0 ou une version supérieure pour le serveur d'administration, conservez les paramètres par défaut, activez et installez **les extensions CGI et ISAPI** dans Développement d'application, **Redirection d'URL** dans Fonctions courantes **compatibilité de gestion IIS6** dans les outils de gestion.

Installation de SQL Server (facultatif)



Remarque

Vous pouvez sauter cette étape si vous ne voulez pas installer de version spécifique de SQL Server. Mobile Security installera automatiquement Microsoft SQL Server 2005 Express Edition lors de l'installation.

Cette tâche est une étape de la procédure de configuration de l'environnement pour l'installation de Mobile Security.

Voir la section *Configuration de l'environnement pour l'installation de Mobile Security à la page 2-2*.

Procédure

- Accédez à l'une des URL suivantes pour la procédure d'installation des outils de gestion de SQL Server :
 - Pour Microsoft SQL Server 2005 (ou Express edition) :
[http://msdn.microsoft.com/en-us/library/ms143516\(v=SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/ms143516(v=SQL.90).aspx)
 - Pour Microsoft SQL Server 2008/2008 R2 (ou Express edition) :
[http://msdn.microsoft.com/en-us/library/ms143219\(v=SQL.100\).aspx](http://msdn.microsoft.com/en-us/library/ms143219(v=SQL.100).aspx)
 - Pour Microsoft SQL Server 2012 (ou Express edition) :
[http://msdn.microsoft.com/en-us/library/bb500395\(v=SQL.110\).aspx](http://msdn.microsoft.com/en-us/library/bb500395(v=SQL.110).aspx)
-



Remarque

Trend Micro recommande l'utilisation de la méthode d'authentification SQL Server au lieu de l'authentification Windows. Cependant, vous pouvez également configurer l'authentification Windows pour SQL Server. Consultez *Utilisation de l'authentification Windows pour SQL Server à la page B-2* pour plus de renseignements.

Configuration des droits d'accès du compte Active Directory (facultatif)



Remarque

Vous ne devez exécuter cette étape que si vous avez l'intention d'utiliser Active Directory pour l'authentification utilisateur ou pour importer des utilisateurs depuis Active Directory. Sinon, ignorez cette étape.

Si vous n'avez pas déjà installé Active Directory, reportez-vous à l'URL suivante pour la procédure d'installation détaillée :

[http://technet.microsoft.com/en-us/library/cc757211\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc757211(WS.10).aspx)

Cette tâche est une étape de la procédure de configuration de l'environnement pour l'installation de Mobile Security.

Voir la section *Configuration de l'environnement pour l'installation de Mobile Security à la page 2-2*.

Procédure

- Créez le compte de service Active Directory pour Mobile Security 9.0 SP2 et attribuez-lui au moins l'accès en lecture seule à Active Directory. Reportez-vous à l'URL suivante pour créer un compte Active Directory pour Windows 2008 :

[http://technet.microsoft.com/en-us/library/dd894463\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd894463(WS.10).aspx)

Application des règles d'accès au réseau pour Mobile Security

Cette tâche est une étape de la procédure de configuration de l'environnement pour l'installation de Mobile Security.

Voir la section *Configuration de l'environnement pour l'installation de Mobile Security à la page 2-2*.

Procédure

- Appliquez les règles d'accès au réseau suivantes :
 - Si vous prévoyez d'utiliser Active Directory, le serveur d'administration devrait être en mesure de se connecter au serveur Active Directory. Si vous utilisez un pare-feu, assurez-vous d'ajouter une exception dans les paramètres du pare-feu pour le serveur d'administration.
 - Le serveur d'administration doit pouvoir se connecter au serveur SQL, là où est installée la base de données Trend Micro Mobile Security. Si vous utilisez un pare-feu, assurez-vous d'ajouter une exception dans les paramètres du pare-feu sur les deux serveurs, serveur d'administration et SQL Server.
 - Ajoutez une exception au port 4343 pour assurer une connexion https entre le serveur d'administration et le serveur de communication :

Si vous avez besoin de personnaliser ce numéro de port, consultez la section [Configuration des ports du serveur de communication à la page B-5](#) pour plus de renseignements.

- Ajoutez une exception aux ports numéros 80 et 443 afin de vous assurer que tous les dispositifs mobiles sont en mesure de se connecter au serveur de communication.
-

Installation des outils d'administration de Microsoft Exchange Server (facultatif)

Les outils d'administration de Microsoft Exchange Server permettent l'intégration de serveur Exchange avec le serveur Mobile Security afin de gérer les dispositifs mobiles Windows Phone, Android et iOS.

Cette tâche est une étape de la procédure de configuration de l'environnement pour l'installation de Mobile Security.

Voir la section [Configuration de l'environnement pour l'installation de Mobile Security à la page 2-2](#).

Procédure

- Accédez à l'une des URL suivantes pour obtenir la procédure d'installation des outils d'administration d'Exchange Server :
 - Pour l'installation des outils d'administration d'Exchange Server 2007 :
[http://technet.microsoft.com/fr-fr/library/bb232090\(v=EXCHG.80\).aspx](http://technet.microsoft.com/fr-fr/library/bb232090(v=EXCHG.80).aspx)
 - Pour l'installation des outils d'administration d'Exchange Server 2010 :
[http://technet.microsoft.com/library/bb232090\(v=EXCHG.141\)](http://technet.microsoft.com/library/bb232090(v=EXCHG.141))
 - Pour l'installation des outils d'administration d'Exchange Server 2013 :
[http://technet.microsoft.com/fr-fr/library/bb232090\(v=exchg.150\).aspx](http://technet.microsoft.com/fr-fr/library/bb232090(v=exchg.150).aspx)
-

Installation de l'outil BES d'administration des utilisateurs (facultatif)

Pour gérer les terminaux BlackBerry, vous devez installer Outil BES d'administration des utilisateurs sur le serveur d'administration.



AVERTISSEMENT!

Avant d'installer l'outil BES d'administration des utilisateurs, assurez-vous que vous avez déjà installé BlackBerry Enterprise Server et que vous avez activé les dispositifs mobiles BlackBerry.

Cette tâche est une étape de la procédure de configuration de l'environnement pour l'installation de Mobile Security.

Voir la section *Configuration de l'environnement pour les dispositifs mobiles BlackBerry (Facultatif)* à la page 2-7.

Procédure

1. Accédez à l'URL suivante :

<http://us.blackberry.com/support/downloads/>

2. Dans la liste de **Logiciels commerciaux**, cliquez sur **Kit de ressources de BlackBerry Enterprise Server**, puis lisez les instructions sur la page Web pour télécharger l'**BlackBerry Enterprise Server User Administration Tool v5.0 Service Pack 2** à partir du **Kit de ressources de BlackBerry Enterprise Server v5.0 Service Pack 2**.
3. Consultez l'URL suivante pour une procédure détaillée d'installation :

<http://docs.blackberry.com/en/admin/deliverables/46354/1075538.jsp>

Chapitre 3

Installation et suppression des composants du serveur

Ce chapitre guide les administrateurs dans l'installation des composants du serveur Trend Micro™ Mobile Security for Entreprise9.0 SP2. Ce chapitre les guide également dans la suppression des composants du serveur.

Ce chapitre contient les sections suivantes :

- *Installation des composants du serveur à la page 3-3*
- *Avant l'installation à la page 3-3*
- *Procédure d'installation de Trend Micro Mobile Security à la page 3-3*
- *Installation du serveur d'administration à la page 3-4*
- *Accès à la console Web d'administration à la page 3-10*
- *Enregistrement du produit à la page 3-12*
- *Installation du Serveur de communication local à la page 3-14*
- *Expéditeur de SMS à la page 3-17*
- *Installation de l'expéditeur de SMS à la page 3-18*
- *Configuration de l'intégration d'Exchange Server à la page 3-18*

- *Configuration d'un compte pour Exchange Connector à la page 3-19*
- *Installation du connecteur Exchange à la page 3-22*
- *Mise à niveau de Mobile Security à la page 3-24*
- *Suppression de composants du serveur à la page 3-25*

Installation des composants du serveur

Avant l'installation

Avant de commencer l'installation des composants du serveur Mobile Security :

- assurez-vous que les composants de Mobile Security sont conformes aux exigences spécifiques du système.

Voir la section *Configuration minimale requise à la page 1-9*. Il vous faudra peut-être aussi évaluer la topologie de votre réseau et choisir les composants du serveur Mobile Security que vous souhaitez installer.

- assurez-vous que vous avez déjà effectué toutes les démarches préalables mentionnées dans le chapitre *Configuration de l'environnement à la page 2-1*.

Procédure d'installation de Trend Micro Mobile Security

Le tableau ci-dessous illustre l'approche de base pour l'installation de Trend Micro Mobile Security.

TABLEAU 3-1. Procédure d'installation de Trend Micro Mobile Security

ÉTAPE	ACTION	DESCRIPTION
Étape 1	Installation du serveur d'administration Mobile Security	Voir la section <i>Installation du serveur d'administration à la page 3-4</i> pour la procédure complète.
Étape 2	Connectez-vous à la console Web d'administration de Mobile Security for Enterprise	Voir la section <i>Accès à la console Web d'administration à la page 3-10</i> pour la procédure complète.
Étape 3	Enregistrez le produit	Voir la section <i>Enregistrement du produit à la page 3-12</i> pour la procédure complète.

ÉTAPE	ACTION	DESCRIPTION
Étape 4	(Facultatif) Téléchargez et installez le Serveur de communication local	Vous pouvez sauter cette étape si vous prévoyez d'utiliser le serveur de communication de nuage (CCS). Voir la section Installation du Serveur de communication local à la page 3-14 pour la procédure complète.
Étape 5	(Facultatif) Installez l'expéditeur de SMS	Vous pouvez sauter cette étape si vous ne voulez pas envoyer de notifications SMS aux utilisateurs. Voir la section Installation de l'expéditeur de SMS à la page 3-18 pour la procédure complète.
Étape 6	(Facultatif) Installez le connecteur Exchange	Vous pouvez sauter cette étape si vous ne voulez pas gérer de dispositifs mobiles qui utilisent Exchange ActiveSync. Voir la section Installation du connecteur Exchange à la page 3-22 pour la procédure complète.

Installation du serveur d'administration



Remarque

Mobile Security nécessite le téléchargement du fichier .apk par l'Environnement d'exécution Java (Java Runtime Environment, JRE) depuis le module de gestion d'applications sur le serveur d'administration. Le JRE est installé automatiquement avec l'installation du serveur d'administration. Cependant, si JRE est déjà installé sur l'ordinateur sur lequel vous avez installé le serveur d'administration, l'installation du serveur d'administration n'inclura pas l'installation de JRE. Si la version existante de JRE est inférieure à 1.6, vous devrez désinstaller JRE manuellement, et installer la version 1.6 ou supérieure.

Procédure

1. Téléchargez le programme d'installation du serveur d'administration à partir de l'emplacement suivant :
http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4415&lang_loc=1
2. Extrayez le fichier téléchargé, puis exécutez le programme d'installation du serveur d'administration : MdmServerSetup.exe.
L'écran de **Bienvenue** s'affiche.
3. Cliquez sur **Suivant**.
L'écran **Contrat de licence** s'affiche.
4. Sélectionnez la case **J'accepte** et cliquez sur **Suivant**.

**Remarque**

Mobile Security vous demande d'installer les fichiers redistribuables PHP et Microsoft Visual C++ 2005. Si vous avez déjà installé sur votre ordinateur les fichiers redistribuables PHP et Microsoft Visual C++ 2005, les étapes de l'installation n'apparaîtront pas lors de l'installation. Si l'écran d'installation des fichiers redistribuables PHP Microsoft Visual C++ 2005 s'affiche, cliquez sur **Suivant** sur les écrans pour continuer l'installation.

L'écran **Options de la base de données** s'affiche.

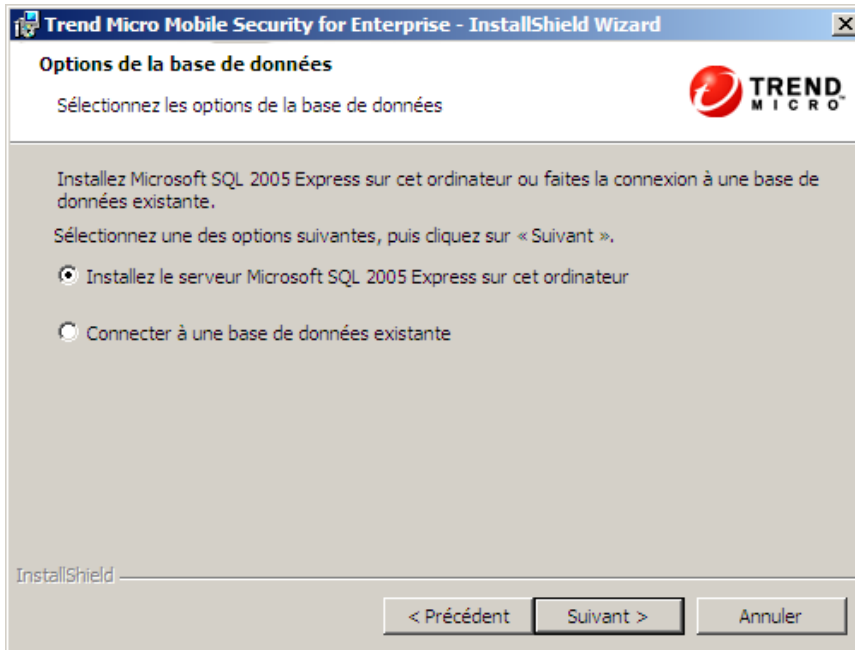


FIGURE 3-1. L'écran Options de la base de données

5. Effectuez l'une des actions suivantes :
 - Si vous n'avez pas de base de données installée ou si vous voulez créer une nouvelle base de données pour Mobile Security :
 - a. Sélectionnez **Installer Microsoft SQL Server 2005 Express sur cet ordinateur**, et cliquez sur **Suivant**.

L'écran **Configuration de la base de données** s'affiche.

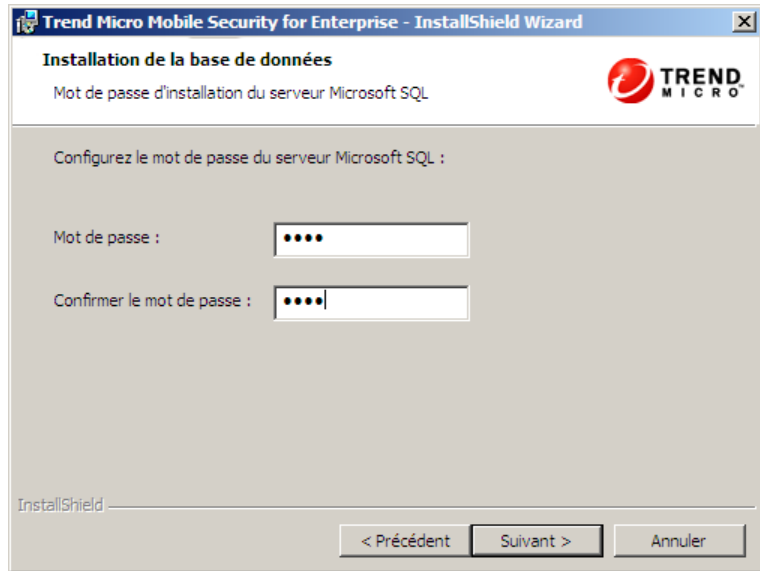


FIGURE 3-2. Écran de configuration de la base de données pour la nouvelle base de données

- b. Saisissez un mot de passe pour votre nouvelle base de données et cliquez sur **Suivant**.

L'écran **Progression de l'installation** apparaît et affiche l'état de l'installation en cours.

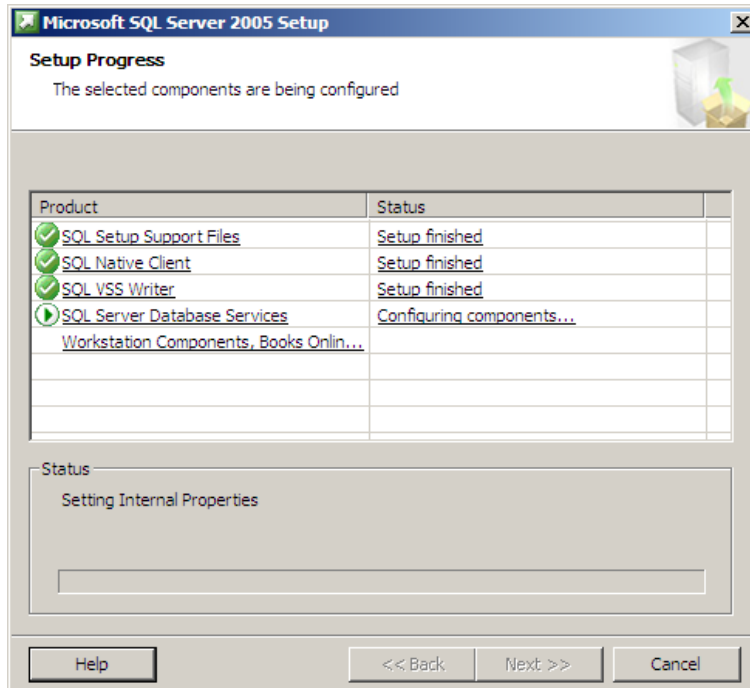


FIGURE 3-3. Écran de progression de l'installation

- c. Une fois la configuration terminée, cliquez sur **Suivant**.

L'écran **Paramètres de connexion du serveur** s'affiche.

- Si vous avez déjà une base de données installée et que vous souhaitez utiliser la base de données existante :
 - a. Sélectionnez **Se connecter à une base de données existante** et cliquez sur **Suivant**.

L'écran **Base de données existante** s'affiche.

FIGURE 3-4. Informations relatives au serveur de base de données existant

- b. Saisissez les informations du serveur de votre base de données existante, puis cliquez sur **Suivant**

L'écran **Paramètres de connexion du serveur** s'affiche.

6. Sélectionnez l'adresse IP dans la liste déroulante et entrez le numéro de port du serveur et cliquez sur **Suivant**.
7. Choisissez un emplacement où vous souhaitez installer Mobile Security et cliquez sur **Suivant**.



Remarque

Cliquez sur **Changer** pour sélectionner un autre emplacement.

8. Cliquez sur **Installer** pour démarrer l'installation.

La fenêtre de progression de l'installation s'affiche. Une fois l'installation terminée, l'écran **Installation de Trend Micro Mobile Security terminée** s'affiche.

9. Cliquez sur **Terminer**.
-

Que faire ensuite

Voir *Procédure d'installation de Trend Micro Mobile Security à la page 3-3* pour la tâche de configuration suivante.

Accès à la console Web d'administration

Procédure

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

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



Remarque

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

L'écran suivant s'affiche.



FIGURE 3-5. Écran de connexion de la console Web d'administration

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



Remarque

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

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



Important

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

- l'option **Affichage de compatibilité des sites Web** est désactivée. Voir *Désactivation du mode de compatibilité sur Internet Explorer à la page 3-12* pour plus de détails.
- JavaScript est activé sur votre navigateur.



Remarque

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

Désactivation du mode de compatibilité sur Internet Explorer

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

Procédure

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

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

2. Si la console d'administration est ajoutée à la liste **Affichage de compatibilité**, sélectionnez le site Web et cliquez sur **Supprimer**.
 3. Effacer les cases à cocher **Afficher les sites intranet dans l'affichage de compatibilité** et **Afficher tous les sites Web dans l'affichage de compatibilité**, puis cliquez sur **Fermer**.
-

Enregistrement du produit

Pendant une période déterminée, Trend Micro propose à tous les utilisateurs enregistrés un service d'assistance technique, des téléchargements de fichiers de signatures de programmes malveillants et des mises à jour de programmes. Au terme de cette période, ils doivent acheter un renouvellement de maintenance pour continuer à bénéficier de ces services. Enregistrez votre serveur Mobile Security pour recevoir les dernières mises à jour de sécurité, et bénéficier d'autres services de produits et de maintenance.

Il vous suffit d'enregistrer le serveur Mobile Security sur le serveur d'administration à l'aide du code d'activation. Les agents de dispositif mobile obtiennent automatiquement

les informations de licence à partir du serveur Mobile Security après la connexion et l'enregistrement des dispositifs mobiles sur le serveur.

Le code d'activation s'affiche dans le format suivant :

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX

Procédure

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

Si c'est la première fois que vous accédez à la console d'administration, l'écran de la **licence du produit** s'affiche. Sinon, cliquez sur **Administration > Licence du produit**, puis cliquez sur **Nouveau code d'activation**.

2. Saisissez le code d'activation dans les champs proposés puis cliquez sur **Enregistrer**.

Licence du produit

Trend Micro™ Mobile Security for Enterprise v9.0 est une solution de sécurité globale pour vos dispositifs mobiles qui vous permet de gérer les agents de gestion du dispositif installés sur les dispositifs mobiles et de générer des rapports à partir d'une console Web.
Trend Micro offre à tous les utilisateurs enregistrés un service d'assistance technique, des téléchargements de signatures de programmes malveillants et des mises à jour de logiciels pendant une période déterminée, après laquelle vous devez payer le renouvellement pour continuer à bénéficier de ces services. Enregistrez le serveur Mobile Security pour vous assurer d'avoir droit à recevoir les dernières mises à jour de sécurité et d'autres produits et services de maintenance.
Pour obtenir le code d'activation, veuillez [enregistrer-vous en ligne](#) à l'aide de la clé d'enregistrement fournie avec votre produit.

Nouveau code d'activation

Service : Trend Micro Mobile Security

Nouveau code d'activation [] . [] . [] . [] . [] . [] . [] . []

Cliquez ici pour obtenir un code d'activation d'essai.

FIGURE 3-6. Enregistrement de Mobile Security après l'installation

3. Vérifiez que l'enregistrement du produit s'est effectué correctement. Cliquez sur **Tableau de bord** pour afficher l'écran du **Tableau de bord**.

Vous devriez voir le message « Trend Micro Mobile Security 9.0 a été activé. » si l'enregistrement du produit s'est effectué correctement.

Une fois l'enregistrement terminé, l'écran de **Mise en route** s'affiche, vous guide à travers les étapes nécessaires pour compléter les paramètres initiaux.

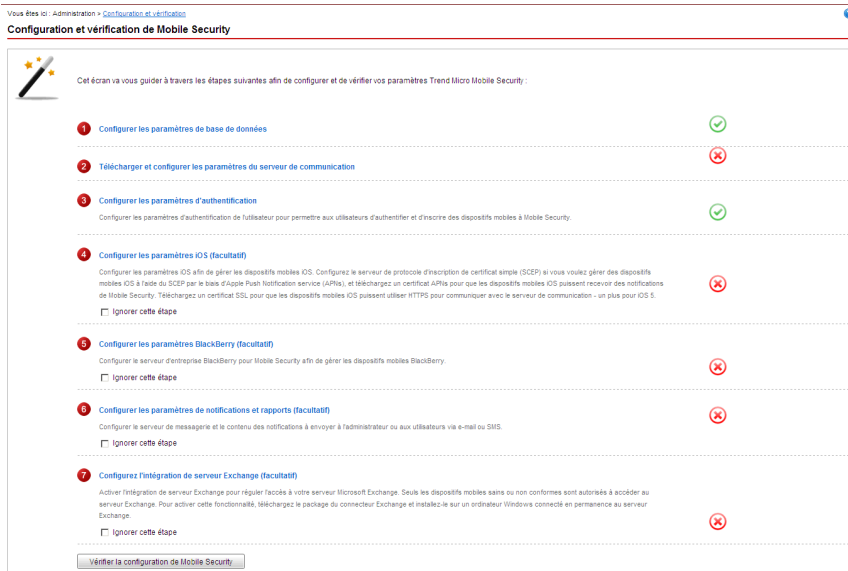


FIGURE 3-7. Écran de mise en route

Que faire ensuite

Voir *Procédure d'installation de Trend Micro Mobile Security à la page 3-3* pour la tâche de configuration suivante.

Installation du Serveur de communication local

Procédure

1. Connectez-vous à la console Web d'administration sur l'ordinateur sur lequel vous souhaitez installer le serveur de communication.
2. Cliquez sur **Administration > Paramètres serveur de communication**.

3. Cliquez sur l'onglet **Paramètres courants**.
4. Sélectionnez le **Serveur de communication local** à partir de la liste déroulante, puis cliquez sur le lien **Cliquer ici pour télécharger** pour télécharger le package d'installation sur l'ordinateur sur lequel vous souhaitez installer le serveur de communication.
5. Double-cliquez sur le fichier d'installation pour démarrer le processus.
L'écran de **Bienvenue** s'affiche.
6. Cliquez sur **Suivant**.
L'écran **Contrat de licence** s'affiche.
7. Cochez la case **J'accepte les termes du contrat de licence** et cliquez sur **Suivant**.
L'écran **Paramètres de connexion du serveur de communication pour dispositifs mobiles** apparaît.
8. Sélectionnez une adresse IP dans la liste déroulante, et saisissez les numéros de port HTTP et HTTPS pour le serveur de communication.
L'adresse IP et le numéro de port sur cet écran sont utilisés pour permettre au serveur de communication de communiquer avec les dispositifs mobiles.

**Remarque**

Trend Micro recommande de sélectionner «TOUTES» pour l'adresse IP.

9. Cliquez sur **Suivant**.
L'écran **Paramètres de connexion du serveur de communication pour le serveur d'administration** apparaît.
10. Sélectionnez une adresse IP dans la liste déroulante, et saisissez un numéro de port HTTPS pour le serveur de communication.
L'adresse IP et le numéro de port sur cet écran sont utilisés pour permettre au serveur de communication de communiquer avec le serveur d'administration.



Remarque

Trend Micro recommande de sélectionner «TOUTES» pour l'adresse IP.

11. Cliquez sur **Suivant**.

L'écran **Certificat du serveur** apparaît.

12. Effectuez l'une des actions suivantes :

- Si vous avez déjà un certificat SSL pour l'inscription de dispositif mobile iOS, procédez comme suit :

- a. Sélectionnez **Importer un fichier de certificat existant .pfx ou .p12** et cliquez sur **Suivant**.

L'écran **Importer certificat** s'affiche.

- b. Cliquez sur **Parcourir** et sélectionnez le certificat public à partir du disque dur.
- c. Entrez le mot de passe du certificat dans le champ **Mot de passe**. Laissez ce champ vide si le certificat n'a pas de mot de passe.
- d. Cliquez sur **Suivant**.

- Si vous ne disposez pas d'un certificat SSL pour l'inscription de dispositif mobile iOS, ou si vous avez besoin d'en créer un nouveau, procédez comme suit :

- a. Sélectionnez **Créer un nouveau certificat privé** et cliquez sur **Suivant**.

L'écran **Créer certificat** s'affiche.

- b. Tapez l'adresse IP du serveur de communication dans le champ **Nom courant** et un mot de passe de certificat dans le champ **Mot de passe**.
- c. Cliquez sur **Suivant**.

13. Choisissez un emplacement où vous souhaitez installer Mobile Security et cliquez sur **Suivant**.

**Remarque**

Cliquez sur **Changer** pour sélectionner un autre emplacement.

14. Cliquez sur **Installer** pour démarrer l'installation.

La fenêtre de progression de l'installation s'affiche. Une fois l'installation terminée, l'écran **Installation terminée** s'affiche.

15. Cliquez sur **Terminer**.
-

Que faire ensuite

Voir [Procédure d'installation de Trend Micro Mobile Security à la page 3-3](#) pour la tâche de configuration suivante.

Expéditeur de SMS

Vous pouvez utiliser l'expéditeur de SMS pour envoyer des messages SMS aux utilisateurs.

Les expéditeurs de SMS sont des dispositifs mobiles Android désignés, connectés au serveur d'administration via les connexions réseau. Un expéditeur de SMS reçoit les commandes du serveur et les relaie aux dispositifs mobiles par le biais de SMS.

Il est possible d'utiliser les SMS pour avertir les dispositifs mobiles qu'ils doivent :

- télécharger et installer l'agent de dispositif mobile
- inscrire l'agent de dispositif mobile sur le serveur Mobile Security
- mettre à jour les composants de l'agent de dispositif mobile depuis le serveur Mobile Security
- synchroniser les stratégies avec le serveur Mobile Security
- supprimer, verrouiller ou localiser le dispositif mobile à distance

Installation de l'expéditeur de SMS



Remarque

Si vous n'utilisez pas l'expéditeur de SMS, toutes les fonctionnalités de Mobile Security fonctionneront normalement pour les dispositifs mobiles iOS, Android et BlackBerry.

Procédure

1. Sur le serveur d'administration, copiez le fichier de configuration à partir du dossier \Mobile Security\SmsSender sur une carte mémoire pour le dispositif pris en charge.
2. Insérez la carte mémoire sur le dispositif et exécutez le fichier de configuration pour installer le programme Expéditeur de SMS.

Une fois l'installation terminée, l'icône de l'application Expéditeur de SMS apparaît dans la liste des applications.

Que faire ensuite

Voir *Procédure d'installation de Trend Micro Mobile Security à la page 3-3* pour la tâche de configuration suivante.

Configuration de l'intégration d'Exchange Server

L'intégration d'Exchange Server est nécessaire pour établir la communication entre le serveur d'administration et Exchange Server.



Remarque

Trend Micro Mobile Security prend en charge uniquement Exchange Server 2007 ou les versions ultérieures, et il prend en charge l'intégration d'Exchange Server pour les dispositifs mobiles Windows Phone, iOS et Android.

Le tableau suivant décrit la procédure de configuration de l'intégration d'Exchange Server pour Trend Micro Mobile Security.

TABEAU 3-2. Procédure de configuration de l'intégration d'Exchange Server

ÉTAPE	ACTION	DESCRIPTION
Étape 1	Installer les outils d'administration de Microsoft Exchange Server	Avant de configurer les Paramètres d'Exchange Server , vous devez installer les outils de gestion de Microsoft Exchange Server sur l'ordinateur où vous souhaitez installer le connecteur Exchange. Voir la section Installation des outils d'administration de Microsoft Exchange Server (facultatif) à la page 2-12.
Étape 2	Configurer un compte pour le connecteur Exchange	Fournit des droits d'accès pour le connecteur Exchange. Voir la section Configuration d'un compte pour Exchange Connector à la page 3-19 pour la procédure complète.
Étape 3	Installer le connecteur Exchange	Établit la communication entre le serveur d'administration et Exchange Server. Voir la section Installation du connecteur Exchange à la page 3-22 pour la procédure complète.
Étape 4	Configurer les paramètres d'intégration d'Exchange Server	Voir la section Configuration de l'intégration d'Exchange Server à la page 4-19 pour la procédure complète.

Configuration d'un compte pour Exchange Connector

Procédure

1. Créez un compte utilisateur sur le serveur Active Directory.

2. Depuis l'ordinateur sur lequel vous souhaitez installer Exchange Connector, accédez à **Démarrer > Outils d'administration > Gestion de l'ordinateur** et procédez comme suit.
 - a. Développez les dossiers **Utilisateurs et groupes locaux** de l'arborescence de gauche, puis double-cliquez sur **Groupes**.
 - b. Cliquez avec le bouton droit sur **Administrateurs**, puis cliquez sur **Propriétés**.
 - c. Cliquez sur le bouton **Ajouter** de l'onglet **Général**, puis procédez comme suit :
 - i. Saisissez le nom d'utilisateur que vous avez créé à *l'étape 1 à la page 3-19* de cette procédure dans le champ **Nom de connexion** et cliquez sur **Rechercher**.

La boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs, des services, des comptes ou un groupe** s'affiche.
 - ii. Saisissez le nom d'utilisateur avec le nom de domaine (par exemple : nom-domaine\nom-utilisateur) dans le champ **Entrer le nom de l'objet à sélectionner** et cliquez sur **Vérifier les noms**.
 - iii. Cliquez sur **OK**.
 - d. Cliquez sur **OK** dans la boîte de dialogue **Propriétés administrateur**.
3. Sur le serveur Active Directory, procédez comme suit :
 - a. Accédez à **Démarrer > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.
 - b. Développez le dossier Utilisateurs de l'arborescence de gauche.
 - c. Cliquez avec le bouton droit sur le compte (nom d'utilisateur) que vous avez créé à *l'étape 1 à la page 3-19* de cette procédure, puis cliquez sur **Ajouter à un groupe**.
 - d. Effectuez l'une des actions suivantes :

- Pour Exchange Server 2007, saisissez **Administrateurs d'organisation Exchange** dans le champ **Entrer le nom de l'objet à sélectionner** et cliquez sur **Vérifier les noms**.
 - Pour Exchange Server 2010 et 2013, saisissez **Gestion de l'organisation** dans le champ **Entrer le nom de l'objet à sélectionner** et cliquez sur **Vérifier les noms**.
- e. Cliquez sur **OK**, puis cliquez à nouveau sur **OK** sur l'écran de confirmation.
4. Sur le serveur Active Directory, procédez comme suit :
- a. Accédez à **Démarrer > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.
 - b. Dans la barre de menu, cliquez sur **Afficher > Fonctions avancées**.
 - c. Développez le dossier Utilisateurs de l'arborescence de gauche.
 - d. Cliquez avec le bouton droit sur le compte (nom d'utilisateur) que vous avez créé à l'*Étape 1 à la page 3-19* de cette procédure, puis cliquez sur **Propriétés**.
 - e. Sur l'onglet **Sécurité**, cliquez sur **Ajouter**.
 - f. Saisissez le nom d'utilisateur que vous avez créé à l'*Étape 1 à la page 3-19* avec le nom de domaine (par exemple : nom_domaine\nom_utilisateur) dans le champ **Entrer le nom de l'objet à sélectionner**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
 - g. Sélectionnez le nom d'utilisateur dans la liste **Nom de groupe ou d'utilisateur**, puis cliquez sur **Avancé**.
 - h. Sélectionnez **Inclure les autorisations pouvant être héritées du parent de cet objet** et cliquez sur **OK**.
 - i. Cliquez sur **OK** dans la boîte de dialogue **Propriétés**.
-

Installation du connecteur Exchange



Remarque

Vous devez installer le connecteur Exchange sur l'ordinateur :

- où les outils de gestion de Microsoft Exchange Server sont installés,
 - qui appartient au même domaine qu'Exchange Server, et
 - doit pouvoir se connecter au serveur d'administration.
-

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Administration > Intégration d'Exchange Server**.
3. Cliquez sur **Cliquer ici pour télécharger** et enregistrez le fichier `ExchangeConnector.zip` sur votre ordinateur.
4. Extrayez le contenu du fichier `ExchangeConnector.zip` et lancez le fichier `ExchangeConnector.exe`.

L'assistant de configuration du connecteur Exchange apparaît.

5. Cliquez sur **Suivant** sur l'écran de **Bienvenue**.
6. Cochez **J'accepte les termes du contrat de licence** et cliquez sur **Suivant**.

Le programme d'installation vérifie maintenant si les outils de gestion Microsoft Exchange sont installés sur l'ordinateur. S'ils sont installés, la configuration lance l'écran suivant.

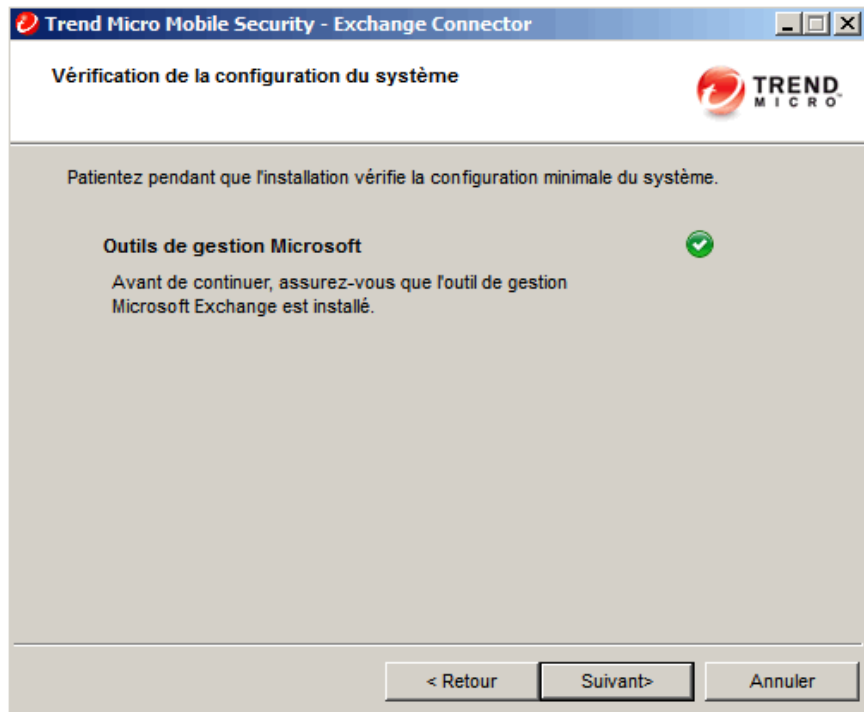


FIGURE 3-8. Vérification de l'installation de gestion Exchange réussie

7. Cliquez sur **Suivant** sur l'écran **Vérification de la configuration minimale requise**.
8. Cliquez sur **Parcourir** et sélectionnez le dossier de destination où vous souhaitez installer le connecteur Exchange, et puis cliquez sur **Suivant**.

L'écran **Compte de service** s'affiche.

9. Saisissez le nom d'utilisateur, le mot de passe et le nom de domaine (que vous avez créé dans [Configuration d'un compte pour Exchange Connector à la page 3-19](#)) pour accéder aux outils de gestion Exchange, puis cliquez sur **Suivant**.

10. Vérifiez les paramètres sur l'écran **Revoir les paramètres** et cliquez sur **Installer**.

La configuration commence à installer le connecteur Exchange.

11. Une fois l'installation terminée, cliquez sur **Suivant** puis cliquez sur **Terminer**.



Remarque

Le temps nécessaire à l'importation des informations des dispositifs mobiles à partir d'Exchange Server sur le serveur Mobile Security dépend du nombre de dispositifs mobiles que vous souhaitez importer. Par exemple, cela peut prendre jusqu'à plusieurs heures pour importer les informations de 5000 dispositifs mobiles depuis Exchange Server vers le serveur Mobile Security.

Que faire ensuite

Voir *Procédure d'installation de Trend Micro Mobile Security à la page 3-3* pour d'autres tâches de configuration.

Voir *Configuration de l'intégration d'Exchange Server à la page 3-18* pour la tâche suivante de configuration de l'intégration d'Exchange Server.

Mise à niveau de Mobile Security

Trend Micro Mobile Security prévoit la mise à niveau vers v9.0 SP2 à partir de la version v9.0 ou antérieure. Voir la section *Mise à jour des composants* dans le *Manuel de l'administrateur* pour la procédure.

Trend Micro Mobile Security ne prévoit pas la mise à niveau vers v9.0 SP2 à partir d'une version antérieure à 9.0. Toutefois, si vous souhaitez effectuer la mise à niveau à partir d'une version antérieure à v9.0, Trend Micro fournit un outil de migration permettant de faire migrer vos données depuis une ancienne version vers v9.0 Patch 1, puis vous pourrez effectuer la mise à niveau vers v9.0 Patch 1.

Consultez le lien suivant pour connaître la procédure détaillée de la migration de vos données depuis une ancienne version vers v9.0 SP2 :

<http://esupport.trendmicro.com/solution/en-US/1098095.aspx>

Suppression de composants du serveur

Cette section vous guide à travers les étapes à effectuer pour supprimer le serveur d'administration et le serveur de communication.

Procédure

1. Dans le Panneau de configuration Windows, double-cliquez sur **Programmes et fonctions**.

La fenêtre **Désinstaller ou modifier un programme** s'affiche.

2. Sélectionnez un des programmes suivants :
 - **Serveur de communication local de Trend Micro** —pour désinstaller le serveur de communication
 - **Trend Micro Mobile Security** —pour désinstaller le serveur d'administration

3. Cliquez sur **Désinstaller**.

Une boîte de dialogue s'affiche.

4. Dans la boîte de dialogue, sélectionnez **Fermer les applications automatiquement et tenter de les redémarrer lorsque l'installation est complète** et cliquez sur **OK**.
-

Chapitre 4

Configuration des composants du serveur

Ce chapitre aide les administrateurs à configurer les composants du serveur pour Trend Micro™ Mobile Security for Enterprise 9.0 SP2.

Ce chapitre contient les sections suivantes :

- *Configuration initiale du serveur à la page 4-3*
- *Configuration des paramètres de base de données à la page 4-5*
- *Configuration des paramètres du serveur de communication à la page 4-6*
- *Configuration des paramètres courants du serveur de communication à la page 4-7*
- *Configuration des paramètres du serveur de communication Android à la page 4-9*
- *Configuration des paramètres du serveur de communication iOS à la page 4-10*
- *Configuration des paramètres du serveur de communication BlackBerry à la page 4-12*
- *Configuration des paramètres d'inscription des dispositifs. à la page 4-14*
- *Personnalisation des Conditions d'utilisation de Mobile Security à la page 4-16*
- *Configuration des paramètres Active Directory (AD) à la page 4-17*
- *Configuration des paramètres de serveur d'administration à la page 4-18*

- *Configuration de l'intégration d'Exchange Server à la page 4-19*
- *États du connecteur Exchange à la page 4-19*
- *Configuration des paramètres de notifications/ rapports à la page 4-20*
- *Configuration des notifications administrateur à la page 4-21*
- *Vérification de la configuration de Mobile Security à la page 4-22*

Configuration initiale du serveur

Le tableau ci-dessous décrit la configuration initiale du serveur Trend Micro Mobile Security après son installation.

TABEAU 4-1. Configuration initiale du serveur Mobile Security

ÉTAPE	ACTION	DESCRIPTION
Étape 1	Configurer les paramètres de base de données.	Voir la section Configuration des paramètres de base de données à la page 4-5 pour la procédure complète.
Étape 2	Configurer les paramètres de serveur de communication.	Voir la section Configuration des paramètres courants du serveur de communication à la page 4-7 pour la procédure complète.
Étape 3	(Facultatif) Configurer les paramètres de serveur de communication pour Android.	Vous pouvez sauter cette étape si vous ne souhaitez pas gérer de dispositifs mobiles Android. Voir la section Configuration des paramètres du serveur de communication Android à la page 4-9 pour la procédure complète.
Étape 4	(Facultatif) Configurer les paramètres de serveur de communication pour iOS.	Vous pouvez sauter cette étape si vous ne souhaitez pas gérer de dispositifs mobiles iOS. Voir la section Configuration des paramètres du serveur de communication iOS à la page 4-10 pour la procédure complète.
Étape 5	(Facultatif) Configurer les paramètres de serveur de communication pour BlackBerry.	Vous pouvez sauter cette étape si vous ne souhaitez pas gérer de dispositifs mobiles BlackBerry. Voir la section Configuration des paramètres du serveur de communication BlackBerry à la page 4-12 pour la procédure complète.
Étape 6	Configurer les paramètres d'inscription des dispositifs.	Voir la section Configuration des paramètres d'inscription des dispositifs. à la page 4-14 pour la procédure complète.

ÉTAPE	ACTION	DESCRIPTION
Étape 7	(Facultatif) Personnaliser les Conditions d'utilisation de Mobile Security.	<p>Vous pouvez sauter cette étape si vous souhaitez utiliser les Conditions d'utilisation de Mobile Security par défaut.</p> <p>Voir la section Personnalisation des Conditions d'utilisation de Mobile Security à la page 4-16 pour la procédure complète.</p>
Étape 8	(Facultatif) Configurer les paramètres Active Directory.	<p>Vous pouvez sauter cette étape si vous ne souhaitez pas importer d'utilisateurs depuis le serveur Active Directory.</p> <p>Voir la section Configuration des paramètres Active Directory (AD) à la page 4-17 pour la procédure complète.</p>
Étape 9	(Facultatif) Configurer les paramètres du serveur d'administration.	<p>Vous pouvez sauter cette étape si votre serveur d'administration n'utilise pas de proxy pour accéder à Internet et si vous voulez utiliser l'adresse IP du serveur et le numéro de port par défaut.</p> <p>Voir la section Configuration des paramètres de serveur d'administration à la page 4-18 pour la procédure complète.</p>
Étape 10	(Facultatif) Configurer l'intégration d'Exchange Server.	<p>Vous pouvez sauter cette étape si vous ne voulez pas gérer de dispositifs mobiles qui utilisent Exchange ActiveSync.</p> <p>Voir la section Configuration de l'intégration d'Exchange Server à la page 4-19 pour la procédure complète.</p>
Étape 11	(Facultatif) Configurer les paramètres de notifications/rapports.	<p>Vous pouvez sauter cette étape si vous ne souhaitez pas envoyer d'invitations par SMS ou courriel aux utilisateurs.</p> <p>Voir la section Configuration des paramètres de notifications/rapports à la page 4-20.</p>

ÉTAPE	ACTION	DESCRIPTION
Étape 12	(Facultatif) Configurer les notifications administrateur.	Vous pouvez sauter cette étape si vous ne souhaitez pas recevoir les notifications de message d'erreur et les rapports programmés réguliers par courriel. Voir la section Configuration des notifications administrateur à la page 4-21 pour la procédure complète.
Étape 13	Vérifier la configuration de Mobile Security (Recommandé).	Utilisez l'écran de Configuration et vérification afin de vérifier les configurations de Mobile Security. Voir Vérification de la configuration de Mobile Security à la page 4-22 pour la procédure.
Étape 14	Changer le mot de passe du compte administrateur pour la console Web d'administration.	Utilisez l'écran Gestion des comptes d'administration après vous être connecté à la console Web d'administration. Reportez-vous à la rubrique <i>Modification compte administrateur</i> dans le <i>Guide de l'administrateur</i> pour la procédure.



Remarque

Vous devez effectuer la configuration initiale du serveur pour le serveur Mobile Security avant de continuer et d'installer l'agent de dispositif mobile sur les dispositifs mobiles.

Configuration des paramètres de base de données

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Administration > Paramètres de base de données**.
3. Entrez le nom du serveur ou l'adresse IP, votre nom d'utilisateur, votre mot de passe et le nom de la base de données.



Remarque

Si vous utilisez un port spécifique pour SQL Server, utilisez le format :

- Pour SQL Server : *<Nom du serveur SQL ou adresse IP>,<Port>*
- Pour SQL Server Express : *<Nom du serveur SQL ou adresse IP>,<Port>\<Nom de l'instance de SQL Server Express>*

4. Cliquez sur **Enregistrer**.

Que faire ensuite

Voir [Configuration initiale du serveur à la page 4-3](#) pour la tâche de configuration suivante.

Configuration des paramètres du serveur de communication

L'écran des paramètres de serveur de communication fournit les paramètres suivants :

- **Paramètres courants**—configuration des paramètres de base du serveur de communication.
- **Paramètres Android**—configuration des paramètres de personnalisation d'agent et de notifications pour la gestion des dispositifs mobiles Android.
- **Paramètres iOS**—configuration des paramètres SCEP et téléchargement des certificats APN (Apple Push Notification service) et SSL pour la gestion des dispositifs mobiles iOS.
- **Paramètres Windows Phone**—configuration de la programmation qui définit la fréquence à laquelle les dispositifs mobiles Windows Phone se connectent à un serveur Mobile Security pour mettre à jour les commandes et les paramètres de stratégie.
- **Paramètres BlackBerry**—configuration des paramètres de BlackBerry Enterprise Server pour la gestion des dispositifs mobiles BlackBerry.

Configuration des paramètres courants du serveur de communication

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Administration > Paramètres serveur de communication**.
3. Cliquez sur l'onglet **Paramètres courants**.
4. Sous la section **Type de serveur de communication**, sélectionnez l'une des deux options suivantes :
 - **Serveur de communication local**—si vous avez déjà installé le serveur de communication localement dans votre réseau.
 - **Serveur de communication du nuage**—si vous voulez utiliser le serveur de Communication déployé dans le nuage.
5. Sous la section **Paramètres de communication entre serveur de Communication et dispositifs mobiles**, configurez les éléments suivants :
 - **Nom de domaine externe ou adresse IP**—nom de domaine ou adresse IP du serveur de communication local.
 - **Port HTTP et port HTTPS**—utilisé par le serveur de communication local pour communiquer avec les dispositifs mobiles.

Les ports HTTP et HTTPS par défaut sont 8080 et 4343.



Remarque

Si vous configurez ces deux ports, les dispositifs mobiles utiliseront le port HTTPS pour communiquer avec le serveur de communication. Les dispositifs mobiles utiliseront le port HTTP uniquement s'ils ne peuvent pas communiquer en utilisant le port HTTPS.

6. Sous la section **Paramètres de communication entre serveur de Communication et serveur d'administration**, configurez les éléments suivants :

- **Nom du serveur de communication ou adresse IP**—nom de domaine ou adresse IP du serveur de communication local.
- **Port HTTPS**—utilisé par le serveur de communication local pour communiquer avec le serveur d'administration.



Remarque

S'il vous est nécessaire de personnaliser ce port HTTPS, consultez *Configuration des ports du serveur de communication à la page B-5* pour plus de renseignements.

7. Sous la section **Fréquence de collecte des informations**, configurez les éléments suivants :
 - **Fréquence de collecte des informations**—sélectionnez la fréquence à laquelle Mobile Security recueille les informations relatives aux applications installées sur les dispositifs mobiles.
 - **Fréquence de collecte des informations lorsque le dispositif mobile est en itinérance**—sélectionnez la fréquence à laquelle Mobile Security recueille les informations relatives aux applications installées sur les dispositifs mobiles lorsque le dispositif mobile est en itinérance.



Remarque

Ce paramètre s'applique uniquement aux dispositifs mobiles Android et iOS.

Mobile Security recueillera les informations relatives aux applications installées sur le dispositif mobile au moment de l'inscription du dispositif mobile, puis selon la fréquence choisie.

La modification de la fréquence réinitialise le minuteur.

8. Sous la section **Détection des dispositifs débridés**, sélectionnez **Suppression sélective sur le dispositif si celui-ci a fait l'objet d'un débridage** si vous souhaitez supprimer automatiquement et de manière sélective les dispositifs mobiles débridés.
 9. Cliquez sur **Enregistrer**.
-

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Configuration des paramètres du serveur de communication Android

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Administration > Paramètres serveur de communication**.
3. Cliquez sur l'onglet **Paramètres Android**.
4. Sous la section **Paramètres de notifications push**, sélectionnez **Activer les notifications push** si vous voulez envoyer les notifications push à des dispositifs mobiles Android.



Remarque

Si vous n'activez pas ce paramètre, les utilisateurs de dispositifs mobiles Android devront mettre à jour manuellement les stratégies de l'entreprise sur le dispositif mobile.

5. Sous la section **Personnalisation d'agent**, sélectionnez **Activer la personnalisation d'agent** pour ajouter l'adresse IP et le numéro de port du serveur dans l'application client Android que les utilisateurs téléchargeront à partir du serveur Mobile Security. Il ajoutera automatiquement la clé d'inscription prédéfinie à l'application client Android, si l'option **Activer la clé d'inscription prédéfinie** est sélectionnée dans les paramètres d'inscription de dispositif.

Cela signifie que l'adresse IP, le numéro de port et la clé d'inscription prédéfinie seront automatiquement inscrits dans l'application client et que les utilisateurs n'auront pas besoin de saisir ces renseignements manuellement.



Remarque

Ce paramètre est désactivé si vous utilisez le serveur de communication du nuage.

6. Cliquez sur **Enregistrer**.

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Configuration des paramètres du serveur de communication iOS

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Administration > Paramètres serveur de communication**.
3. Cliquez sur l'onglet **Paramètres iOS**.
4. Sous la section **Paramètres Apple Push Notification service (APNs)**, configurez les éléments suivants :
 - **Type de certificat** : Sélectionnez le type de votre certificat.
 - **Certificat** : Sélectionnez un certificat APNs (Apple Push Notification service) dans la liste déroulante, ou téléchargez-en un autre.
5. Sous la section **Paramètres de l'Extension du protocole d'inscription du certificat simple (SCEP)**, configurer les éléments suivants :
 - a. Sélectionnez **Activer SCEP**.
 - b. S'ils sont activés, remplissez les champs avec les informations suivantes :
 - **URL d'utilisateur SCEP** :
http://SCEP_IP/certsrv/mscep
 - **URL d'administrateur SCEP** :
Pour Windows Server 2008 :
http://SCEP_IP/certsrv/mscep_admin

Pour Windows Server 2003 :

http://SCEP_IP/certsrv/mscep

- **Compte d'utilisateur** : <Nom de l'utilisateur pour la connexion au serveur SCEP>
 - **Mot de passe de l'utilisateur** : <Mot de passe de l'utilisateur pour la connexion au serveur SCEP>
 - **Nom de certificat** : <un nom de certificat>
 - **Sujet** : O=TrendMicro,CN=Enroll
6. Sous la section **Informations d'identification du profil client**, configurez les éléments suivants :
- **Informations d'identification du profil client** : Sélectionnez un certificat pour information d'identification dans la liste déroulante, ou téléchargez-en un autre.
7. Cliquez sur **Enregistrer**.

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Configuration des paramètres du serveur de communication Windows Phone

Procédure

1. 1. Cliquez sur Administration → Paramètres du serveur de communication. 2. Cliquez sur l'onglet Paramètres Windows Phone. 3. Sélectionnez la fréquence à laquelle les dispositifs Windows Phone 8 se connectent au serveur Mobile Security pour mettre à jour les commandes et paramètres de stratégie. Plus la fréquence est élevée, plus la batterie des dispositifs mobiles s'épuisera. Le nouveau paramètre ne s'applique qu'aux dispositifs inscrits ultérieurement. 4. Cliquez sur Enregistrer.
2. Connectez-vous à la console Web d'administration.

3. Cliquez sur **Administration > Paramètres serveur de communication**.
 4. Cliquez sur l'onglet **Paramètres Windows Phone**.
 5. Définissez la fréquence à laquelle les dispositifs mobiles Windows Phone se connectent à un serveur Mobile Security pour mettre à jour les commandes et les paramètres de stratégie dans l'**intervalle de synchronisation Windows Phone**.
-

Configuration des paramètres du serveur de communication BlackBerry



Remarque

Avant de configurer les paramètres du serveur de communication BlackBerry, vous devez installer l'outil de commande **BRK-besuseradminclient** sur le serveur d'administration de Mobile Security.

Pour trouver le chemin d'accès de l'outil de commande de BlackBerry :

1. Connectez-vous au service d'administration BlackBerry.
 2. À partir du menu **Serveurs et composants**, cliquez sur **Topologie de la solution BlackBerry > Domaine BlackBerry > Affichage du composant**.
 3. Dans le volet droit, vous pouvez voir le nom de l'instance BlackBerry Enterprise Server.
-

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Administration > Paramètres serveur de communication**.
3. Cliquez sur l'onglet **Paramètres BlackBerry**.
4. Sous la section **Informations d'identification Service d'administration BlackBerry**, configurez les éléments suivants :
 - **Nom du serveur** : Nom du serveur BES (nom de votre ordinateur) ou adresse IP à laquelle vous avez installé le service d'administration BES

- **Port** : port utilisé pour la connexion de l'outil d'administration BES au serveur BES. Par défaut, le port est 443.
- **Compte utilisateur** : nom de l'administrateur pour le service d'administration BES
- **Mot de passe** : mot de passe pour le compte utilisateur
- **Nom de domaine** : Nom de domaine du serveur BES

**Remarque**

Si votre serveur Mobile Security ne parvient pas à se connecter au serveur BES à l'aide du nom du serveur BES, entrez l'adresse IP du serveur BES dans le champ **nom de serveur**.

-
5. Sous la section **Paramètres de base de données BlackBerry**, configurez les éléments suivants :

- **Adresse de la base de données** : nom de la base de données de la configuration BES ou adresse IP
- **Nom d'utilisateur** : nom d'utilisateur de base de données

**Remarque**

Vous devez créer un utilisateur de base de données avec les permissions de Connexion et Lecture de la base de données.

- **Mot de passe** : Mot de passe de connexion de l'utilisateur de la base de données
- **Nom de la base de données** : Nom de la base de données de configuration de BES

**Remarque**

Pour les paramètres de la base de données BlackBerry, Trend Micro Mobile Security prend uniquement en charge le mode d'authentification **SQL Server** pour SQL server.

6. Sous la section **Paramètres de l'outil de commande BlackBerry**, configurez les éléments suivants :
 - **Chemin d'accès de l'outil** : Chemin d'accès de l'installation de l'outil d'administration BlackBerry. Par exemple : C:\Program Files\Research In Motion\BlackBerry Enterprise Server Resource Kit\BlackBerry Enterprise Server User Administration Tool Client
 7. Cliquez sur **Enregistrer**.
-

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Configuration des paramètres d'inscription des dispositifs.

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Administration > Paramètres d'inscription des dispositifs**.
3. Cliquez sur l'onglet **Authentification**.
4. Sous la section **Authentification utilisateur**, sélectionnez une des options suivantes :
 - **Authentification à l'aide d'Active Directory**—pour utiliser les informations utilisateur depuis Active Directory afin d'authentifier les dispositifs mobiles.
 - **Authentification à l'aide d'une clé d'inscription**—pour utiliser une clé d'inscription pour authentifier les dispositifs mobiles.

Mobile Security génère automatiquement une clé d'inscription et l'envoi aux dispositifs dans un message d'invitation.
 - **Limitation d'utilisation de la clé d'inscription**—sélectionnez un des éléments suivants :

- **À utiliser plusieurs fois**—sélectionnez cette option si vous voulez utiliser une clé d'inscription pour chaque dispositif mobile à inscrire.
 - **À utiliser une seule fois**—sélectionnez cette option si vous voulez utiliser une clé d'inscription différente pour chaque dispositif mobile à inscrire.
 - **La clé d'inscription expire dans**—sélectionnez cette option si vous voulez cesser d'utiliser la clé d'inscription générée automatiquement après un certain temps, puis sélectionnez la durée dans la liste déroulante.
 - **Utiliser une clé d'inscription prédéfinie**—sélectionnez cette option si vous voulez générer manuellement la clé d'inscription, puis cliquez sur **Générer** pour générer la clé d'inscription. Cette clé d'inscription ne sera pas envoyée à l'utilisateur dans un message d'invitation.
 - **La clé d'inscription expire le**—sélectionnez cette option si vous voulez cesser d'utiliser la clé d'inscription générée manuellement à une certaine date, puis sélectionnez la date dans le calendrier.
5. Sous la section **Authentification dispositif**, effectuez l'une des actions suivantes :
- **Désactiver ce paramètre**—pour désactiver l'authentification des dispositifs mobiles.
 - **Authentifier à l'aide de l'IMEI ou de l'adresse Wi-Fi MAC**—ce paramètre vous permet de télécharger une liste des dispositifs mobiles que vous souhaitez authentifier.
 - a. Cliquez sur **Exporter le modèle de liste de dispositifs approuvés** pour télécharger le modèle et créer la liste des dispositifs approuvés.
 - b. Après avoir créé la liste, cliquez sur **Parcourir** pour sélectionner et importer la liste des dispositifs mobiles que vous avez créée lors de l'étape précédente.
 - c. Cliquez sur **Vérifier le format des données** pour vérifier le format de données dans la liste des dispositifs approuvés. Après la vérification, Mobile Security affiche tous les dispositifs mobiles dans la liste **État des dispositifs approuvés**.

- d. Sélectionnez une des options suivantes :
- **Supprimer les dispositifs non authentifiés**—pour supprimer les dispositifs mobiles qui existent déjà dans l'écran **Gestion des dispositifs**, mais n'existent pas dans la liste des dispositifs approuvés que vous importez.
 - **Afficher les dispositifs non authentifiés dans le groupe "non authentifiés"**—pour déplacer tous les dispositifs mobiles qui existent déjà dans l'écran **Gestion des dispositifs**, mais n'existent pas dans la liste des dispositifs approuvés que vous importez, vers le groupe **non authentifiés**.



Remarque

Si vous utilisez l'authentification de dispositif, Mobile Security regroupera tous les dispositifs mobiles en fonction de la liste de dispositifs approuvés que vous utilisez.

6. Cliquez sur **Enregistrer**.
-

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Personnalisation des Conditions d'utilisation de Mobile Security

Vous pouvez personnaliser les **Conditions d'utilisation** pour les utilisateurs qui veulent télécharger, installer et utiliser l'agent de dispositif mobile.

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Administration > Paramètres d'inscription des dispositifs**.
3. Sur l'onglet **Personnalisation des Conditions d'utilisation**, cliquez sur **Télécharger l'exemple des Conditions d'utilisation** et enregistrez le fichier `Eula_agreement.zip` sur votre ordinateur.

4. Extrayez le contenu du fichier `Eula_agreement.zip`.
5. À l'aide d'un éditeur HTML, ouvrez le fichier `Eula_agreement.html`, effectuez les modifications nécessaires, puis enregistrez le fichier.
6. Sur l'onglet **Personnalisation des Conditions d'utilisation** de l'écran **Paramètres d'inscription de dispositifs**, cliquez sur **Parcourir** puis sélectionnez le fichier que vous avez modifié lors de l'étape précédente (*Étape 5 à la page 4-17*) de cette procédure, et cliquez sur **Ouvrir**.

L'affichage des Conditions d'utilisation met à jour le contenu du fichier téléchargé.

7. Cliquez sur **Enregistrer**.
-

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Configuration des paramètres Active Directory (AD)

Trend Micro Mobile Security 9.0 SP2 vous offre la possibilité de configurer l'authentification des utilisateurs basée sur Active Directory (AD). Une fois configurée, vous pouvez utiliser votre Active Directory d'entreprise afin d'ajouter des dispositifs mobiles à la liste de dispositifs.

Si vous ne souhaitez pas utiliser Active Directory pour l'authentification utilisateur ou si vous ne souhaitez pas ajouter d'utilisateurs depuis active directory, vous n'avez alors pas besoin de configurer ce paramètre.

Procédure

1. Connectez-vous à la console Web d'administration.
 2. Cliquez sur **Administration > Paramètres Active Directory**.
 3. Entrez le nom de l'hôte ou son adresse IP, son numéro de port, votre nom d'utilisateur et mot de passe de domaine.
 4. Cliquez sur **Enregistrer**.
-

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Configuration des paramètres de serveur d'administration

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Administration > Paramètres serveur d'administration**.
3. Cliquez sur l'onglet **Connexion**, puis spécifiez le nom du serveur d'administration ou l'adresse IP et son numéro de port. Le numéro de port par défaut du serveur d'administration est 443.



Remarque

L'adresse IP et le numéro de port sur cet écran sont utilisés pour accéder à la console Web d'administration via un navigateur Web.

4. Si le serveur d'administration utilise un serveur proxy pour se connecter à Internet, spécifiez les paramètres de proxy dans l'onglet **Proxy** :
 - a. Dans l'onglet **Proxy**, sélectionnez **Utilisez les paramètres de proxy suivants pour le serveur d'administration**, et indiquez le nom du serveur proxy ou l'adresse IP et le numéro de port.
 - b. Si le serveur proxy nécessite une authentification, entrez l'ID utilisateur et le mot de passe dans la section **Authentification du Proxy**.
5. Cliquez sur **Enregistrer**.

Vous devrez désormais utiliser la nouvelle adresse IP et le numéro de port pour vous connecter à la console Web d'administration.

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Configuration de l'intégration d'Exchange Server

Procédure

1. Sous la section **Connecteur Exchange**, sélectionnez **Activer cette option pour assurer que seuls les dispositifs mobiles compatibles accèdent à Exchange Server**.

Consultez *États du connecteur Exchange à la page 4-19* pour connaître les différents états du connecteur Exchange affichés sur l'écran **d'intégration d'Exchange Server**.

2. Sous la section **Contrôle d'accès Exchange**, effectuez ce qui suit :
 - a. Sélectionnez **Autoriser l'accès aux données d'entreprise (courriels, calendrier, contacts, etc.) pour les dispositifs suivants** puis sélectionnez l'une des options suivantes :
 - Dispositifs sains seuls
 - Dispositifs sains et non-compatiblesVoir le sujet *Information du Tableau de bord* dans le *Manuel de l'administrateur* sur les différents états d'enregistrement des dispositifs mobiles.
 - b. Sélectionnez le nombre de jours après lesquels les dispositifs à l'exception des dispositifs sélectionnés seront bloqués à partir de la liste déroulante.
 3. Cliquez sur **Enregistrer**.
-

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Pour d'autres étapes de configuration de l'intégration d'Exchange Server, voir *Configuration de l'intégration d'Exchange Server à la page 3-18*.

États du connecteur Exchange

Le tableau ci-dessous répertorie les différents états du connecteur Exchange affichés sur l'écran **Intégration d'Exchange Server**.

TABLEAU 4-2. États du connecteur Exchange

ÉTAT	DESCRIPTION
Normal	Le connecteur Exchange est connecté au serveur d'administration.
En attente du connecteur Exchange	Le serveur d'administration attend que le connecteur Exchange se connecte au serveur d'administration.
Avertissement	Le connecteur Exchange n'est plus connecté au serveur d'administration depuis plus de cinq minutes.
Déconnecté	Le connecteur Exchange n'est plus connecté au serveur d'administration depuis plus de neuf minutes.
Désactivé	Le connecteur Exchange est connecté au serveur d'administration, mais désactivé dans les paramètres d'intégration d'Exchange Server de Mobile Security.

Configuration des paramètres de notifications/rapports

Vous pouvez configurer la source de notification de manière à envoyer les courriels de notification aux administrateurs. Ce paramètre est également nécessaire si vous souhaitez envoyer les détails d'installation et d'inscription de l'agent de dispositif mobile aux utilisateurs par SMS et/ou courriel.

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Notifications/Rapports > Paramètres**.
3. Vous pouvez désormais configurer les paramètres du serveur SMTP et la liste d'expéditeurs de SMS pour les notifications sortantes :
 - Pour configurer les paramètres du serveur SMTP pour les messages de notification par courriel : tapez dans le champ de l'adresse électronique de

l'expéditeur **De**, l'adresse IP du serveur SMTP et le numéro de port. Si le serveur SMTP nécessite une authentification, sélectionnez **Authentification**, puis entrez le nom d'utilisateur et le mot de passe.

- Pour configurer le texte du message des notifications : dans la section **Paramètres des expéditeurs de SMS**, cliquez sur **Ajouter**, saisissez le numéro de téléphone d'un expéditeur de SMS sur la fenêtre contextuelle qui apparaît, et cliquez sur **Enregistrer**. Le numéro de téléphone que vous venez d'ajouter apparaît dans la liste d'expéditeurs de SMS. Vérifiez que le champ **État** affiche **Connecté** pour le numéro que vous avez configuré. Si le champ **État** affiche **Déconnecté**, assurez-vous que l'expéditeur de SMS peut se connecter au serveur d'administration.



AVERTISSEMENT!

Assurez-vous que le numéro de téléphone utilisé ici est le même que celui qui est configuré sur le dispositif de l'expéditeur de SMS. Sinon, l'expéditeur de SMS ne sera pas en mesure de se connecter au serveur d'administration.

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Pour d'autres étapes sur la configuration de l'agent de dispositif mobile, voir *Configuration Agent de dispositif mobile à la page 5-4*.

Configuration des notifications administrateur

Vous pouvez configurer des paramètres de notifications et rapports administrateur afin de recevoir les notifications de message d'erreur et les rapports programmés réguliers par courriel.

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Notifications/Rapports > Notifications/rapports administrateur**.
3. Sélectionnez les notifications et les rapports que vous souhaitez recevoir par courriel puis cliquez sur les notifications et les rapports individuels pour modifier

leurs contenus. Cliquez sur **Enregistrer** quand vous avez terminé, pour revenir à l'écran **Notifications/rapports administrateur**.



Remarque

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

4. Cliquez sur **Enregistrer**.
-

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Vérification de la configuration de Mobile Security

Mobile Security fournit l'écran **Configuration et vérification** pour vérifier si tous les paramètres que vous avez configurés sont corrects.

Procédure

1. Connectez-vous à la console Web d'administration.
 2. Cliquez sur **Administration > Configuration et Vérification**.
 3. Cliquez sur **Vérifier la configuration de Mobile Security**.
-

Que faire ensuite

Voir *Configuration initiale du serveur à la page 4-3* pour la tâche de configuration suivante.

Chapitre 5

Gestion de l'Agent de dispositif mobile

Ce chapitre fournit les exigences et les modèles des dispositifs mobiles que l'Agent de dispositif mobile prend en charge, et aborde les différentes méthodes de déploiement de l'agent de dispositif mobile sur différentes plateformes.

Ce chapitre contient les sections suivantes :

- *Plates-formes et dispositifs mobiles pris en charge à la page 5-3*
- *Stockage et mémoire du dispositif à la page 5-3*
- *Configuration Agent de dispositif mobile à la page 5-4*
- *Configuration du serveur pour l'envoi de messages d'invitation (Facultatif) à la page 5-5*
- *Configuration du message d'installation à la page 5-5*
- *Envoi d'invitations aux dispositifs mobiles à la page 5-6*
- *Installation du MDA sur les dispositifs mobiles à la page 5-10*
- *Dispositifs mobiles iOS à la page 5-10*
- *Dispositifs mobiles Android à la page 5-10*
- *Inscription du MDA sur le serveur Mobile Security à la page 5-13*

- *Dispositifs mobiles Android à la page 5-13*
- *Dispositifs mobiles iOS à la page 5-15*
- *Dispositifs mobiles Windows Phone à la page 5-19*

Plates-formes et dispositifs mobiles pris en charge



Remarque

Assurez-vous que les dispositifs mobiles peuvent se connecter au serveur de communication par Wi-Fi, 3G/GPRS ou en utilisant une connexion Internet sur un ordinateur hôte.

Avant d'installer et d'utiliser le programme client d'agents de dispositif mobile (connu sous le nom d'agent de dispositif mobile) sur les dispositifs mobiles, assurez-vous que vos dispositifs mobiles disposent de la configuration minimale requise.

Stockage et mémoire du dispositif

TABEAU 5-1. Configuration minimale requise

SYSTÈME D'EXPLOITATION	MÉMOIRE (Mo)	ESPACE DISQUE (Mo)
Android 2.1 à 4.4.x	10	8
iOS 4.3 à 8.0	4	3



Remarque

Pour les dispositifs mobiles BlackBerry, Mobile Security prend en charge BES 5.x.



Remarque

Les dispositifs mobiles BlackBerry ne requièrent pas l'installation d'un logiciel client Mobile Security (Agent de dispositif mobile).

Configuration Agent de dispositif mobile

TABEAU 5-2. Procédure de configuration Agent de dispositif Mobile

ÉTAPE	ACTION	DESCRIPTION	
Étape 1	(Facultatif) Installer l'expéditeur de SMS	Si vous souhaitez envoyer les détails d'installation et d'inscription aux utilisateurs par SMS et/ou courriel, réalisez ces étapes.	Si vous ne souhaitez pas envoyer de notifications par SMS, vous devez installer un expéditeur de SMS. Voir la section Installation de l'expéditeur de SMS à la page 3-18 pour la procédure complète.
Étape 2	(Facultatif) Configurer les paramètres de notifications des dispositifs mobiles.		Voir la section Configuration des paramètres de notifications/ rapports à la page 4-20 pour la procédure complète.
Étape 3	(Facultatif) Configurer le message d'installation que Mobile Security envoie par e-mail et/ou SMS aux utilisateurs.		Le message d'installation contient l'URL à laquelle les utilisateurs peuvent accéder pour télécharger et installer le package d'installation MDA. Voir la section Configuration du message d'installation à la page 5-5 pour la procédure complète.
Étape 4	(Facultatif) Envoyer une invitation aux dispositifs mobiles		Voir la section Envoi d'invitations aux dispositifs mobiles à la page 5-6 pour la procédure complète.
Étape 5	Installer MDA sur les dispositifs mobiles	Voir la section Installation du MDA sur les dispositifs mobiles à la page 5-10 pour la procédure complète.	

ÉTAPE	ACTION	DESCRIPTION
Étape 6	Synchronisation de MDA avec le serveur Mobile Security	Voir la section Inscription du MDA sur le serveur Mobile Security à la page 5-13 pour la procédure complète.

Configuration du serveur pour l'envoi de messages d'invitation (Facultatif)

Vous pouvez configurer les messages d'invitation pour envoyer les détails d'installation et d'inscription aux utilisateurs par SMS et/ou courriel.

Vous pouvez ignorer cette section si vous ne voulez pas utiliser le message d'invitation pour l'installation MDA et l'inscription.

Configuration du message d'installation

Utilisez l'écran **Message d'installation** pour saisir le message que vous souhaitez afficher.

Cette tâche est une étape de la procédure de configuration de l'agent de dispositif mobile.

Voir la section [Configuration Agent de dispositif mobile à la page 5-4](#).

Procédure

1. Connectez-vous à la console Web d'administration.
2. Cliquez sur **Notifications/Rapports > Notifications utilisateur**.
3. Cliquez sur le texte **Inscription de dispositifs mobiles** pour ouvrir l'écran **Configuration d'inscription de dispositif mobile**.
4. Vérifiez le sujet, le courriel et/ou le SMS par défaut dans la ou les zones de textes correspondantes, et modifiez-les le cas échéant.



Remarque

Le message d'installation doit comprendre les caractères «%DOWNLOADURL%» qui seront automatiquement remplacés par l'URL qui permet aux utilisateurs de télécharger le fichier d'installation de l'agent de dispositif mobile.



Remarque

La notification par courriel envoie uniquement le lien de téléchargement pour télécharger les fichiers d'installation client, et ne remplit pas automatiquement l'adresse IP et le numéro de port du serveur dans l'écran d'inscription.

5. Cliquez sur **Enregistrer**.
 6. Cliquez sur **Notifications/Rapports > Notifications utilisateur**.
 7. Sélectionnez **Inscription de dispositif mobile** et cliquez sur **Enregistrer**.
-

Envoi d'invitations aux dispositifs mobiles

Cette tâche est une étape de la procédure de configuration de Agent de dispositif mobile.

Voir la section *Configuration Agent de dispositif mobile à la page 5-4*.

Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.
L'écran **Dispositifs** apparaît.
3. Vous pouvez désormais inviter un dispositif mobile, un lot de dispositifs mobiles, un groupe d'utilisateurs ou d'adresses électroniques (liste de distribution) depuis Active Directory :
 - Pour inviter un dispositif mobile :
 - a. Cliquez sur **Inviter des utilisateurs > Inviter un seul utilisateur**.

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

- b. Dans la fenêtre **Inviter un seul utilisateur**, configurez les champs suivants :
- **Numéro de téléphone**—saisissez le numéro de téléphone d'un dispositif mobile. Pour vous assurer que le dispositif mobile peut correctement recevoir des messages de notification d'un expéditeur de SMS, vous pouvez entrer l'indicatif de pays (contenant entre 1 et 5 chiffres). Inutile de saisir le préfixe international de numérotation directe.
 - **Courriel**—entrez l'adresse électronique de l'utilisateur pour envoyer un courriel de notification.
 - **Nom d'utilisateur**—tapez le nom du dispositif mobile pour l'identifier dans l'arborescence des dispositifs.
 - **Groupe**—sélectionnez le nom du groupe auquel le dispositif mobile appartient depuis la liste déroulante. Vous pourrez modifier ultérieurement le groupe auquel l'agent de dispositif mobile appartient.

**Conseil**

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

- Pour inviter un lot de dispositifs mobiles :
 - a. Cliquez sur **Inviter des utilisateurs > Inviter un lot**.
 - b. Entrez les informations des dispositifs en utilisant le format suivant dans la zone de texte de la fenêtre qui s'affiche :

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

**Remarque**

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

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

- Pour inviter un utilisateur ou un groupe d'adresses électroniques (liste de distribution) à partir d'Active Directory :
 - a. Cliquez sur **Inviter des utilisateurs** > **Inviter à partir d'Active Directory**.
 - b. Entrez les informations utilisateur dans le champ de recherche fourni et cliquez sur **Rechercher**.
 - c. Sélectionnez l'utilisateur parmi les résultats de la recherche et cliquez sur **Inviter des dispositifs**.

4. Cliquez sur **Enregistrer**.

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

Envoi d'invitations aux dispositifs mobiles

Cette tâche est une étape de la procédure de configuration de l'Agent de dispositif mobile.

Voir la section [Configuration Agent de dispositif mobile à la page 5-4](#).


Procédure

1. Connectez-vous à la console d'administration Mobile Security.
2. Cliquez sur **Dispositifs** dans la barre de menu.
L'écran **Dispositifs** apparaît.
3. Vous pouvez désormais inviter un dispositif mobile, un lot de dispositifs mobiles, un groupe d'utilisateurs ou d'adresses électroniques (liste de distribution) depuis Active Directory :
 - Pour inviter un dispositif mobile :
 - a. Cliquez sur **Inviter des utilisateurs** > **Inviter un seul utilisateur**.

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

- b. Dans la fenêtre **Inviter un seul utilisateur**, configurez les champs suivants :
- **Numéro de téléphone**—saisissez le numéro de téléphone d'un dispositif portable. Pour vous assurer que le dispositif mobile peut correctement recevoir des messages de notification d'un expéditeur de SMS, vous pouvez entrer l'indicatif de pays (contenant entre 1 et 5 chiffres). Inutile de saisir le préfixe international de numérotation directe.
 - **Courriel**—entrez l'adresse électronique de l'utilisateur pour envoyer un courriel de notification.
 - **Nom d'utilisateur**—tapez le nom du dispositif mobile pour l'identifier dans l'arborescence des dispositifs.
 - **Groupe**—sélectionnez le nom du groupe auquel le dispositif mobile appartient depuis la liste déroulante. Vous pourrez modifier ultérieurement le groupe auquel l'agent de dispositif mobile appartient.

**Conseil**

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

- Pour inviter un lot de dispositifs mobiles :
 - a. Cliquez sur **Inviter des utilisateurs > Inviter un lot**.
 - b. Entrez les informations des dispositifs en utilisant le format suivant dans la zone de texte de la fenêtre qui s'affiche :

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

**Remarque**

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

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

- Pour inviter un groupe d'utilisateurs ou d'adresses électroniques (liste de distribution) à partir d'Active Directory :
 - a. Cliquez sur **Inviter des utilisateurs** > **Inviter à partir d'Active Directory**.
 - b. Entrez les informations utilisateur dans le champ de recherche fourni et cliquez sur **Rechercher**.
 - c. Sélectionnez l'utilisateur parmi les résultats de la recherche et cliquez sur **Inviter des dispositifs**.

4. Cliquez sur **Enregistrer**.

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

Installation du MDA sur les dispositifs mobiles

Cette tâche est une étape de la procédure de configuration de l'agent de dispositif mobile.

Voir la section [Configuration Agent de dispositif mobile à la page 5-4](#).

Dispositifs mobiles iOS

Vous pouvez installer le MDA pour les dispositifs mobiles iOS depuis Apple Store. Pour télécharger et installer le MDA, allez sur Apple Store, recherchez l'application **ENT Security**, et cliquez sur **Installer**.

Dispositifs mobiles Android

Vous pouvez installer le MDA sur les dispositifs mobiles Android par l'une des méthodes suivantes :

- **Méthode d'installation 1**—Téléchargez et installez le MDA directement sur un dispositif mobile. Voir [Méthode d'installation 1 à la page 5-11](#) pour la procédure.

- **Méthode d'installation II**—Téléchargez le package d'installation MDA sur un ordinateur à l'aide d'un navigateur Web, puis transférez-le sur le dispositif mobile et installez-le. Voir *Méthode d'installation II à la page 5-12* pour la procédure.
- **Méthode d'installation III**—Téléchargez le package d'installation MDA sur un ordinateur à l'aide de la console de gestion des dispositifs mobiles, puis transférez-le sur le dispositif mobile et installez-le. Voir *Méthode d'installation III à la page 5-13* pour la procédure.

Méthode d'installation I

Cette méthode vous permet de télécharger et installer le MDA directement sur un dispositif mobile.

Voir *Méthode d'installation II à la page 5-12* et *Méthode d'installation III à la page 5-13* pour les deux autres méthodes.

Procédure

1. Effectuez l'une des actions suivantes :
 - Si vous utilisez le Serveur de communication local ou serveur de communication du nuage, ouvrez le SMS ou le courriel reçu de Mobile Security et accédez à l'URL depuis le dispositif mobile sur lequel vous souhaitez installer le MDA afin de télécharger le package d'installation.
 - Si vous utilisez le Serveur de communication local, accédez à l'une des URL suivantes à l'aide d'un navigateur Web depuis le dispositif mobile sur lequel vous souhaitez installer le MDA afin de télécharger le package d'installation :
http://External_domain_name_or_IP_address:HTTP_port/mobile
ou
https://External_domain_name_or_IP_address:HTTPS_port/mobile



Remarque

Remplacez *External_domain_name_or_IP_address*, *HTTP_port*, et *HPTTS_port* par ce que vous avez configuré dans **Administration > Paramètres du serveur de communication > Paramètres courants > Paramètres pour la communication entre serveur de communication et dispositifs mobiles**.

2. Si l'installation ne démarre pas automatiquement, lancez le package d'installation et terminez l'installation.
-

Méthode d'installation II

Si vous utilisez le serveur de communication local, cette méthode vous permet de télécharger le package d'installation MDA sur un ordinateur à l'aide d'un navigateur Web, puis de le transférer sur le dispositif mobile pour l'installer.

Voir *Méthode d'installation I* à la page 5-11 et *Méthode d'installation III* à la page 5-13 pour les deux autres méthodes.

Procédure

1. Sur un ordinateur, accédez à l'une des URL ci-dessous pour télécharger le package d'installation :

http://External_domain_name_or_IP_address:HTTP_port/mobile

ou

https://External_domain_name_or_IP_address:HTTPS_port/mobile



Remarque

Remplacez *External_domain_name_or_IP_address*, *HTTP_port*, et *HPTTS_port* par ce que vous avez configuré dans **Administration > Paramètres du serveur de communication > Paramètres courants > Paramètres pour la communication entre serveur de communication et dispositifs mobiles**.

2. Sélectionnez le système d'exploitation du dispositif mobile pour télécharger le package d'installation.

3. Copiez le package d'installation du dispositif mobile.
 4. Lancez le fichier d'installation et effectuez l'installation.
-

Méthode d'installation III

Cette méthode vous permet de télécharger le package d'installation MDA sur un ordinateur qui utilise la console Web d'administration, puis de le transférer sur le dispositif mobile pour l'installer.

Voir *Méthode d'installation I* à la page 5-11 et *Méthode d'installation II* à la page 5-12 pour les deux autres méthodes.

Procédure

1. Connectez-vous à la console Web d'administration.
 2. Cliquez sur **Administration > Paramètres d'inscription des dispositifs**.
 3. Sur l'onglet **Installation de l'agent**, sélectionnez le package d'installation de l'agent et cliquez sur **Télécharger** pour télécharger le fichier ZIP sur votre ordinateur.
 4. Décompressez le fichier ZIP et copiez le fichier d'installation sur le dispositif mobile.
 5. Lancez le fichier d'installation et effectuez l'installation.
-

Inscription du MDA sur le serveur Mobile Security

Vous devez inscrire manuellement le MDA sur le serveur Mobile Security si vous installez manuellement le MDA ou si le processus d'inscription automatique échoue.

Cette tâche est une étape de la procédure de configuration de l'agent de dispositif mobile.

Dispositifs mobiles Android

Vous pouvez inscrire le MDA en utilisant l'une des méthodes suivantes :

- Inscription à l'aide d'un code QR.

Utilisez cette méthode si vous utilisez le Serveur de communication local ou le serveur de communication du nuage.

- Inscription à l'aide de l'adresse du serveur.

Utilisez cette méthode si vous utilisez le Serveur de communication local.

- Inscription sans adresse de serveur.

Utilisez cette méthode si vous utilisez le serveur de communication du nuage.

Inscription à l'aide du code QR

Procédure

1. Lancez le programme Agent de dispositif mobile sur le dispositif mobile.
2. Sélectionnez **Inscription à l'aide du code QR**.
3. Ouvrez le courriel d'invitation sur un ordinateur ou un autre dispositif mobile et scannez le code QR reçu dans le courriel d'invitation à l'aide de l'appareil photo du dispositif mobile.
4. Si nécessaire, saisissez un nom d'utilisateur et un mot de passe dans les champs prévus et cliquez sur **OK**.

L'agent de dispositif mobile sera enregistré sur le serveur Mobile Security.

Inscription à l'aide de l'adresse du serveur

Procédure

1. Lancez le programme Agent de dispositif mobile sur le dispositif mobile.
2. Cliquez sur **Inscription manuelle**.
3. Cliquez sur l'onglet **Serveur local**, saisissez l'adresse du serveur et le numéro de port dans les champs correspondants, puis cliquez sur **Suivant**.

4. Saisissez la clé d'inscription ou le nom d'utilisateur et mot de passe dans les champs correspondants, puis cliquez sur **Suivant**.

L'agent de dispositif mobile sera enregistré sur le serveur Mobile Security.

Inscription sans adresse de serveur

Procédure

1. Lancez le programme Agent de dispositif mobile sur le dispositif mobile.
2. Cliquez sur **Inscription manuelle**.
3. Cliquez sur l'onglet **Serveur du nuage**, saisissez la clé d'inscription que vous avez reçue dans le courriel d'invitation, puis cliquez sur **Suivant**.

L'agent de dispositif mobile sera inscrit sur le serveur Mobile Security.

Dispositifs mobiles iOS

Pour pouvoir gérer les dispositifs mobiles iOS depuis le serveur Mobile Security, vous devez installer un profil de mise en service sur les dispositifs mobiles. Ce profil de mise en service doit vous identifier, vous (par le biais de votre certificat de développement) et votre dispositif (en indiquant son identifiant de dispositif unique).



AVERTISSEMENT!

Le code JavaScript doit être activé pour Safari pour l'inscription de dispositifs mobiles iOS. Sinon l'inscription échouera.

Vous pouvez inscrire le MDA en utilisant l'une des méthodes suivantes :

- Inscription à l'aide d'un code QR.

Utilisez cette méthode si vous utilisez le Serveur de communication local ou le serveur de communication du nuage.

- Inscription à l'aide de l'adresse du serveur.

Utilisez cette méthode si vous utilisez le Serveur de communication local.

- Inscription sans adresse de serveur.

Utilisez cette méthode si vous utilisez le serveur de communication du nuage.

Inscription à l'aide du code QR

Procédure

1. Lancez le programme Agent de dispositif mobile sur le dispositif mobile.
2. Saisissez **Inscription à l'aide du code QR**.
3. Ouvrez le courriel d'invitation sur un ordinateur ou un autre dispositif mobile et scannez le code QR reçu dans le courriel d'invitation en utilisant l'appareil photo du dispositif mobile.



Remarque

Il se peut qu'une boîte de dialogue s'ouvre pour vous demander d'installer la racine CA configurée pour le Serveur de communication local. Si vous ne voyez pas cette boîte de dialogue, sautez les étapes 4 à 6 et passez directement à l'étape 7.

4. Sélectionnez **OK**.
L'écran **Installer un profil** s'affiche pour **TMMSMDM-CA**.
5. Dans l'écran **Installer un profil**, cliquez sur **Installer**, puis dans l'écran **Avertissement**, cliquez sur **Installer**.
6. Une fois le profil installé, cliquez sur **Terminé** dans l'écran **Profil installé**.
7. Si nécessaire, saisissez un nom d'utilisateur et un mot de passe dans les champs prévus et cliquez sur **Connexion**.

L'écran **Installer un profil** s'affiche pour le **Profil d'inscription MDM**.

8. Sur l'écran **Installer un profil**, appuyez sur **Installer**, puis sur **Installer maintenant** sur la boîte de dialogue contextuelle de confirmation.

9. Si le dispositif mobile requiert un code, saisissez votre code sur l'écran **Entrer code** qui s'affiche, puis appuyez sur **Terminé**.

L'écran **Installation de profil** s'affiche.

10. Sélectionnez **Installer** dans l'écran **Avertissement** de confirmation.

Le processus d'installation de profil démarre. Une fois le processus terminé, l'écran **Profil installé** s'affiche.

11. Sélectionnez **Terminé**.

Inscription à l'aide de l'adresse du serveur

Procédure

1. Lancez le programme Agent de dispositif mobile sur le dispositif mobile.
2. Cliquez sur **Inscription manuelle**.
3. Cliquez sur l'onglet **Serveur local**, saisissez l'adresse du serveur et le numéro de port dans les champs correspondants, puis cliquez sur **Inscrire**.
4. Saisissez la clé d'inscription ou le nom d'utilisateur et mot de passe dans les champs correspondants, puis cliquez sur **Suivant**.

Une boîte de dialogue s'ouvre vous demandant d'installer la racine CA configurée pour le serveur de communication.



Remarque

Il se peut qu'une boîte de dialogue s'ouvre pour vous demander d'installer la racine CA configurée pour le Serveur de communication local. Si vous ne voyez pas cette boîte de dialogue, sautez les étapes 5 à 7 et passez directement à l'étape 8.

5. Sélectionnez **OK**.

L'écran **Installer un profil** s'affiche pour **TMMSMDM-CA**.

6. Dans l'écran **Installer un profil**, cliquez sur **Installer**, puis dans l'écran **Avertissement**, cliquez sur **Installer**.

7. Une fois le profil installé, cliquez sur **Terminé** dans l'écran **Profil installé**.
8. Si nécessaire, saisissez un nom d'utilisateur et un mot de passe dans les champs prévus et cliquez sur **Connexion**.

L'écran **Installer un profil** s'affiche pour le **Profil d'inscription MDM**.

9. Sur l'écran **Installer un profil**, appuyez sur **Installer**, puis sur **Installer maintenant** sur la boîte de dialogue contextuelle de confirmation.
10. Si le dispositif mobile requiert un code, saisissez votre code sur l'écran **Entrer code** qui s'affiche, puis appuyez sur **Terminé**.

L'écran **Installation de profil** s'affiche.

11. Appuyez sur **Installer** sur l'écran **Avertissement** de confirmation.

Le processus d'installation de profil démarre. Une fois le processus terminé, l'écran **Profil installé** s'affiche.

12. Sélectionnez **Terminé**.
-

Inscription sans adresse de serveur

Procédure

1. Lancez le programme Agent de dispositif mobile sur le dispositif mobile.
2. Cliquez sur **Inscription manuelle**.
3. Sur l'onglet **Serveur nuage**, saisissez le code d'authentification, puis cliquez sur **Inscription**.

L'écran **Installer un profil** s'affiche pour le **Profil d'inscription MDM**.

4. Sur l'écran **Installer un profil**, appuyez sur **Installer**, puis sur **Installer maintenant** sur la boîte de dialogue contextuelle de confirmation.
5. Si le dispositif mobile requiert un code, saisissez votre code sur l'écran **Entrer code** qui s'affiche, puis appuyez sur **Terminé**.

L'écran **Installation de profil** s'affiche.

6. Appuyez sur **Installer** sur l'écran **Avertissement** de confirmation.
Le processus d'installation de profil démarre. Une fois le processus terminé, l'écran **Profil installé** s'affiche.
 7. Sélectionnez **Terminé**.
-

Dispositifs mobiles Windows Phone

Vous pouvez inscrire les dispositifs mobiles Windows Phone à l'aide de l'adresse du serveur de communication local :



Remarque

Mobile Security ne prend pas en charge Windows Phone pour le serveur de communication du nuage.

Inscription sous Windows Phone 8.0

Procédure

1. Sur l'écran principal, cliquez sur l'icône **Paramètres**.
2. Cliquez sur applications de l'entreprise.
3. Sur l'écran **APPLICATIONS DE L'ENTREPRISE**, cliquez sur **ajouter un compte**, puis entrez les informations suivantes :
 - **Adresse e-mail** : l'adresse e-mail de votre société
 - **Mot de passe** : le mot de passe de votre compte de domaine ou la clé d'inscription
4. Cliquez sur **se connecter**.
5. Sur l'écran suivant, entrez les informations ci-dessous :
 - **Nom d'utilisateur** : si vous effectuez l'inscription à l'aide d'Active Directory, entrez le nom d'utilisateur de votre compte de domaine ; si vous utilisez une clé d'inscription, laissez ce champ vide.

- **Domaine** : si vous effectuez l'inscription à l'aide d'Active Directory, entrez le nom d'utilisateur de votre compte de domaine ; si vous utilisez une clé d'inscription, laissez ce champ vide.
- **Serveur** : <adresse_ip:port>/mobile.



Remarque

Remplacez <adresse_ip:port> par l'adresse IP et le numéro de port du serveur.

6. Cliquez sur **se connecter**.
 7. Si le message **Problème de certificat** apparaît, cliquez sur **continuer**.
 8. Si l'écran **Créer un mot de passe** apparaît, cliquez sur **définir**, puis entrez votre nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmez le mot de passe**, puis cliquez sur **terminé**.
 9. Sur l'écran **COMPTE AJOUTÉ**, cliquez sur **terminé**.
-

Inscription sous Windows Phone 8.1

Procédure

1. Sur l'écran principal, cliquez sur **Paramètres**.
 2. Cliquez sur **espace de travail**.
 3. Sur l'écran **espace de travail**, cliquez sur **ajouter un compte**, puis entrez votre adresse e-mail et cliquez sur **se connecter**.
 4. Sur l'écran suivant, entrez les informations ci-dessous dans le champ **Serveur** : <adresse_ip:port>/mobile, puis cliquez sur **se connecter**.
-



Remarque

Remplacez <adresse_ip:port> par l'adresse IP et le numéro de port du serveur.

5. Si le message **Problème de certificat** apparaît, cliquez sur **continuer**.
6. Sur l'écran suivant, entrez les informations ci-dessous :

- **Mot de passe** : le mot de passe de votre compte de domaine ou la clé d'inscription.
 - **Nom d'utilisateur** : si vous effectuez l'inscription à l'aide d'Active Directory, entrez le nom d'utilisateur de votre compte de domaine ; si vous utilisez une clé d'inscription, laissez ce champ vide.
 - **Domaine** : si vous effectuez l'inscription à l'aide d'Active Directory, entrez le nom d'utilisateur de votre compte de domaine ; si vous utilisez une clé d'inscription, laissez ce champ vide.
7. Cliquez sur **se connecter**.
 8. Si l'écran **Créer un mot de passe** apparaît, cliquez sur **définir**, puis entrez votre nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmez le mot de passe**, puis cliquez sur **terminé**.
 9. Sur l'écran **COMPTE AJOUTÉ**, cliquez sur **terminé**.
-

Annexe A

Configurations des ports de réseau


Cette annexe fournit toutes les configurations de ports de réseau dont vous avez besoin lors de l'installation ou de la configuration de Trend Micro Mobile Security.

Cette annexe contient les sections suivantes :


- *Configuration des ports de réseau pour le modèle de sécurité renforcée avec le serveur de communication du nuage à la page A-2*
- *Configuration des ports de réseau pour le modèle de sécurité renforcée avec serveur de communication local à la page A-5*
- *Configuration des ports de réseau pour le modèle de sécurité de base à la page A-10*

Configuration des ports de réseau pour le modèle de sécurité renforcée avec le serveur de communication du nuage

Si vous utilisez le modèle de sécurité renforcée (installation sur deux serveurs) avec le serveur de communication du nuage, configurez les ports de réseau suivants pour les composants Mobile Security :


COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
Serveur d'administration	<p>Ouvrez les ports suivants :</p> <ul style="list-style-type: none"> • Port HTTPS 443 pour les opérations suivantes : <ul style="list-style-type: none"> • Connexions entrantes sur le serveur Mobile Security. • Si vous souhaitez ajouter des applications externes à partir de Google Play. <p>Le nom d'hôte pour le magasin Google Play est : play.google.com.</p> <hr/> <p> Remarque</p> <p>C'est numéro de port HTTPS par défaut. Si vous voulez modifier le numéro de port HTTPS que vous souhaitez utiliser pour le serveur d'administration, voir Configuration des paramètres de serveur d'administration à la page 4-18 pour des détails.</p> • Port HTTPS 80, pour les opérations suivantes : <ul style="list-style-type: none"> • Serveur de licences <p>Le nom d'hôte du serveur de licences est : licenseupdate.trendmicro.com.</p> • Si vous utilisez le serveur Trend Micro ActiveUpdate comme source de mise à jour. <p>Le nom d'hôte du serveur ActiveUpdate est mobilesecurity.activeupdate.trendmicro.com.</p> <ul style="list-style-type: none"> • Si vous souhaitez tirer parti du service MARS (mobile application reputation service) de Trend Micro et afficher les informations de sécurité des fichiers APK téléchargés. <p>Le nom d'hôte du serveur MARS</p>	Utilisé pour accéder à la console Web d'administration Mobile Security.

COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
<p>Serveur d'administration</p>	<p>Ouvrez les ports suivants :</p> <ul style="list-style-type: none"> • Ports HTTP 80 et HTTPS 443 pour les opérations suivantes : • Connexions sortantes vers le Service de communication du nuage • Si vous souhaitez ajouter des applications iOS externes depuis App Store Apple <p>Le nom d'hôte pour l'App Store Apple est : itunes.apple.com.</p> <ul style="list-style-type: none"> • Si vous souhaitez utiliser le contrôle d'applications basé sur les catégories pour les dispositifs mobiles iOS <p>Ajoutez les deux hôtes suivants du Service de communication du nuage dans les exceptions de pare-feu :</p> <ul style="list-style-type: none"> • ccs01.trendmicro.com • ccs02.trendmicro.com 	<p>Utilisé pour accéder à la console Web d'administration Mobile Security.</p>
<p>Extension du protocole d'inscription du certificat simple (SCEP)</p>	<p>Ouvrez le port HTTP 80 pour le serveur de communication et les dispositifs mobiles iOS.</p>	<p>Utilisé pour l'inscription des dispositifs mobiles iOS.</p> <p>Si vous n'utilisez pas de serveur SCEP pour la gestion des dispositifs mobiles iOS, ce port n'est pas requis.</p>



COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
SQL Server	<p>Ouvrez les ports suivants :</p> <ul style="list-style-type: none"> • Port TCP 1433 pour le serveur Mobile Security. • Port UDP 1434 pour le serveur Mobile Security. <hr/> <p> Remarque</p> <p>Il s'agit du port TCP par défaut pour se connecter à SQL Server. Cependant, vous pouvez également utiliser un autre port pour SQL Server, si nécessaire.</p>	Établit une connexion entre le serveur Mobile Security et SQL Server à distance.
BlackBerry Enterprise Server (BES)	<p>Ouvrez les ports suivants :</p> <ul style="list-style-type: none"> • Ouvrez le port TCP 3101 pour l'infrastructure du protocole de routage du serveur (SRP) BES. • Ouvrez le port TCP 443 pour le serveur d'administration et l'outil de commande BES. 	Si vous n'utilisez pas Mobile Security pour la gestion des dispositifs mobiles BlackBerry, ces ports ne sont pas requis.


Configuration des ports de réseau pour le modèle de sécurité renforcée avec serveur de communication local

Si vous utilisez le modèle de sécurité renforcée (Installation sur deux serveurs) avec le serveur de communication local, configurez les ports de réseau suivants pour les composants Mobile Security :

COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
Serveur d'administration	<p>Ouvrez les ports suivants :</p> <ul style="list-style-type: none"> • Port HTTPS 443 pour les opérations suivantes : <ul style="list-style-type: none"> • Connexions entrantes sur le serveur Mobile Security. • Si vous souhaitez ajouter des applications externes à partir de Google Play. <p>Le nom d'hôte pour le magasin Google Play est : play.google.com.</p> <hr/> <p> Remarque</p> <p>C'est numéro de port HTTPS par défaut. Si vous voulez modifier le numéro de port HTTPS que vous souhaitez utiliser pour le serveur d'administration, voir Configuration des paramètres de serveur d'administration à la page 4-18 pour des détails.</p> • Port HTTPS 80, pour les opérations suivantes : <ul style="list-style-type: none"> • Serveur de licences <p>Le nom d'hôte du serveur de licences est : licenseupdate.trendmicro.com.</p> • Si vous utilisez le serveur Trend Micro ActiveUpdate comme source de mise à jour. <p>Le nom d'hôte du serveur ActiveUpdate est mobilesecurity.activeupdate.trendmicro.com.</p> • Si vous souhaitez tirer parti du service MARS (mobile application reputation service) de Trend Micro et afficher les informations de sécurité des fichiers APK téléchargés. <p>Le nom d'hôte du serveur MARS est : mars.trendmicro.com.</p> 	Utilisé pour accéder à la console Web d'administration Mobile Security.

COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
Serveur d'administration	<p>Ouvrez les ports suivants :</p> <ul style="list-style-type: none">• Ports HTTP 80 et HTTPS 443 pour les opérations suivantes :• Si vous souhaitez ajouter des applications iOS externes depuis App Store Apple <p>Le nom d'hôte pour l'App Store Apple est : itunes.apple.com.</p> <ul style="list-style-type: none">• Si vous souhaitez utiliser le contrôle d'applications basé sur les catégories pour les dispositifs mobiles iOS	Utilisé pour accéder à la console Web d'administration Mobile Security.


COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
Serveur de communication	<p>Ouvrez le port HTTP 8080.</p> <hr/>  Remarque Il s'agit du numéro de port HTTP par défaut pour la configuration sur deux serveurs. Si vous voulez modifier le numéro de port HTTP que vous souhaitez utiliser afin de permettre aux dispositifs mobiles de communiquer avec le serveur de communication durant l'installation, voir Configuration des paramètres courants du serveur de communication à la page 4-7 pour des détails.	Utilisé pour la communication entre les dispositifs mobiles et le serveur de communication.
	<p>Ouvrez le port HTTPS 4343.</p> <hr/>  Remarque Il s'agit du numéro de port HTTPS par défaut pour la configuration sur deux serveurs.	Utilisé pour la communication sécurisée entre les dispositifs mobiles et le serveur de communication.
	<p>Ouvrez le port TCP 2195 pour le serveur Apple Push Notification service (APNs). Le nom d'hôte Apple Push Notification Service est <code>gateway.push.apple.com</code>.</p>	<p>Permet au serveur APN d'Apple de gérer les dispositifs mobiles iOS.</p> <p>Si vous n'utilisez pas de serveur APN pour la gestion des dispositifs mobiles iOS, ce port n'est pas nécessaire.</p>
	<p>Ouvrez le port TCP 4343. Il s'agit du port par défaut pour permettre la connexion entrante sur le serveur de communication à partir du serveur d'administration. Si vous voulez modifier le numéro de port HTTP que vous souhaitez utiliser afin de permettre aux dispositifs mobiles de communiquer avec le serveur de communication durant l'installation, voir Configuration des paramètres courants du serveur de communication à la page 4-7 pour des détails.</p>	Établit une connexion entre le serveur d'administration et le serveur de stratégie.

COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
Active Directory	Ouvrez l'un des ports suivants : <ul style="list-style-type: none"> • Port TCP 389 (Contrôleur de domaine) pour le serveur d'administration • Port TCP 3268 (Catégorie globale) pour le serveur d'administration 	Utilisé pour l'authentification d'utilisateur à l'aide d'Active Directory. Si vous n'utilisez pas Active Directory pour l'authentification ou l'importation d'utilisateurs, ce port n'est pas requis.
Extension du protocole d'inscription du certificat simple (SCEP)	Ouvrez le port HTTP 80 pour le serveur de communication et les dispositifs mobiles iOS.	Utilisé pour l'inscription des dispositifs mobiles iOS. Si vous n'utilisez pas de serveur SCEP pour la gestion des dispositifs mobiles iOS, ce port n'est pas requis.
SQL Server	Ouvrez les ports suivants : <ul style="list-style-type: none"> • Port TCP 1433 pour le serveur d'administration • Port UDP 1434 pour le serveur d'administration <hr/>  Remarque Le port TCP 1433 est le port par défaut pour se connecter à SQL Server. Cependant, vous pouvez également utiliser un autre port TCP pour SQL Server, si nécessaire.	Établit une connexion entre le serveur de communication et le serveur d'administration avec SQL Server à distance.



COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
BlackBerry Enterprise Server (BES)	Ouvrez les ports suivants : <ul style="list-style-type: none">• Ouvrez le port TCP 3101 pour l'infrastructure du protocole de routage du serveur (SRP) BES.• Ouvrez le port TCP 443 pour le serveur d'administration et l'outil de commande BES.	Si vous n'utilisez pas Mobile Security pour la gestion des dispositifs mobiles BlackBerry, ces ports ne sont pas requis.


Configuration des ports de réseau pour le modèle de sécurité de base

Si vous utilisez le modèle de sécurité de base (Installation sur un serveur), configurez les ports de réseau suivants pour les composants Mobile Security :

COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
<p>Serveur d'administration et serveur de communication local</p>	<p>Ouvrez les ports suivants :</p> <ul style="list-style-type: none"> • Port HTTPS 443 pour les opérations suivantes : <ul style="list-style-type: none"> • Connexions entrantes sur le serveur Mobile Security. • Si vous souhaitez ajouter des applications externes à partir de Google Play. <p>Le nom d'hôte pour le magasin Google Play est : play.google.com.</p> <hr/> <p> Remarque</p> <p>C'est numéro de port HTTPS par défaut. Si vous voulez modifier le numéro de port HTTPS que vous souhaitez utiliser pour le serveur d'administration, voir Configuration des paramètres de serveur d'administration à la page 4-18 pour des détails.</p> • Port HTTPS 80, pour les opérations suivantes : <ul style="list-style-type: none"> • Serveur de licences <p>Le nom d'hôte du serveur de licences est : licenseupdate.trendmicro.com.</p> • Si vous utilisez le serveur Trend Micro ActiveUpdate comme source de mise à jour. <p>Le nom d'hôte du serveur ActiveUpdate est mobilesecurity.activeupdate.trendmicro.com.</p> • Si vous souhaitez tirer parti du service MARS (mobile application reputation service) de Trend Micro et afficher les informations de sécurité des fichiers APK téléchargés. <p>Le nom d'hôte du serveur MARS est : mars.trendmicro.com.</p> 	<p>Utilisateur pour l'accès à la console Web d'administration Mobile Security.</p>

COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
Serveur d'administration et serveur de communication local	<p>Ouvrez les ports suivants :</p> <ul style="list-style-type: none">• Ports HTTP 80 et HTTPS 443 pour les opérations suivantes :• Si vous souhaitez ajouter des applications iOS externes depuis App Store Apple <p>Le nom d'hôte pour l'App Store Apple est : itunes.apple.com.</p> <ul style="list-style-type: none">• Si vous souhaitez utiliser le contrôle d'applications basé sur les catégories pour les dispositifs mobiles iOS	Utilisateur pour l'accès à la console Web d'administration Mobile Security.

COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
Serveur d'administration et serveur de communication local	Ouvrez le port HTTP 8080. <hr/>  Remarque Il s'agit du numéro de port HTTP par défaut pour la configuration sur deux serveurs.	Utilisé pour la communication entre les dispositifs mobiles et le serveur Mobile Security.
	Ouvrez le port HTTPS 4343. <hr/>  Remarque Il s'agit du numéro de port HTTPS par défaut pour la configuration sur deux serveurs. Si vous voulez modifier le numéro de port HTTP que vous souhaitez utiliser afin de permettre aux dispositifs mobiles de communiquer avec le serveur de communication durant l'installation, voir Configuration des paramètres courants du serveur de communication à la page 4-7 pour des détails.	Utilisé pour une communication sécurisée entre les dispositifs mobiles et le serveur Mobile Security.
	Ouvrez le port TCP 2195 pour le serveur Apple Push Notification service (APNs). Le nom d'hôte Apple Push Notification Service est <code>gateway.push.apple.com</code> .	Permet au serveur APN d'Apple de gérer les dispositifs mobiles iOS. Si vous ne gérez pas de dispositifs mobiles iOS, ce port n'est pas requis.

COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
Active Directory	<p>Ouvrez l'un des ports suivants :</p> <ul style="list-style-type: none"> • Port TCP 389 (Contrôleur de domaine) pour le serveur d'administration • Port TCP 3268 (Catégorie globale) pour le serveur d'administration 	<p>Utilisé pour l'authentification d'utilisateur à l'aide d'Active Directory.</p> <p>Si vous n'utilisez pas Active Directory pour l'authentification ou l'importation d'utilisateurs, ce port n'est pas requis.</p>
Extension du protocole d'inscription du certificat simple (SCEP)	<p>Ouvrez le port HTTP 80 pour le serveur de communication et les dispositifs mobiles iOS.</p>	<p>Utilisé pour l'inscription des dispositifs mobiles iOS.</p> <p>Si vous n'utilisez pas de serveur SCEP pour la gestion des dispositifs mobiles iOS, ce port n'est pas requis.</p>
SQL Server	<p>Ouvrez les ports suivants :</p> <ul style="list-style-type: none"> • Port TCP 1433 pour le serveur Mobile Security. • Port UDP 1434 pour le serveur Mobile Security. <hr/> <p> Remarque</p> <p>Il s'agit du port TCP par défaut pour se connecter à SQL Server. Cependant, vous pouvez également utiliser un autre port pour SQL Server, si nécessaire.</p> <hr/>	<p>Établit une connexion entre le serveur Mobile Security et SQL Server à distance.</p>

COMPOSANT	PORTS DE RÉSEAU	DÉTAILS
BlackBerry Enterprise Server (BES)	Ouvrez les ports suivants : <ul style="list-style-type: none"><li data-bbox="504 300 866 381">• Ouvrez le port TCP 3101 pour l'infrastructure du protocole de routage du serveur (SRP) BES.<li data-bbox="504 397 907 479">• Ouvrez le port TCP 443 pour le serveur d'administration et l'outil de commande BES.	Si vous n'utilisez pas Mobile Security pour la gestion des dispositifs mobiles BlackBerry, ces ports ne sont pas requis.

Annexe B

Configurations facultatives

Cette annexe fournit les procédures de configurations facultatives que vous pouvez effectuer au cours de l'installation de Trend Micro Mobile Security.

Cette annexe contient les sections suivantes :

- *Utilisation de l'authentification Windows pour SQL Server à la page B-2*
- *Configuration des ports du serveur de communication à la page B-5*
- *Augmentation de l'extensibilité du serveur à la page B-6*
- *Configuration de SCEP à la page B-7*

Utilisation de l'authentification Windows pour SQL Server

Trend Micro recommande l'utilisation de la méthode d'authentification SQL Server au lieu de l'authentification Windows. Cependant, vous pouvez également configurer l'authentification Windows pour SQL Server.

Procédure

1. Créer un compte utilisateur dans le serveur Active Directory avec les droits d'accès à la base de données de Mobile Security. Vous pouvez sauter cette étape si vous disposez déjà d'un compte utilisateur avec les droits d'accès requis.
 - a. Créer un compte utilisateur sur le serveur Active Directory.
 - b. Démarrez SQL Server Management Studio et connectez-vous à la base de données de Mobile Security.
 - c. Développez le dossier `Security` dans l'arborescence de l'Explorateur d'objets.
 - d. Effectuez un clic droit sur **Connexions** puis cliquez sur **Nouvelles connexions**.
 - e. Cliquez sur **Général** depuis **Sélectionnez une page** sur la gauche, puis procédez comme suit :
 - i. Tapez le nom d'utilisateur que vous avez créé dans *l'étape a à la page B-2* de cette procédure dans le champ **Nom de connexion** et cliquez sur **Rechercher**.

La boîte de dialogue Sélectionner un utilisateur ou un groupe apparaît.
 - ii. Saisissez le nom d'utilisateur avec le nom de domaine (par exemple : `domainenom\nom d'utilisateur`) dans le champ **Saisir le nom de l'objet à sélectionner** puis cliquez sur **Vérifier les noms**.
 - iii. Sélectionnez **OK**.

- f. Sélectionnez **Rôles du serveur** depuis **Sélectionner une page** sur la gauche, puis sélectionnez les rôles suivants :
 - public
 - Administrateur système
- g. Sélectionnez **OK**.

Le compte d'utilisateur apparaît dans le dossier `Logins` sur l'**Explorateur d'objets**.

2. Ajoutez le serveur d'administration Mobile Security dans le même domaine que le serveur Active Directory.
3. Sur le serveur d'administration, accédez à **Démarrer > Outils d'administration > Gestion de l'ordinateur** et procédez ainsi :
 - a. Développez les dossiers des utilisateurs locaux et des groupes de l'arborescence de gauche, puis double-cliquez sur **Groupes**.
 - b. Effectuez un clic droit sur **Administrateurs** et cliquez sur **Propriétés**.
 - c. Cliquez sur le bouton **Ajouter** sur l'onglet **Général**, et procédez ainsi :
 - i. Tapez le nom d'utilisateur que vous avez créé dans *l'étape a à la page B-2* de cette procédure dans le champ **Nom de connexion** et cliquez sur **Rechercher**.

La boîte de dialogue Sélectionner Utilisateurs, Ordinateurs, Services ou Groupe apparaît.
 - ii. Saisissez le nom d'utilisateur avec le nom de domaine (par exemple : `domainenom\nom d'utilisateur`) dans le champ **Saisir le nom de l'objet à sélectionner** et cliquez sur **Vérifier les noms**.
 - iii. Sélectionnez **OK**.
 - d. Cliquez sur **OK** dans la boîte de dialogue **Propriétés administrateur**.
4. Sur le serveur d'administration, rendez-vous à l'emplacement suivant :
`C:\Program Files\Trend Micro\ Mobile Security\`

ou

C:\Program Files(x86)\Trend Micro \Mobile Security\)

5. Ouvrir TmDatabase.ini dans un éditeur de texte. Si le fichier TmDatabase.ini n'existe pas, créez un fichier en utilisant l'éditeur de texte et nommez-le TmDatabase.ini.
6. Ajoutez le texte suivant dans le fichier TmDatabase.ini :

```
ConnectionStringFormat=Provider=sqloledb;Data Source=
%server%;Initial Catalog=%database%;Integrated
Security=SSPI;
```

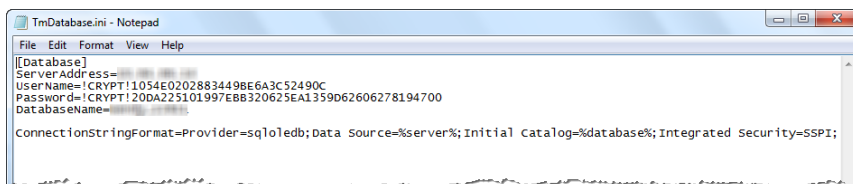


FIGURE B-1. fichier TmDatabase.ini

7. Sur le serveur d'administration, ouvrez les Services Windows, et double-cliquez sur **Service de module de gestion de Mobile Security**.
8. Sur l'onglet **Se connecter**, sélectionnez **Ce compte** : et saisissez le nom du compte qui aura accès à la base de données, ainsi que son mot de passe dans les champs **Mot de passe** et **Confirmer le mot de passe**, puis cliquez sur **OK**.
9. Effectuez un clic droit sur **Service de module de gestion de Mobile Security** dans la liste de services, puis cliquez sur **Redémarrer**.
10. Configurez les paramètres de la base de données sur la console Web d'administration :
 - a. Connectez-vous à la console Web d'administration.
 - b. Cliquez sur **Administration > Paramètres de base de données**.
 - c. Saisissez l'adresse IP du serveur de la base de données, le nom d'utilisateur, mot de passe et nom de la base de données.

- d. Cliquez sur **Enregistrer**.
-

Configuration des ports du serveur de communication

Trend Micro Mobile Security 9.0 SP2 vous permet de personnaliser les ports utilisés par le serveur de communication afin d'établir la connexion avec le serveur d'administration.

Procédure

1. Sur l'ordinateur où le serveur de communication est installé, ouvrez le fichier `configuration.xml` dans un éditeur de texte (situé dans `C:\Program Files\Trend Micro\Communication Server\` ou `C:\Program Files(x86)\Trend Micro\Communication Server\`)
 2. Modifiez les valeurs de `mdms_https_port` à votre numéro de port requis.
 3. Enregistrez puis fermez le fichier `configuration.xml`.
 4. Ouvrez les services Windows et cliquez avec le bouton droit sur **Service de communication Mobile Security**, puis cliquez sur **Redémarrer**.
 5. Connectez-vous à la console Web d'administration.
 6. Cliquez sur **Administration > Paramètres serveur de communication > Paramètres courants**.
 7. Sous la section **Paramètres pour la communication entre serveur de communication et le serveur d'administration**, donnez pour valeur du **Port HTTPS** le numéro de port que vous avez configuré dans *l'Étape 2 à la page B-5* de cette procédure.
 8. Cliquez sur **Enregistrer**.
-

Augmentation de l'extensibilité du serveur

En fonction de vos exigences, vous pouvez augmenter l'extensibilité du serveur et améliorer ses performances.

Procédure

1. Ouvrez le **Gestionnaire Internet Information Services (IIS)**, puis sélectionnez le serveur sur lequel vous souhaitez effectuer cette procédure.
2. Cliquez sur **Pools d'applications** dans le volet gauche, sélectionnez le pool d'applications dans lequel Mobile Security est installé à partir de la liste située dans le volet central, et cliquez sur **Paramètres avancés...** dans le volet de droite.

La boîte de dialogue **Paramètres avancés** apparaît.

3. Dans la boîte de dialogue **Paramètres avancés**, effectuez les modifications suivantes :
 - a. Modifiez la valeur du paramètre **Longueur de la file** pour **65535**.
 - b. Modifiez la valeur du paramètre **Processus de traitement maximum** pour **5** ou plus.
4. Après avoir effectué les modifications, cliquez sur **OK**, puis fermez le **Gestionnaire Internet Information Services (IIS)**.
5. Ouvrez l'invite de **commande** de Windows, puis effectuez les tâches suivantes :
 - a. Saisissez la commande suivante afin de modifier la valeur de la limite de demandes simultanées IIS à 100000 :

```
c:\windows\system32\inetsrv\appcmd.exe set config /  
section:serverRuntime /appConcurrentRequestLimit:100000
```

**Remarque**

Afin de vérifier cette modification, ouvrez le fichier `applicationHost.config` en saisissant la commande `%systemroot%\System32\inetsrv\config\applicationHost.config` dans l'invite de commande, puis vérifiez la valeur du paramètre **serverRuntime appConcurrentRequestLimit**, qui devrait être 100000.

- b. Saisissez la commande suivante afin de modifier la valeur de la limite de demandes simultanées IIS à 100000 dans le registre Windows :

```
reg add HKLM\System\CurrentControlSet\Services\HTTP  
\Parameters /v MaxConnections /t REG_DWORD /d 100000
```

Configuration de SCEP

La configuration de l'Extension du protocole d'inscription du certificat simple (SCEP) offre une sécurité supplémentaire aux dispositifs mobiles iOS.

Voir la section *Configuration de l'environnement pour les dispositifs mobiles iOS (Facultatif)* à la page 2-4.

Procédure

1. Installez l'autorité de certification

Pour la procédure d'installation détaillée de l'autorité de certification, consultez l'URL suivante :

<http://msdn.microsoft.com/en-us/library/ff720354.aspx>

**Remarque**

Si vous ne souhaitez pas utiliser SCEP, il n'est pas nécessaire d'installer l'autorité de certification.

2. Configurez l'Extension du protocole d'inscription du certificat simple (SCEP)

Si vous avez installé SCEP sur Windows Server 2008, installez le Service d'inscription de périphérique réseau pour Windows Server. Consultez l'URL suivante pour la procédure d'installation et de déploiement du Service d'inscription de périphérique réseau :

<http://esupport.trendmicro.com/solution/en-us/1060187.aspx>

ou

[http://technet.microsoft.com/en-us/library/ff955646\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff955646(WS.10).aspx)



Remarque

Si vous souhaitez utiliser SCEP, Trend Micro vous recommande de l'utiliser sur Windows Server 2008.

Si vous avez installé SCEP sur Windows Server 2003, installez le composant additionnel SCEP pour les services de certificats. Allez sur l'URL suivante pour télécharger le composant additionnel SCEP pour les Services de certificats :

<http://esupport.trendmicro.com/solution/en-us/1060258.aspx>

ou

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9F306763-D036-41D8-8860-1636411B2D01&displaylang=e&displaylang=en>

3. Vérifiez les horloges système

Assurez-vous que l'heure des horloges système du serveur SCEP, du serveur de communication et du serveur d'administration est correcte.

4. Modifiez les propriétés du module de stratégie pour l'autorité de certification :

- a. Sur l'ordinateur sur lequel l'autorité de certification est installée, ouvrez la console de gestion de l'**autorité de certification**.
- b. Cliquez sur l'onglet **Module de stratégie**, puis cliquez sur **Propriétés**.
- c. Sélectionnez **Respectez les paramètres dans le modèle de certificat, le cas échéant. Sinon, émettez le certificat automatiquement**.
- d. Sélectionnez **OK**.

5. Appliquez l'ensemble des règles suivantes :
 - Les dispositifs mobiles iOS doivent pouvoir se connecter au serveur de communication.
 - Le serveur de communication doit pouvoir se connecter au serveur SCEP.
 - Les dispositifs mobiles iOS doivent pouvoir se connecter directement au serveur SCEP lors de l'inscription au serveur Mobile Security.
6. Vérifiez l'installation SCEP (facultatif) :
 - Pour SCEP s'exécutant sous Windows Server 2008, accédez à l'URL suivante à partir du serveur de communication :
http://SCEPServerIP/certsrv/mscep_admin

**Remarque**

Remplacez *SCEPServerIP* par l'adresse IP réelle du serveur SCEP dans l'URL.

- Pour SCEP s'exécutant sous Windows Server 2003, accédez à l'URL suivante à partir du serveur de communication :
<http://SCEPServerIP/certsrv/mscep>

**Remarque**

Remplacez *SCEPServerIP* par l'adresse IP réelle du serveur SCEP dans l'URL.

Si vous voyez la page Web similaire à la suivante, votre serveur est configuré correctement :

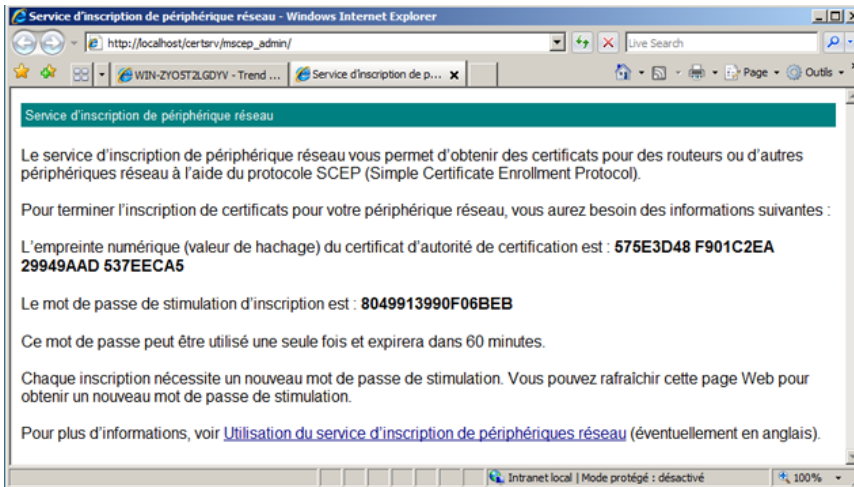


FIGURE B-2. Vérification de la configuration



Remarque

Lorsqu'un dispositif mobile iOS est inscrit, il peut accéder à l'URL suivante :

<http://SCEPserverIP/certsrv/mscep>

Le dispositif mobile iOS ne doit se connecter au serveur SCEP que pour l'inscription et n'a besoin de cette connexion pour aucune utilisation ultérieure.

Annexe C

Génération et configuration d'un certificat APNs (Apple Push Notification service)

Trend Micro Mobile Security requiert la gestion des dispositifs mobiles iOS par le certificat APNs (Apple Push Notification service). Cette annexe introduit la procédure détaillée de génération du certificat APNs (Apple Push Notification service) et de son téléchargement vers le serveur Mobile Security.

Pour d'autres conditions d'installation, voir *Configuration de l'environnement pour les dispositifs mobiles iOS (Facultatif)* à la page 2-4.

Cette annexe contient les sections suivantes :

- *Introduction au certificat APNs à la page C-3*
- *Génération d'un certificat APNs (Apple Push Notification service) à la page C-3*
- *Génération d'un certificat APNs (Apple Push Notification service) à partir d'un Windows Server à la page C-5*
- *Génération d'un certificat APNs (Apple Push Notification service) à partir d'un poste de travail Mac à la page C-20*
- *Téléchargement du certificat APNs (Apple Push Notification service) vers le serveur Mobile Security à la page C-26*

- *Génération et configuration d'un certificat APNs dans Windows Server 2003 à l'aide d'IIS 6.0 à la page C-28*

Introduction au certificat APNs

Le service Apple Push Notification (APNs) permet au serveur Trend Micro Mobile Security for Enterprise de communiquer de manière sécurisée et sans fil (over-the-air, OTA) avec vos dispositifs. Chaque entreprise doit avoir son propre certificat APNs (Apple Push Notification service) afin de garantir un mécanisme sécurisé qui permet à ses dispositifs de communiquer à travers le réseau Apple Push Notification.

Trend Micro Mobile Security for Enterprise se sert de votre certificat APNs pour gérer vos dispositifs iOS ou pour envoyer des notifications à vos dispositifs lorsque l'administrateur requiert des informations ou gère vos dispositifs iOS. Seule la notification est envoyée par le biais du serveur APNs.

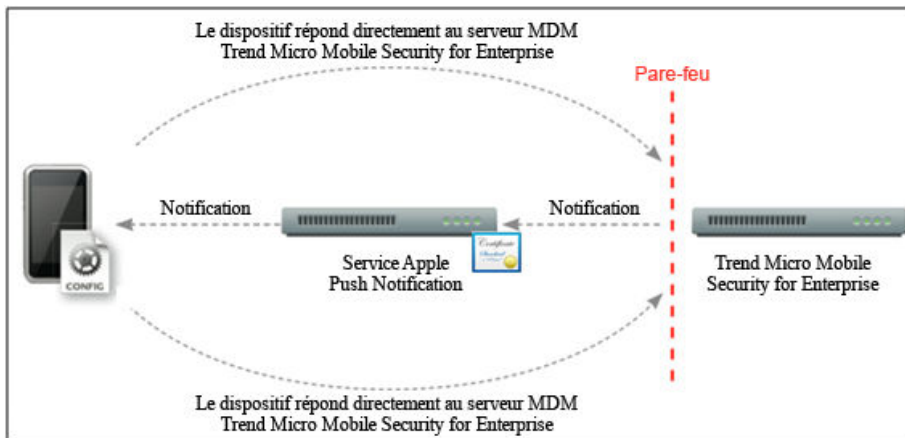


FIGURE C-1. Processus de notification

Génération d'un certificat APNs (Apple Push Notification service)

Cette section explique le processus de génération d'un certificat APNs (Apple Push Notification Service) pour la gestion des dispositifs mobiles iOS.

Procédure

1. Générer une demande de signature de certificat (CSR) à partir d'un serveur Windows ou d'un poste de travail Mac.
2. Faites en sorte que Trend Micro ou Apple signe la CSR.
 - **Utilisation du certificat signé par Trend Micro** : Trend Micro fournit un procédé simple pour signer votre CSR :

- a. Accédez au portail de signature de certificat APNs (Apple Push Notification service) de Trend Micro et fournissez les informations relatives à votre entreprise, votre code d'activation de produit et une copie de votre CSR :

http://forms.trendmicro.com/download_trials/csr/?dom=us

Une fois que la demande est présentée au portail, un courriel incluant la CSR signée vous sera envoyé.

- b. À l'aide d'un identifiant Apple vérifié, téléchargez la CSR signée sur le portail des certificats APNs (Apple Push Notification service).

Apple créera un certificat APNs (Apple Push Notification service).

- **Utilisation du certificat signé par Apple** : Si vous souhaitez utiliser le certificat signé par Apple, assurez-vous que vous disposez des éléments suivants avant de poursuivre :
 - Un compte développeur d'entreprise Apple existant (<http://developer.apple.com/programs/ios/enterprise>)
 - Le rôle assigné à votre compte développeur est celui d'Agent (un rôle d'administrateur ne serait pas valide)
 - Les autorisations d'administrateur sur votre serveur Windows ou poste de travail Mac OS X

Pour utiliser le certificat signé par Apple, voir *Utilisation du certificat signé par Apple à la page C-12* pour Windows ou *Utilisation du certificat signé par Apple à la page C-22* pour Mac.

3. Installez votre Certificat APNs (Apple Push Notification service) sur votre serveur Windows ou sur le poste de travail Mac, puis exportez le certificat afin de l'enregistrer sur votre ordinateur.

Une fois que vous avez exporté le certificat, poursuivez en téléchargeant ce certificat sur le serveur Trend Micro Mobile Security.

Génération d'un certificat APNs (Apple Push Notification service) à partir d'un Windows Server

Les étapes suivantes vous guideront pour générer un certificat APNs (Apple Push Notification service) à partir d'un Windows Server. Si vous avez déjà généré votre certificat à partir d'un poste de travail Mac OS X, vous pouvez ignorer cette section et télécharger votre certificat vers le serveur MDM Trend Micro Mobile Security for Enterprise.

Étape 1 : Génération d'une demande de signature d'un certificat (Certificate Signing Request, CSR)

Procédure

1. Accédez à **Démarrer>Outils d'administrationGestionnaire Internet Information Services (IIS)**, et sélectionnez le nom du serveur.
2. Double-cliquez sur l'icône **Certificats de serveur**.

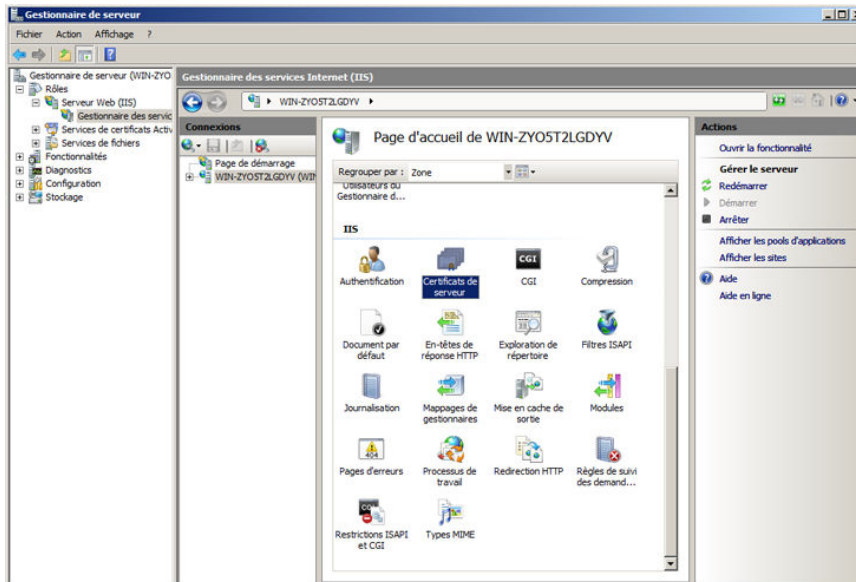


FIGURE C-2. Accès aux certificats de serveur



Remarque

L'IIS version 7.0 est utilisée pour configurer le certificat APNs (Apple Push Notification service) dans ce document.

3. Dans le volet **Actions** sur la droite, cliquez sur **Créer une demande de certificat**.

L'assistant de **demande de certificat** apparaît.

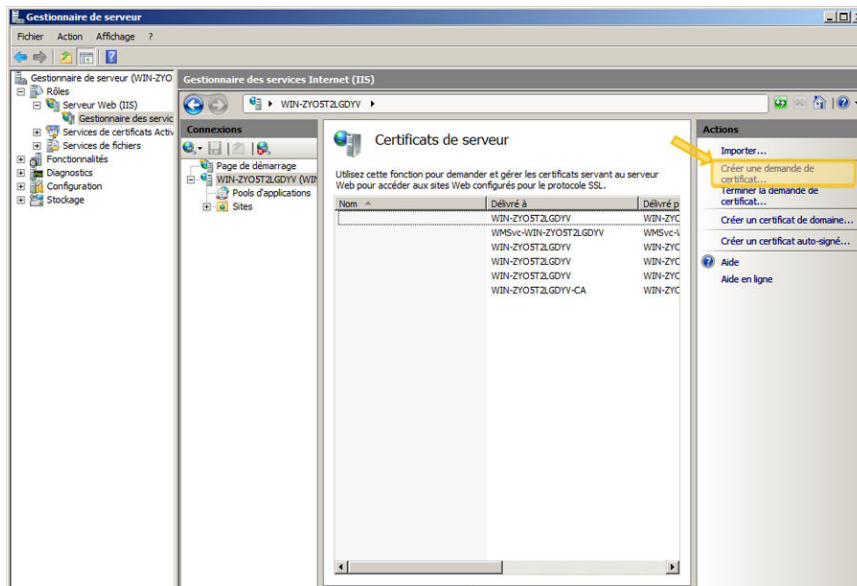


FIGURE C-3. Démarrage de l'assistant de demande de certificat

4. Dans la fenêtre de **Propriétés du nom unique**, saisissez les informations suivantes :
 - **Nom commun**—le nom associé à votre compte développeur Apple
 - **Organisation**—le nom légalement enregistré de votre organisation/société
 - **Unité d'organisation**—le nom de votre service au sein de l'organisation
 - **Ville/localité**—la ville dans laquelle votre organisation est située
 - **Département/région**—le département dans lequel votre organisation est située

- **Pays/région**—le pays ou la région dans lequel/laquelle votre organisation est située

Demande de certificat ? X

Propriétés du nom unique

Indiquez les informations requises pour le certificat. Lorsque vous entrez le département ou région et la ville/localité, utilisez des noms complets et officiels, et n'employez aucune abréviation.

Nom commun :

Organisation :

Unité d'organisation :

Ville/localité :

Département/région :

Pays/région :

Précédent Suivant Terminer Annuler

FIGURE C-4. Écran de Propriétés du nom unique

5. Cliquez sur **Suivant**.

La fenêtre de Propriétés du fournisseur de services de chiffrement apparaît.

6. Sélectionnez **Fournisseur de services de chiffrement Microsoft RSA SChannel** dans le champ **Fournisseur de services de chiffrement** et **2048** dans le champ **Longueur en bits**, puis cliquez sur **Suivant**.

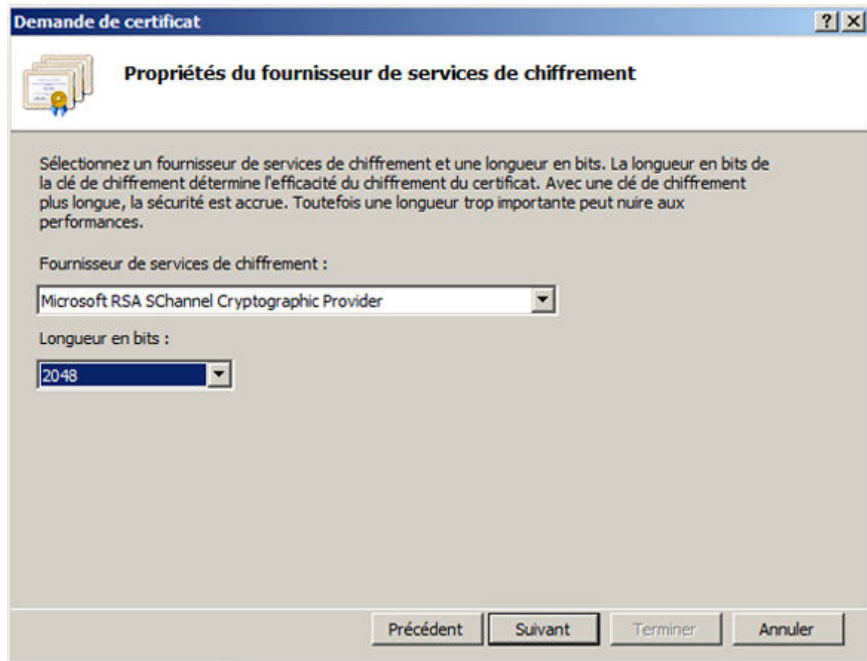


FIGURE C-5. Écran de Propriétés du fournisseur de services de chiffrement

7. Sélectionnez un emplacement dans lequel vous souhaitez enregistrer le fichier de demande de certificat.

Assurez-vous de mémoriser le nom du fichier et l'emplacement dans lequel vous l'enregistrez.

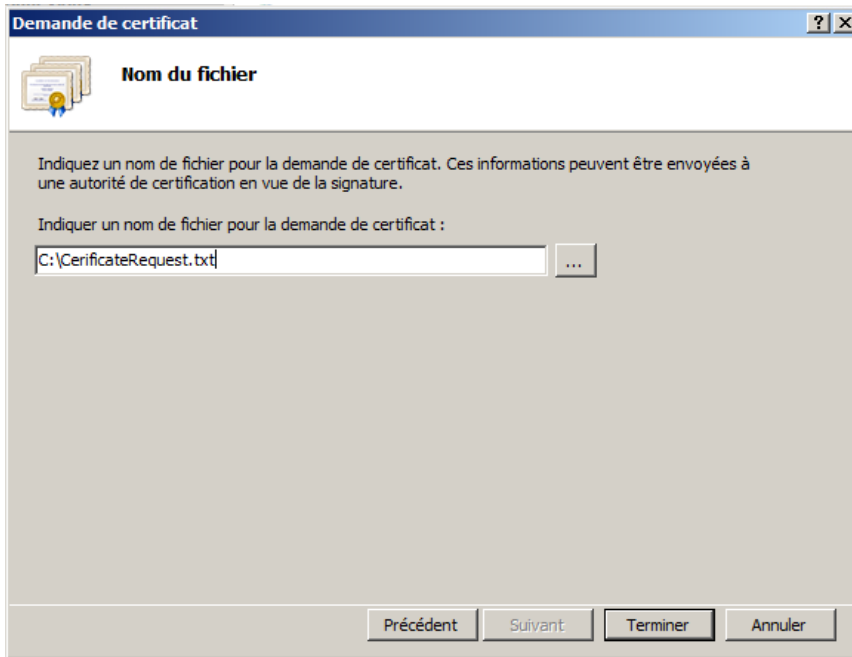


FIGURE C-6. Écran Nom du fichier

8. Cliquez sur **Terminer**.

Vous avez créé une CSR et vous pouvez désormais la télécharger vers votre portail de développement Apple.



Important

Trend Micro vous recommande d'enregistrer le fichier CSR que vous venez de créer dans un endroit sûr. Vous en aurez besoin lorsque vous renouvelerez votre certificat APNs ultérieurement. L'utilisation d'un autre certificat APNs vous obligerait à inscrire à nouveau tous les dispositifs mobiles iOS sur le serveur Mobile Security. Consultez [Renouvellement d'un certificat APNs à la page C-29](#) pour plus de renseignements.

Étape 2 : Téléchargement de la CRS et Génération du certificat APN (Apple Push Notification service)

Une fois la CSR générée, vous pouvez effectuer l'une des actions suivantes :

- Télécharger la CSR sur le Portail de signature de certificats Trend Micro afin de la faire signer par Trend Micro, puis l'utiliser pour générer le certificat APN (Apple Push Notification service).
- Télécharger la CSR vers le portail de développement Apple afin de la faire signer par Apple, puis l'utiliser pour générer un certificat APNs (Apple Push Notification service).



Remarque

La procédure suivante considère que vous disposez du certificat APNs (Apple Push Notification service) signé par Trend Micro.

Si vous souhaitez utiliser le certificat APNs (Apple Push Notification service) signé par Apple, sautez cette procédure et consultez *Utilisation du certificat signé par Apple à la page C-12* pour Windows ou *Utilisation du certificat signé par Apple à la page C-22* pour Mac.

Procédure

1. Sur un navigateur Web, naviguez jusqu'à l'URL suivante :
http://forms.trendmicro.com/download_trials/csr/?dom=us
2. Remplissez les champs appropriés et téléchargez la CSR que vous venez de créer, puis cliquez sur **Procéder**.

Trend Micro signera et vous renverra votre certificat signé.
3. Téléchargez le certificat signé depuis le portail de Trend Micro ou à partir du courriel que vous avez reçu.
4. Téléchargez la CSR sur le portail de certificats Apple Push :
 - a. Ouvrez le navigateur Web et atteignez l'URL :
<https://identity.apple.com/pushcert/>

- b. Ouvrez votre session à l'aide de votre identifiant et mot de passe Apple.
La page **Mise en route** s'affiche.
 - c. Cliquez sur le bouton **Créer un certificat**.
L'écran **Conditions d'utilisation** s'affiche.
 - d. Cliquez sur **Accepter** pour accepter les conditions.
L'écran Créer un nouveau certificat Push s'affiche.
 - e. Cliquez sur **Parcourir**, sélectionnez le fichier signé au préalable par Trend Micro, puis cliquez sur **Télécharger**. Patientez jusqu'à ce que le portail génère le fichier (.pem) du certificat APNs (Apple Push Notification service).
 - f. Cliquez sur **Télécharger** pour enregistrer le fichier .pem sur votre ordinateur, puis passez à *Étape 3 : Installation de votre certificat APNs (Apple Push Notification service) à la page C-14* pour Windows.
-

Utilisation du certificat signé par Apple



Remarque

Sautez cette procédure si vous possédez déjà le certificat APNs (Apple Push Notification service) signé par Trend Micro.

Procédure

1. Sur le navigateur Web, naviguez jusqu'à l'URL suivante :
<https://developer.apple.com/>
2. Cliquez sur le lien **Espace membre**.
3. Ouvrez votre session à l'aide de votre identifiant et mot de passe Apple.
4. Cliquez sur **Portail de mise en service iOS**.

**Remarque**

Si le portail de mise en service iOS n'apparaît pas, votre compte de développement n'a pas été paramétré pour le développement iOS.

5. Dans le volet gauche, cliquez sur **ID d'application**, puis cliquez sur **Nouvel ID d'application**.
 6. Remplissez les champs appropriés. Le champ de **notation de l'identifiant de l'offre groupée (Suffixe de l'identifiant d'application)** doit être configuré comme suit : `com.apple.mgmt.mycompany.tmms`
-

**Remarque**

Remplacez **mycompany** par le nom de votre société.

**Remarque**

Notez la valeur de **notation de l'identifiant de l'offre groupée (Suffixe de l'identifiant d'application)**. Vous aurez besoin de cette valeur lors de la configuration du serveur Mobile Security.

7. Cliquez sur **Soumettre**.
L'**ID d'application** que vous venez d'ajouter apparaît dans la liste.
 8. Cliquez sur **Configurer**.
-

**Conseil**

Si vous ne pouvez pas voir ni cliquer sur **Configurer**, vérifiez que vous êtes bien connecté avec le rôle d'Agent.

9. Sélectionnez **Activer Apple Push Notification service**, puis cliquez sur **Configurer** pour créer un certificat SSL Production Push.
-

**Conseil**

Si vous ne pouvez pas sélectionner **Activer Apple Push Notification service**, essayez d'utiliser le navigateur Web Safari ou Firefox, et vérifiez que vous êtes bien connecté avec le rôle d'Agent.

10. L'Assistant de certification SSL apparaît et vous demande de créer une demande de signature d'un certificat (que vous avez déjà créée à l'*Étape 1 : Génération d'une demande de signature d'un certificat (Certificate Signing Request, CSR) à la page C-20*). Cliquez sur **Continuer**.
11. Cliquez sur **Choisir un fichier** et téléchargez la demande de signature d'un certificat que vous avez créée à l'*Étape 1 : Génération d'une demande de signature d'un certificat (Certificate Signing Request, CSR) à la page C-20*. (Par exemple, CertificateSigningRequest.certSigningRequest2).
12. Cliquez sur **Générer**.

Une fois terminé, l'écran apparaît et vous confirme que votre certificat SSL APNs (Apple Push Notification service) a été généré.

13. Cliquez sur **Continuer**.

L'écran **Télécharger et installer votre certificat SSL APNs (Apple Push Notification service)** s'affiche.

14. Cliquez sur **Télécharger** pour enregistrer le fichier `.cer` sur votre ordinateur, puis passez à l'*Étape 3 : Installation de votre certificat APNs (Apple Push Notification service) à la page C-14* pour Windows.



Remarque

Pour installer le certificat APNs (Apple Push Notification service) sur un ordinateur sous Windows, vous devez changer manuellement l'extension, de `.pem` à `.cer`.

Étape 3 : Installation de votre certificat APNs (Apple Push Notification service)

Procédure

1. Accédez à **Démarrer > Outils d'administration > Gestionnaire Internet Information Services (IIS)**, sélectionnez le nom du serveur et double-cliquez sur **Certificats de serveur**.

2. Dans le volet **Actions** sur la droite, cliquez sur **Terminer la demande de certificat**.

L'assistant de complétion de demande de certificat apparaît.

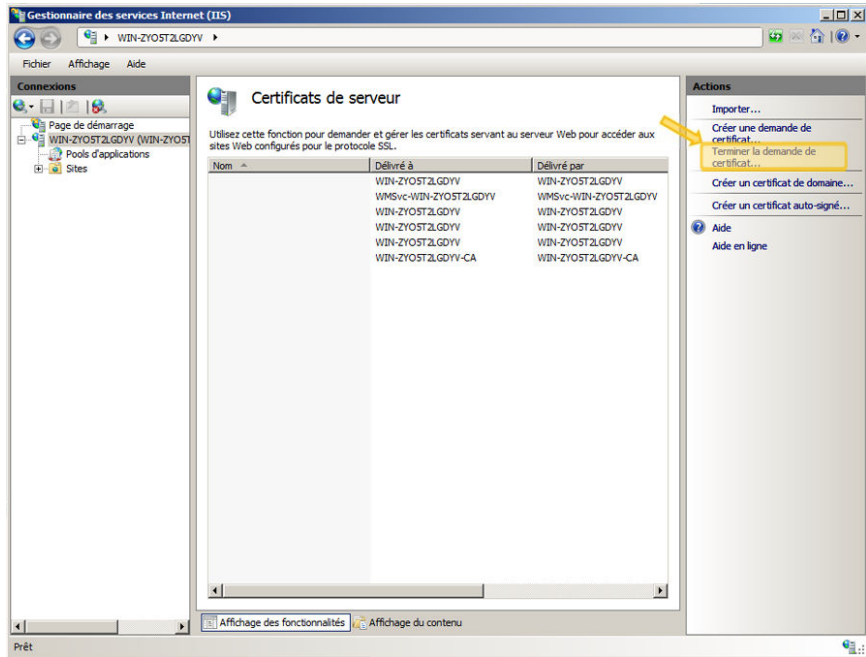


FIGURE C-7. Complétion de demande de certificat



Remarque

Si vous utilisez IIS 7.5, le fait de cliquer sur **Complétion de demande de certificat** peut faire apparaître le message d'erreur suivant :

Une chaîne de certificat n'a pas pu être créée dans une autorité racine approuvée.

Si cela se produit, consultez la section [Configuration de IIS 7.5 pour l'installation du certificat APNs \(Apple Push Notification service\) à la page C-19](#) pour voir la procédure à suivre pour résoudre ce problème.

3. Sélectionnez le fichier de certificat `.cer` que vous avez téléchargé à partir du portail développeur Apple et saisissez `APNs MDM Trend Micro Mobile Security for Enterprise` dans le champ **Nom convivial**.



Remarque

Si vous avez généré le fichier de certificat à partir du poste de travail Mac, vous devez changer manuellement l'extension du fichier de `.pem` à `.cer`.

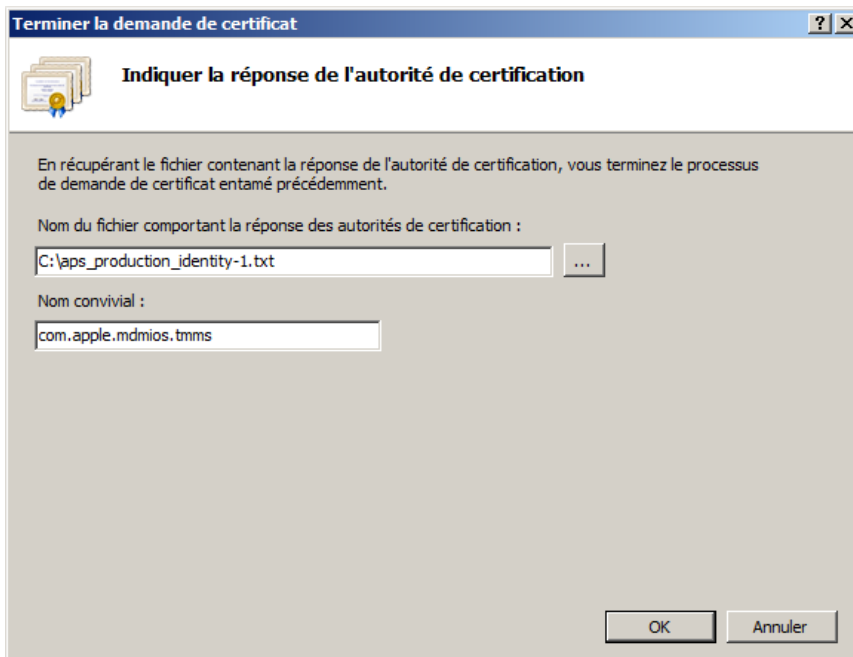


FIGURE C-8. Écran Indiquer la réponse de l'autorité de certification



Conseil

Le nom convivial ne fait pas partie du certificat, mais il est utilisé par l'administrateur du serveur afin d'identifier facilement le certificat.

4. Sélectionnez **OK**.

Le certificat sera installé sur le serveur.

5. Vérifiez que votre certificat Apple Production Push Services apparaît dans la liste de **Certificats de serveur**. Si vous voyez le certificat, suivez les étapes suivantes afin de l'exporter et de le télécharger vers le serveur MDM Trend Micro Mobile Security for Enterprise.
6. Cliquez avec le bouton droit sur la liste de **Certificats de serveur**, puis cliquez sur **Exporter**.

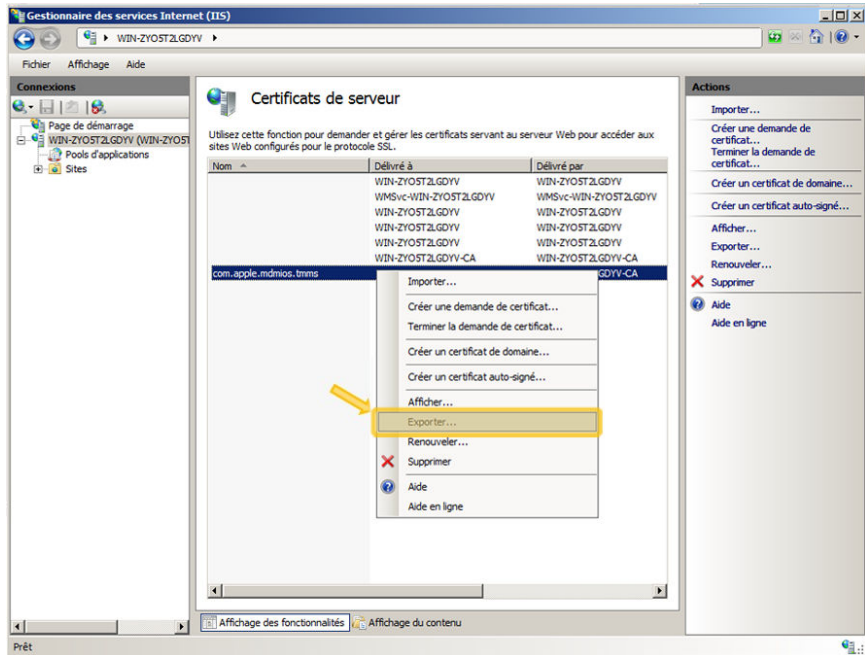


FIGURE C-9. Exporter le certificat

7. Sélectionnez l'emplacement dans lequel vous souhaitez enregistrer le fichier, choisissez un mot de passe pour l'exportation, puis cliquez sur **OK**.

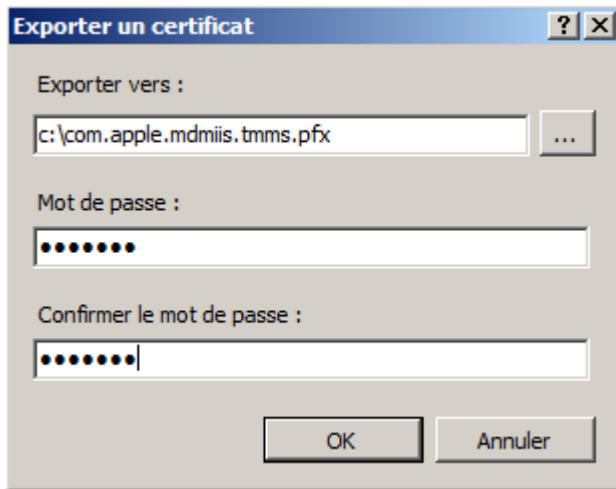


FIGURE C-10. Spécifier un mot de passe pour le certificat



Conseil

Si vous disposez uniquement de l'option enregistrer en tant que fichier `.cer` au lieu d'un `.pfx`, cela signifie que vous n'exportez pas le certificat correctement. Assurez-vous d'avoir sélectionné le bon fichier à exporter.



Remarque

Assurez-vous de mémoriser le mot de passe, ou conservez-le dans un endroit sûr. Le mot de passe sera demandé lors du téléchargement du certificat vers le serveur MDM Trend Micro Mobile Security for Enterprise.

Une fois toutes ces étapes terminées, vous devriez disposer des éléments suivants :

- Certificat APNs (Apple Push Notification service) (au format `.pfx`, et non `.cer`)
- Le mot de passe que vous avez défini lors de l'exportation du certificat

Vous pouvez désormais télécharger votre certificat vers le serveur Trend Micro Mobile Security. Voir *Téléchargement du certificat APNs (Apple Push Notification service) vers le serveur Mobile Security à la page C-26* pour la procédure.

Configuration de IIS 7.5 pour l'installation du certificat APNs (Apple Push Notification service)

Si vous utilisez IIS 7.5, le téléchargement du certificat vers IIS peut échouer, avec le message d'erreur suivant :

Une chaîne de certificat n'a pas pu être créée dans une autorité racine approuvée.

Cela peut se produire pour les raisons suivantes :

- Le certificat APNs (Apple Push Notification service) est signé par l'autorité de certification racine Apple au lieu d'une autorité de certification publique.
- La vérification renforcée pour l'autorité de certification racine approuvée par IIS 7.5.

Procédure

1. Télécharger le certificat **Racine Apple** et le certificat **Intégration d'application** à partir de l'URL :
<http://www.apple.com/certificateauthority/>
2. Double-cliquez sur le certificat **Racine Apple**, puis sur la fenêtre **Certificat**, cliquez sur **Installer le certificat**.
3. Sur l'écran de bienvenue, cliquez sur **Suivant**.
4. Sélectionnez **Placez tous les certificats dans la banque suivante** puis cliquez sur **Parcourir**.
5. Dans la fenêtre **Sélectionner la banque de certificats**, sélectionnez **Afficher les banques physiques**, puis cliquez sur **Autorité de certification racine approuvée** > **Ordinateur local** puis cliquez sur **OK**.
6. Cliquez sur **Suivant** sur l'écran **Assistant de l'import de certificat**, puis cliquez sur **Terminer**.
7. Répétez les *Étapes 2 à la page C-19 à 5 à la page C-19* pour le certificat **d'intégration d'applications**. Cependant, à *l'étape 4 à la page C-19*, sélectionnez **Autorités de**

certification intermédiaires > Ordinateur local au lieu de **Autorité de certification racine approuvée > Ordinateur local**.

Génération d'un certificat APNs (Apple Push Notification service) à partir d'un poste de travail Mac

La procédure suivante vous guidera pour la génération d'un certificat APNs (Apple Push Notification service) sur un poste de travail Mac OS X. Pour Windows Server, vous pouvez ignorer cette section, et aller directement à la section *Génération d'un certificat APNs (Apple Push Notification service) à partir d'un Windows Server à la page C-5*.

Étape 1 : Génération d'une demande de signature d'un certificat (Certificate Signing Request, CSR)

Procédure

1. Sur votre ordinateur Mac, allez sur **Applications > Utilitaires > Trousseau d'accès**.
2. Dans le volet gauche, sélectionnez Connexion dans la section **Trousseau**, puis sélectionnez **Certificats** dans la section **Catégorie**.
3. Dans la barre de menu supérieur, sélectionnez **Trousseau d'accès > Assistant de certification > Demander un certificat à une autorité de certification**.

L'**Assistant de certification** s'affiche.

4. Saisissez l'adresse électronique et le nom du compte développeur Apple enregistré dans les champs **Adresse électronique de l'utilisateur** et **Nom commun**, sélectionnez **Enregistré sur le disque** puis cliquez sur **Continuer**.
5. Sélectionnez l'emplacement dans lequel vous souhaitez enregistrer le fichier, puis cliquez sur **Enregistrer**.

Vous avez créé une CSR et vous pouvez désormais la télécharger vers votre portail de développement Apple.

**Important**

Trend Micro vous recommande d'enregistrer le fichier CSR que vous venez de créer dans un endroit sûr. Vous en aurez besoin lorsque vous renouvelerez votre certificat APNs ultérieurement. L'utilisation d'un autre certificat APNs vous obligerait à inscrire à nouveau tous les dispositifs mobiles iOS sur le serveur Mobile Security. Consultez [Renouvellement d'un certificat APNs à la page C-29](#) pour plus de renseignements.

Étape 2 : Téléchargement de la CRS et Génération du certificat APN (Apple Push Notification service)

Une fois la CSR générée, vous pouvez effectuer l'une des actions suivantes :

- Télécharger la CSR sur le Portail de signature de certificats Trend Micro afin de la faire signer par Trend Micro, puis l'utiliser pour générer le certificat APN (Apple Push Notification service).
- Télécharger la CSR vers le portail de développement Apple afin de la faire signer par Apple, puis l'utiliser pour générer un certificat APNs (Apple Push Notification service).

**Remarque**

La procédure suivante considère que vous disposez du certificat APNs (Apple Push Notification service) signé par Trend Micro.

Si vous souhaitez utiliser le certificat APNs (Apple Push Notification service) signé par Apple, sautez cette procédure et consultez [Utilisation du certificat signé par Apple à la page C-12](#) pour Windows ou [Utilisation du certificat signé par Apple à la page C-22](#) pour Mac.

Procédure

1. Sur un navigateur Web, naviguez jusqu'à l'URL suivante :
http://forms.trendmicro.com/download_trials/csr/?dom=us
2. Remplissez les champs appropriés et téléchargez la CSR que vous venez de créer, puis cliquez sur **Procéder**.

Trend Micro signera et vous renverra votre certificat signé.

3. Téléchargez le certificat signé depuis le portail de Trend Micro ou à partir du courriel que vous avez reçu.
 4. Téléchargez la CSR sur le portail de certificats Apple Push :
 - a. Ouvrez le navigateur Web et atteignez l'URL :
<https://identity.apple.com/pushcert/>
 - b. Ouvrez votre session à l'aide de votre identifiant et mot de passe Apple.
La page **Mise en route** s'affiche.
 - c. Cliquez sur le bouton **Créer un certificat**.
L'écran **Conditions d'utilisation** s'affiche.
 - d. Cliquez sur **Accepter** pour accepter les conditions.
L'écran Créer un nouveau certificat Push s'affiche.
 - e. Cliquez sur **Parcourir**, sélectionnez le fichier signé au préalable par Trend Micro, puis cliquez sur **Télécharger**. Patientez jusqu'à ce que le portail génère le fichier (.pem) du certificat APNs (Apple Push Notification service).
 - f. Cliquez sur **Télécharger** pour enregistrer le fichier .pem sur votre ordinateur, puis passez à *Étape 3 : Installation de votre certificat APNs (Apple Push Notification service) à la page C-25* pour Mac.
-

Utilisation du certificat signé par Apple



Remarque

Sautez cette procédure si vous possédez déjà le certificat APNs (Apple Push Notification service) signé par Trend Micro.

Procédure

1. Sur le navigateur Web, naviguez jusqu'à l'URL suivante :

<https://developer.apple.com/>

2. Cliquez sur le lien **Espace membre**.
3. Ouvrez votre session à l'aide de votre identifiant et mot de passe Apple.
4. Cliquez sur **Portail de mise en service iOS**.



Remarque

Si le portail de mise en service iOS n'apparaît pas, votre compte de développement n'a pas été paramétré pour le développement iOS.

5. Dans le volet gauche, cliquez sur **ID d'application**, puis cliquez sur **Nouvel ID d'application**.
6. Remplissez les champs appropriés. Le champ de **notation de l'identifiant de l'offre groupée (Suffixe de l'identifiant d'application)** doit être configuré comme suit : `com.apple.mgmt.mycompany.tmms`



Remarque

Remplacez **mycompany** par le nom de votre société.



Remarque

Notez la valeur de **notation de l'identifiant de l'offre groupée (Suffixe de l'identifiant d'application)**. Vous aurez besoin de cette valeur lors de la configuration du serveur Mobile Security.

7. Cliquez sur **Soumettre**.
L'**ID d'application** que vous venez d'ajouter apparaît dans la liste.
8. Cliquez sur **Configurer**.



Conseil

Si vous ne pouvez pas voir ni cliquer sur **Configurer**, vérifiez que vous êtes bien connecté avec le rôle d'Agent.

9. Sélectionnez **Activer Apple Push Notification service**, puis cliquez sur **Configurer** pour créer un certificat SSL Production Push.



Conseil

Si vous ne pouvez pas sélectionner **Activer Apple Push Notification service**, essayez d'utiliser le navigateur Web Safari ou Firefox, et vérifiez que vous êtes bien connecté avec le rôle d'Agent.

10. L'Assistant de certification SSL apparaît et vous demande de créer une demande de signature d'un certificat (que vous avez déjà créée à l'*Étape 1 : Génération d'une demande de signature d'un certificat (Certificate Signing Request, CSR) à la page C-20*). Cliquez sur **Continuer**.
 11. Cliquez sur **Choisir un fichier** et téléchargez la demande de signature d'un certificat que vous avez créée à l'*Étape 1 : Génération d'une demande de signature d'un certificat (Certificate Signing Request, CSR) à la page C-20*. (Par exemple, CertificateSigningRequest.certSigningRequest2).
 12. Cliquez sur **Générer**.

Une fois terminé, l'écran apparaît et vous confirme que votre certificat SSL APNs (Apple Push Notification service) a été généré.
 13. Cliquez sur **Continuer**.

L'écran **Télécharger et installer votre certificat SSL APNs (Apple Push Notification service)** s'affiche.
 14. Cliquez sur **Télécharger** pour enregistrer le fichier .cer sur votre ordinateur, puis passez à l'*Étape 3 : Installation de votre certificat APNs (Apple Push Notification service) à la page C-25* pour Mac.
-

Étape 3 : Installation de votre certificat APNs (Apple Push Notification service)

Procédure

1. Allez à l'emplacement dans lequel vous avez téléchargé le fichier, et double-cliquez sur le fichier pour le télécharger automatiquement vers le Trousseau d'accès puis complétez la demande de signature.
2. Accédez à **Applications > Utilitaires > Trousseau d'accès**.
3. Dans le volet gauche, sélectionnez **connexion** dans la section **Trousseau**, puis sélectionnez **Certificats** dans la section **Catégorie**.
4. Vérifiez que votre certificat Apple Production Push Services apparaît bien dans la liste et qu'une clé privée d'associé se trouve en dessous lorsque vous le développez. Si vous voyez le certificat, suivez les étapes suivantes afin de l'exporter et de le télécharger sur le serveur Trend Micro Mobile Security.



Remarque

Si vous ne voyez pas votre certificat APNs ou que la clé privée n'apparaît pas, vérifiez que le Trousseau d'accès de connexion est sélectionné, que la catégorie Certificats est sélectionnée et que votre clé de certificat a été développée. Si vous ne voyez toujours pas votre certificat, répétez toutes les étapes ci-dessus.

5. Effectuez un clic droit sur (ou maintenez la touche Ctrl enfoncée et cliquez) la clé privée, puis cliquez sur **Exporter**.
6. Choisissez le nom du fichier et l'emplacement dans lequel vous souhaitez enregistrer le fichier, et sélectionnez le format de fichier **Échange d'informations personnelles (.p12)**.



Conseil

Si vous disposez uniquement de l'option enregistrer en tant que fichier **.cer** au lieu d'un **.p12**, cela signifie que vous n'exportez pas le certificat correctement. Assurez-vous d'avoir sélectionné la clé privée à exporter lors de la dernière étape, et que le format de votre fichier est bien **Échange d'informations personnelles (.p12)**.

7. Cliquez sur **Enregistrer**.
8. Choisissez un mot de passe pour l'exportation puis cliquez sur **OK**.



Conseil

Assurez-vous de mémoriser le mot de passe, ou conservez-le dans un endroit sûr. Le mot de passe sera demandé lors du téléchargement du certificat vers le serveur MDM Trend Micro Mobile Security for Enterprise.

Une fois toutes ces étapes terminées, vous devriez disposer des éléments suivants :

- Certificat APNs (Apple Push Notification service) (au format `.p12`, et non `.cer`)
- Le mot de passe que vous avez défini lors de l'exportation du certificat

Vous pouvez désormais télécharger votre certificat vers le serveur Trend Micro Mobile Security. Voir *Téléchargement du certificat APNs (Apple Push Notification service) vers le serveur Mobile Security à la page C-26* pour la procédure.

Téléchargement du certificat APNs (Apple Push Notification service) vers le serveur Mobile Security

Cette section explique le processus de téléchargement du certificat APNs (Apple Push Notification service) vers le serveur Trend Micro Mobile Security for Enterprise afin de commencer à gérer les dispositifs iOS.



Remarque

Assurez-vous de disposer des éléments suivants avant de commencer :

- Fichier du certificat APNs (Apple Push Notification service) (au format `.pfx` ou `.p12`, et non `.cer`)
 - Le mot de passe que vous aviez défini lors de l'exportation du certificat
 - Le compte administrateur du serveur MDM Trend Micro Mobile Security for Enterprise
-

Procédure

1. Connectez-vous à la console Web d'administration.
2. Effectuez l'une des actions suivantes :
 - Cliquez sur **Administration** > **Gestion des certificats**, cliquez sur **Ajouter**, sélectionnez le certificat Apple Push Notification Server du disque dur, puis cliquez sur **Enregistrer**.



FIGURE C-11. Ajout d'un certificat par le biais de la gestion de certificat

- Cliquez sur **Administration** > **Paramètres du Serveur de communication**, cliquez sur l'onglet **Paramètres iOS**, et sélectionnez le certificat Apple Push

Notification Server du disque dur dans le champ **Certificat**, enfin cliquez sur **Enregistrer**.

Paramètres du serveur de communication

Paramètres communs Paramètres Android **Paramètres iOS** Paramètres BlackBerry

Paramètres du service de notifications Push Apple (APNs)

Type de certificat : Production Développement

Certificat : APSP:bdceec92-352e-4ec8-82fa-b3908e5aea15

Sujet du certificat : com.apple.mgmt.External.bdceec92-352e-4ec8-82fa-b3908e5aea15

Paramètres du protocole d'inscription de certificat simple (SCEP)

Activer SCEP

URL d'utilisateur SCEP :

URL d'administrateur SCEP :

Compte d'utilisateur :

Mot de passe de l'utilisateur :

Nom de certificat :

Sujet :

Informations d'identification du profil client

Informations d'identification du profil client : Veuillez sélectionner des informations d'identification ou en charger de nouvelles

Enregistrer Réinitialiser

FIGURE C-12. Ajout d'un certificat par le biais des paramètres du Serveur de communication

Une fois ces étapes terminées, vous pouvez désormais gérer vos dispositifs mobiles iOS.

Génération et configuration d'un certificat APNs dans Windows Server 2003 à l'aide d'IIS 6.0

Pour la procédure à suivre pour la génération et la configuration du certificat APNs dans Windows Server 2003 à l'aide d'Internet Information Services (IIS) 6.0, consultez l'URL suivante :

<http://esupport.trendmicro.com/solution/en-us/1060668.aspx>

Renouvellement d'un certificat APNs

Vous devez renouveler votre certificat APNs avant son expiration pour pouvoir continuer à gérer les dispositifs mobiles iOS. Consultez l'URL suivante pour une procédure détaillée :

<http://esupport.trendmicro.com/solution/en-us/1095594.aspx>



Remarque

Pour renouveler le certificat APNs, vous devrez utiliser le même fichier CSR que vous avez utilisé pour générer le certificat APNs. Si vous disposez du même fichier CSR, vous pouvez générer un nouveau certificat APNs. Cependant, l'utilisation d'un autre certificat APNs, vous obligera à inscrire à nouveau tous les dispositifs mobiles iOS sur le serveur Mobile Security.

Index

A

- Active Directory
 - Compte de service, 2-11
 - Paramètres, 4-17
- Affichage de compatibilité, 3-12
- Apple Store, 5-10

C

- certificat APNs
 - À propos, C-3
- certificat APNs (Apple Push Notification service)
 - nom d'hôte, A-13
- Certificat APNs (Apple Push Notification service)
 - Demande de signature de certificat, C-4
 - Portail des certificats APNs (Apple Push Notification service), C-4
 - Portail de signature de certificat, C-4
- configuration de port
 - modèle de sécurité de base
 - serveur d'administration, A-11–A-13
 - serveur de communication local, A-11–A-13
 - Modèle de sécurité de base
 - Active Directory, A-14
 - BES, A-15
 - serveur SCEP, A-14
 - SQL Server, A-14
 - serveur de communication du nuage
 - BES, A-5
 - serveur d'administration, A-3, A-4
 - serveur SCEP, A-4
 - SQL Server, A-5

serveur de communication local

- Active Directory, A-9
 - BES, A-10
 - serveur d'administration, A-6, A-7
 - serveur de communication, A-8
 - serveur SCEP, A-9
 - SQL Server, A-9
- configuration minimale requise
 - BES 5.x, 5-3
 - connecteurExchange
 - états, 4-19
 - console d'administration Web
 - nom d'utilisateur et mot de passe, 3-11
 - URL, 3-10
 - console Web d'administration, 3-12

E

- Écran de la Licence du produit, 3-13
- environnement
 - dispositifs mobiles BlackBerry, 2-7
 - dispositifs mobiles iOS, 2-4
 - installation, 2-2
- Environnement Java Runtime, 3-4
- Exchange Server
 - Fichier ExchangeConnector.zip, 3-22
 - Outils de gestion, 3-19, 3-22
 - versions prises en charge, 3-18
- expéditeur de SMS, 3-17, 3-18
- Expéditeur de SMS
 - Fichier de configuration, 3-18

F

- Fichier .apk, 3-4
- fichier configuration.xml, B-5
- Fichier Eula_agreement.zip, 4-16

format du code d'activation, 3-13

G

Gestionnaire IIS, B-6

I

inscription MDA

Windows Phone, 5-19

Inscription MDA

Android, 5-13

iOS, 5-15

Installation LCS

Certificat SSL, 3-16

création de certificat, 3-16

Importation de certificat, 3-16

L

l'outil BES d'administration des utilisateurs,
2-13

les clés publiques et privées
du certificat de

Mobile Security, 1-7

les informations d'identification
du certificat de

Mobile Security, 1-7

limite de demandes simultanées IIS, B-6

M

message d'erreur, C-15

message d'invitation, 5-5

méthodes d'installation MDA, 5-10

Mobile Security

Active Directory, 1-7

Agent de dispositif mobile, 1-7

architecture, 1-2

certificat

autorité, 1-7

Certificat Apple Push Notification

service Certificat APNs (Apple

Push Notification service), 1-7

certificat SSL, 1-7

SCEP, 1-7

composants, 1-5

configuration minimale requise, 1-9

Connecteur Exchange de Mobile
Security, 1-12

Expéditeur de SMS, 1-11

IIS, 1-11

Microsoft Exchange Server, 1-11

navigateur Web, 1-11

serveur d'administration et serveur
de communication, 1-10

SQL Server, 1-12

Connecteur Exchange, 1-6

Expéditeur de SMS, 1-6

informations mises à jour, v

méthodes de communication, 1-2

Microsoft SQL Server, 1-7

Modèle de sécurité de base, 1-2, 1-4

Modèle de sécurité renforcée

Serveur de communication du
nuage, 1-2

Serveur de communication local,
1-2, 1-4

Serveur de communication sur
nuage, 1-3

modèles de déploiement, 1-2

outil d'administration des utilisateurs
BES, 1-8

Serveur d'administration, 1-6

Serveur de communication, 1-6

Serveur de communication du nuage,
1-6

- Serveur de communication local, 1-6
- Serveur SMTP, 1-8
- Types de serveur de communication, 1-6
- mot de passe
 - console d'administration Web, 3-11
- mot de passe pour certificat, C-26
- mot de passe pour le certificat, C-17
- N**
- nom convivial, C-16
- O**
- Outils d'administration de Microsoft Exchange Server, 2-12
- P**
- Paramètres Android
 - notifications push, 4-9
- Paramètres BlackBerry
 - Chemin d'accès de l'installation de l'outil d'administration, 4-14
 - Mode d'authentification SQL Server, 4-13
 - outil de commande, 4-12
 - serveur BES, 4-12
 - utilisateur de base de données, 4-13
- paramètres courants
 - Fréquence de collecte d'informations, 4-8
 - type de serveur de communication, 4-7
- paramètres d'inscription
 - authentification, 4-14
 - clé d'inscription, 4-14
- Paramètres de connexion du serveur de communication, 3-15
- paramètres des notifications/rapports
 - Liste d'expéditeurs de SMS, 4-21
 - paramètres des notifications/ rapports
 - Paramètres du serveur SMTP, 4-20
- Paramètres du serveur de communication, 4-6
 - paramètres Android, 4-6
 - paramètres BlackBerry, 4-6
 - paramètres courants, 4-6
 - paramètres iOS, 4-6
 - paramètres Windows Phone, 4-6
- paramètres iOS
 - Certificat Apple Push Notification service (APNs), 4-10
 - Paramètres SCEP, 4-10
- Portail de développement Apple, C-10, C-20
- propriétés du nom unique, C-7
- R**
- règles d'accès au réseau, 2-12
- S**
- SCEP
 - Autorité de certification, B-7
 - Service d'inscription de périphérique réseau, B-8
- Serveur d'administration
 - numéro de port par défaut, 4-18
 - programme d'installation, 3-5
- Serveur MDM Enterprise, C-17
- service de notifications Push Apple
 - nom d'hôte, 2-7
- SMS, 3-17
- SQL Server
 - Méthode d'authentification, 2-10
- T**
- TmDatabase.ini, B-4



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: TSFM96758/141022