TREND MICRO™

2.0 TREND MICRO™ Security

Manuel de l'administrateur

Pour les moyennes et grandes entreprises

pour MAC

Sécurité des points finaux

Nuage protégé

Numéro de référence du document : TSEM25920/130401

Date de publication : Avril 2013

La documentation utilisateur de Trend Micro Security (pour Mac) présente les fonctions principales du logiciel et les instructions d'installation pour votre environnement de production. Lisez attentivement ce manuel avant d'installer ou d'utiliser le logiciel.

Vous trouverez des informations détaillées sur l'utilisation des fonctions spécifiques du logiciel 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 Trend Micro, veuillez nous contacter à l'adresse docs@trendmicro.com.

Veuillez évaluer cette documentation sur le site Web suivant :

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

Table des matières

Préface

Chapitre 1: Présentation de Trend Micro Security (pour Mac)

Chapitre 2: Installation du serveur

Chapitre 3: Démarrage

Chapitre 4: Installation de l'agent

Chapitre 5: Mise à jour de la protection

Chapitre 6: Protection des ordinateurs Mac contre les risques de sécurité

Chapitre 7: Protection des ordinateurs Mac contre les menaces Web

Chapitre 8: Gestion du serveur et des agents

Chapitre 9: Obtenir de l'aide

Annexe A: Prise en charge IPv6 de Trend Micro Security (pour Mac)

Annexe B: Terminologie et concepts liés au produit

Index

Préface

Préface

Bienvenue sur l' du **Manuel de l'administrateur** de Trend Micro Security (pour Mac). Ce document décrit l'installation du serveur et de l'agent Trend Micro Security (pour Mac), les informations de démarrage et la gestion du serveur et de l'agent.

Documentation Trend Micro Security (pour Mac)

La documentation Trend Micro Security (pour Mac) inclut les éléments suivants :

DOCUMENTATION	DESCRIPTION
Manuel de l'administrateur	Document PDF qui décrit l'installation du serveur et de l'agent Trend Micro Security (pour Mac), les informations de démarrage et la gestion du serveur et de l'agent.
Aide	Fichiers HTML contenant des descriptions de procédures, des conseils d'utilisation et des informations relatives à des domaines particuliers.
Fichier Lisez-moi	Contient une liste des problèmes connus et les étapes d'installation de base. Il peut aussi contenir des informations sur le produit qui n'ont pas pu être intégrées à temps dans les autres documents.
Base de connaissances	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, consultez le site Web suivant : http://esupport.trendmicro.com

Consultez et téléchargez la documentation produit à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/trend-micro-security-(for-mac).aspx

Public cible

La documentation Trend Micro Security (pour Mac) est destinée aux utilisateurs suivants :

- **Administrateurs Trend Micro Security (for Mac)** : responsables de la gestion Trend Micro Security (pour Mac), y compris l'installation et la gestion du serveur et de l'agent. Ces utilisateurs doivent disposer d'une connaissance approfondie de la mise en réseau et de la gestion des serveurs.

- **Utilisateurs finaux** : utilisateurs qui ont installé l'agent Trend Micro Security (pour Mac) sur leurs ordinateurs Macintosh. Leur niveau de compétence informatique varie : débutant, expérimenté, etc.

Nomenclatures du document

Pour faciliter la recherche et la compréhension des informations, la documentation Trend Micro Security (pour Mac) utilise les conventions suivantes :

TABLEAU 1. Nomenclatures du document

NOMENCLATURE	DESCRIPTION
MAJUSCULES	Acronymes, abréviations, noms de certaines commandes et touches sur le clavier
Gras	Menus et commandes de menus, boutons de commande, onglets, options et tâches
Italique	Références à d'autres documents ou composants de nouvelles technologies
<Text>	Indique que le texte entre crochets doit être remplacé par les données réelles. Par exemple, `C:\Program Files\<file_name>` peut être `C:\Program Files\sample.jpg`.
Remarque	Introduit des remarques ou recommandations relatives à la configuration
Conseil	Fournit des informations sur les pratiques recommandées concernant Trend Micro
AVERTISSEMENT!	Fournit des avertissements sur les activités pouvant nuire aux ordinateurs de votre réseau

Terminologie

Le tableau suivant fournit la terminologie officielle utilisée dans la documentation Trend Micro Security (pour Mac) :

TERMINOLOGIE	DESCRIPTION
Agent	Programme agent de Trend Micro Security (pour Mac) installé sur un ordinateur Mac.
Point final	Ordinateur Mac sur lequel est installé l'agent
Utilisateur agent (ou utilisateur)	Utilisateur gérant l'agent depuis l'ordinateur Mac
Serveur	Programme associé au serveur Trend Micro Security (pour Mac)
Serveur	Ordinateur où le serveur Trend Micro Security (pour Mac) est installé
Administrateur (ou administrateur Trend Micro Security (pour Mac))	Utilisateur gérant le serveur Trend Micro Security (pour Mac)
Console	Interface utilisateur permettant de configurer et de gérer les paramètres du serveur et de l'agent Trend Micro Security (pour Mac) La console du programme serveur est appelée « console Web » et la console du programme agent « console agent ».
Risque de sécurité	Terme générique regroupant les virus/programmes malveillants, les spywares/graywares et les menaces Web
Service produit	Service Trend Micro Security (pour Mac) géré à partir de la console d'administration Microsoft Management Console (MMC)
Composants	Responsables du scan, de la détection et des actions contre les risques de sécurité

TERMINOLOGIE	DESCRIPTION
`Dossier d'installation de l'agent`	Dossier de l'ordinateur Mac contenant les fichiers de l'agent Trend Micro Security (pour Mac). `/Library/Application Support/TrendMicro`
`Dossier d'installation du serveur`	Dossier du serveur contenant les fichiers du serveur Trend Micro Security (pour Mac). Une fois le serveur Trend Micro Security (pour Mac) installé, le dossier est créé sur le même répertoire que le serveur OfficeScan. Si vous acceptez les paramètres par défaut lors de l'installation du serveur OfficeScan, le dossier d'installation du serveur sera situé à l'un des emplacements suivants : • `C:\Program Files\Trend Micro\OfficeScan \Addon\TMSM` • `C:\Program Files (x86)\Trend Micro \OfficeScan\Addon\TMSM`
Double pile	Entité ayant à la fois une adresse IPv4 et une adresse IPv6. Par exemple : • Un point final à double pile est un ordinateur Mac avec des adresses IPv4 et IPv6. • Un agent à double pile désigne un agent installé sur un point final à double pile. • Un serveur proxy à double pile, tel que DeleGate, peut effectuer des conversions entre adresses IPv4 et IPv6.
IPv4 pur	Entité possédant uniquement une adresse IPv4
IPv6 pur	Entité possédant uniquement une adresse IPv6

Chapitre 1

Présentation de Trend Micro Security (pour Mac)

Ce chapitre présente Trend Micro™ Security (pour Mac) et fournit une présentation de ses fonctionnalités et de ses capacités.

À propos de Trend Micro Security (pour Mac)

Trend Micro™ Security (pour Mac) offre une protection actualisée des points finaux contre les risques de sécurité, les menaces combinées et les attaques Web indépendantes de la plate-forme.

Le serveur Trend Micro Security (pour Mac) est un plugiciel intégré aux produits Trend Micro tels qu'OfficeScan et Worry-free Business Security et installé via l'infrastructure de Plug-in Manager. Le serveur Trend Micro Security (pour Mac) déploie des agents vers les ordinateurs Mac.

Fonctionnalités et avantages principaux

Trend Micro Security (pour Mac) fournit les fonctionnalités et avantages suivants :

- **Protection contre les risques de sécurité**

  Trend Micro Security (pour Mac) protège les ordinateurs Mac contre les risques de sécurité en scannant les fichiers, puis en effectuant une action spécifique pour chaque risque de sécurité détecté. Un nombre important de risques de sécurité détectés sur une courte période signale une épidémie. Trend Micro Security (pour Mac) vous avertit des épidémies afin que vous puissiez agir immédiatement, en nettoyant les ordinateurs infectés et en les isolant jusqu'à ce qu'ils soient inoffensifs.

- **Réputation de sites Web**

  La technologie de réputation de sites Web protège proactivement les ordinateurs Mac au sein ou en dehors du réseau d'entreprise contre les sites Web malveillants et potentiellement dangereux. La réputation de sites Web rompt la chaîne d'infection et empêche le téléchargement de code malveillant.

- **Gestion centralisée**

  Une console d'administration Web offre aux administrateurs un accès transparent à tous les agents du réseau. La console Web coordonne le déploiement automatique des stratégies de sécurité, des fichiers de signatures et des mises à jour logicielles sur chaque agent. Les administrateurs peuvent effectuer une administration à distance et configurer les paramètres des agents seuls ou des groupes d'agents.

Nouveautés de cette version

Trend Micro Security (pour Mac) inclut les nouvelles fonctionnalités et améliorations suivantes :

FONCTIONNALITÉ/ AMÉLIORATION	DÉTAILS
Performances et fonctionnalités de scan améliorées	• Le cache de scan à la demande améliore les performances de scan et réduit sa durée en ignorant les fichiers inoffensifs, déjà scannés précédemment. • Configurez facilement les dossiers d'exclusions de scan en utilisant les caractères génériques. • Permettre aux utilisateurs de différer, d'ignorer ou d'arrêter un scan programmé.
Smart protection pour la réputation de sites Web	Les agents envoient des requêtes de l'évaluation de la réputation de sites Web aux sources Smart Protection afin de déterminer la sécurité des sites Web. Les agents exploitent la liste des sources Smart Protection configurée pour les agents OfficeScan afin de déterminer les sources Smart Protection auxquelles ils doivent envoyer des requêtes.
Améliorations de la mise à jour	Les agents peuvent effectuer des mises à jour de façon programmée et obtenir des mises à jour depuis le serveur ActiveUpdate de Trend Micro si le serveur Trend Micro Security (pour Mac) est indisponible.
Widgets	Si Trend Micro Security (pour Mac) est installé conjointement avec OfficeScan 10.6 ou version ultérieure et Plug-in Manager 2.0 ou version ultérieure, vous pouvez gérer les widgets Trend Micro Security (pour Mac) depuis le tableau de bord d'OfficeScan. Les widgets sont disponibles après avoir activé Trend Micro Security (pour Mac).
Intégration de Control Manager	Les paramètres de l'agent Trend Micro Security (pour Mac) peuvent désormais être déployés depuis la gestion des stratégies de Control Manager.
Prise en charge IPv6	Les agents et serveurs Trend Micro Security (pour Mac) peuvent désormais être installés sur des ordinateurs IPv6.

FONCTIONNALITÉ/ AMÉLIORATION	DÉTAILS
Aide en nuage	Disposez des informations sur le produit les plus récentes à partir du système d'aide en nuage de Trend Micro, en cliquant sur le lien d'Aide à partir de n'importe quel écran d'une console Web. Si la console Web est isolée du réseau Internet, le lien ouvre une copie en local de l'Aide, actualisée au moment de la sortie du produit.

Le serveur Trend Micro Security (pour Mac)

Le serveur Trend Micro Security (pour Mac) est un référentiel central contenant toutes les configurations de vos agents, les journaux des risques de sécurité, ainsi que les mises à jour.

Le serveur exécute deux tâches primordiales :

- surveiller et gérer les agents Trend Micro Security (pour Mac)
- télécharger les composants dont les agents ont besoin. Par défaut, le serveur Trend Micro Security (pour Mac) télécharge les composants à partir du serveur ActiveUpdate de Trend Micro, puis les distribue aux agents

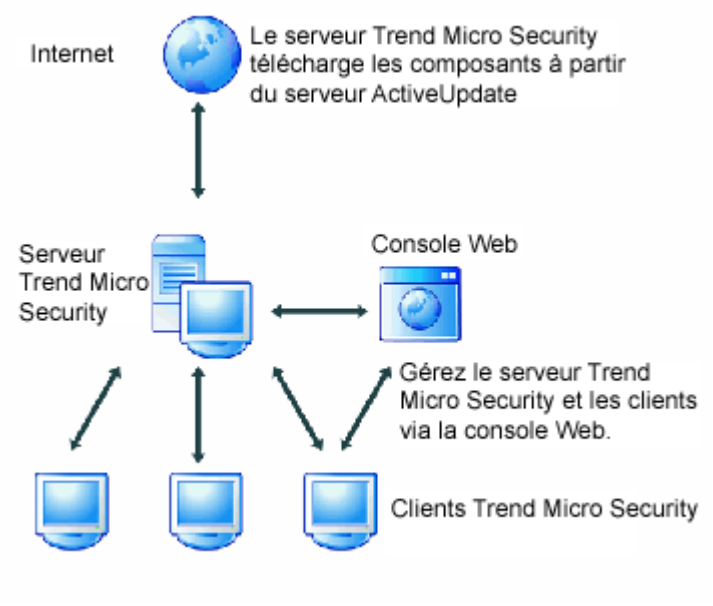


FIGURE 1-1. Fonctionnement du serveur Trend Micro Security (pour Mac)

Trend Micro Security (pour Mac) offre une communication en temps réel et bidirectionnelle entre le serveur et les agents. Gérez les agents à partir d'une console Web basée sur un navigateur à laquelle vous accédez à partir d'un point du réseau, quel qu'il soit. Le serveur communique avec l'agent via le protocole ActiveMQ™.

L'agent Trend Micro Security (pour Mac)

Vous pouvez protéger les ordinateurs Mac contre les risques de sécurité en installant l'agent Trend Micro Security (pour Mac) sur chaque ordinateur. L'agent met à votre disposition trois types de scan :

- Scan en temps réel
- Scan programmé
- Scan manuel

L'agent effectue son rapport sur le serveur Trend Micro Security (pour Mac) parent à partir duquel il a été installé. L'agent envoie en temps réel les informations relatives à l'état et aux événements au serveur. Les agents communiquent avec le serveur via le protocole ActiveMQ.

Chapitre 2

Installation du serveur

Ce chapitre décrit la configuration système requise et la procédure relatives à l'installation du serveur Trend Micro Security (pour Mac).

Configuration minimale requise pour l'installation du serveur

La configuration minimale suivante est requise pour l'installation du serveur Trend Micro Security (pour Mac) :

TABLEAU 2-1. Configuration minimale requise pour l'installation du serveur

RESSOURCE	CONFIGURATION MINIMALE
Serveur OfficeScan	L'une des versions suivantes : • 10.6 avec ou sans patch • 10.5 avec ou sans patch • 10.0 avec ou sans patch
Plug-in Manager	2.0
Mémoire RAM	1 Go minimum, 2 Go recommandés

Espace disque disponible	• 1,5 Go minimum si le serveur OfficeScan est installé sur le lecteur système (habituellement, le lecteur C:)
	• Si le serveur OfficeScan n'est pas installé sur le lecteur système :
	  • 600 Mo minimum sur le lecteur d'installation du serveur OfficeScan. Le serveur Trend Micro Security (pour Mac) sera installé sur ce lecteur.
	  • 900 Mo minimum sur le lecteur système. Les programmes tiers utilisés par le serveur Trend Micro Security (pour Mac) seront installés sur ce lecteur.

RESSOURCE	CONFIGURATION MINIMALE

Autres	• Microsoft™ .NET Framework 2.0 SP2
	• Java Runtime Environment™ (JRE) 1,6 ou une version ultérieure, avec la mise à jour la plus récente
	
	Remarque
	Pour des performances optimales, installez JRE 1.7 ou une version ultérieure. Installez JRE pour Windows x86 ou JRE pour Windows x64, en fonction du système d'exploitation de l'ordinateur hôte.
	
	• Les logiciels tiers suivants seront installés automatiquement :
	  • Microsoft SQL Server 2005 ou 2008 Express
	  • Apache™ ActiveMQ 5.6.0
	  • Microsoft Visual C++ 2005 Redistributable

Source de mise à jour

Avant de procéder à l'installation du serveur Trend Micro Security (pour Mac), vérifiez la source de mise à jour de Plug-in Manager en accédant à **Mises à jour** > **Serveur** > **Source de mise à jour** dans la console Web OfficeScan. Plusieurs sources de mise à jour sont disponibles :

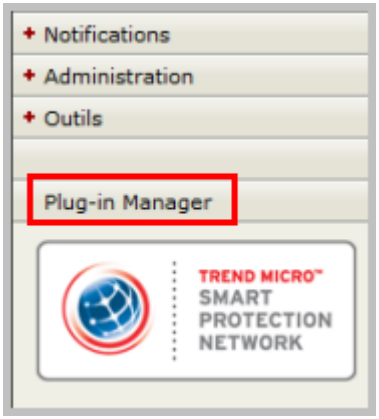
TABLEAU 2-2. Sources de mise à jour possibles

SOURCE DE MISE À JOUR SÉLECTIONNÉE	DESCRIPTION ET INSTRUCTIONS
`Serveur ActiveUpdate`	Le serveur ActiveUpdate de Trend Micro est la source de mise à jour par défaut pour OfficeScan. Une connexion Internet est requise pour accéder à ce serveur. Si le serveur se connecte à Internet par le biais d'un serveur proxy, assurez-vous que la connexion Internet puisse être établie à l'aide des paramètres proxy.
`Autre source de mise à jour`	Si vous avez spécifié plusieurs sources de mise à jour : • Veillez à ce que le serveur puisse se connecter à la première source de mise à jour de la liste. Si ce n'est pas possible, il n'essaye pas de se connecter aux autres sources de mise à jour. • Vérifiez que la première source de mise à jour contient la version la plus récente de la liste des composants Plug-in Manager (`OSCE_AOS_COMP_LIST.xml`) et le pack d'installation de Trend Micro Security (pour Mac). Pour obtenir de l'aide au sujet de la configuration d'une source de mise à jour, contactez votre fournisseur d'assistance.
`Emplacement Intranet contenant une copie du fichier actuel`	Si la source de mise à jour est un emplacement Intranet : • Assurez-vous qu'il existe une connexion opérationnelle entre le serveur et la source de mise à jour. • Vérifiez que la source de mise à jour contient la version la plus récente de la liste des composants Plug-in Manager (`OSCE_AOS_COMP_LIST.xml`) et le pack d'installation de Trend Micro Security (pour Mac). Pour obtenir de l'aide au sujet de la configuration de la source Intranet, contactez votre fournisseur d'assistance.

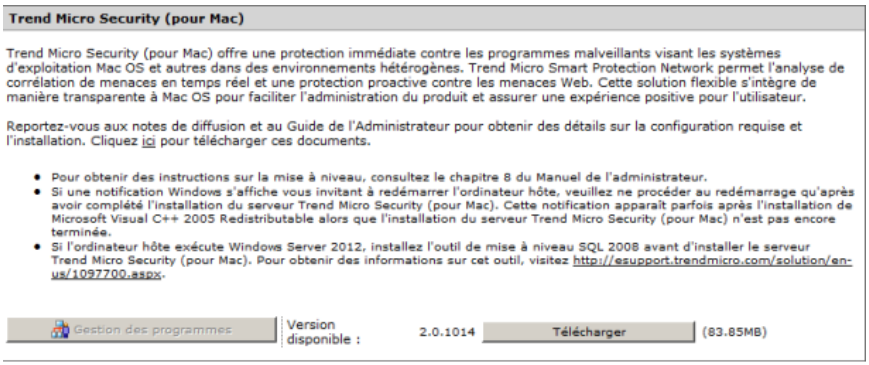
Installation du serveur Trend Micro Security (pour Mac)

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Plug-in Manager** dans le menu principal.



2. Accédez à la section **Trend Micro Security (pour Mac)**, puis cliquez sur **Télécharger**.

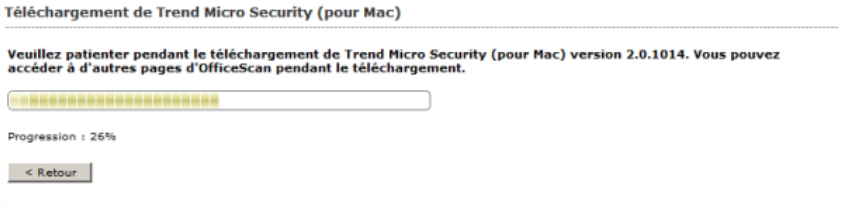


La taille du fichier à télécharger s'affiche à côté du bouton **Télécharger**.

Plug-in Manager télécharge le pack vers `<OfficeScan server installation folder>\PCCSRV\Download`.

`<OfficeScan server installation folder>` est généralement `C:\Program Files\Trend Micro\OfficeScan`.

3. Surveillez la progression du téléchargement.



Vous pouvez naviguer dans une autre fenêtre pendant le téléchargement.

Si vous rencontrez des problèmes lors du téléchargement du pack, consultez les journaux de mise à jour du serveur sur la console Web OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Journaux de mise à jour du serveur**.

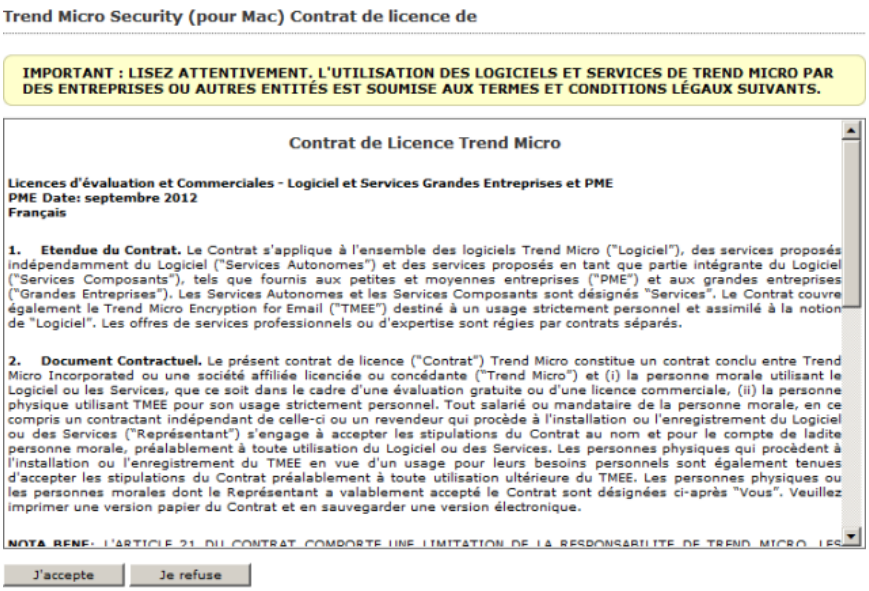
4. Pour installer immédiatement Trend Micro Security (pour Mac), cliquez sur **Installer immédiatement**. Pour l'installer ultérieurement, procédez comme suit :

   a. Cliquez sur **Installer ultérieurement**.

   b. Ouvrez l'écran Plug-in Manager.

   c. Accédez à la section **Trend Micro Security (pour Mac)**, puis cliquez sur **Installer**.

5. Lisez le contrat de licence puis acceptez-le en cliquant sur **J'accepte**.



L'installation démarre.

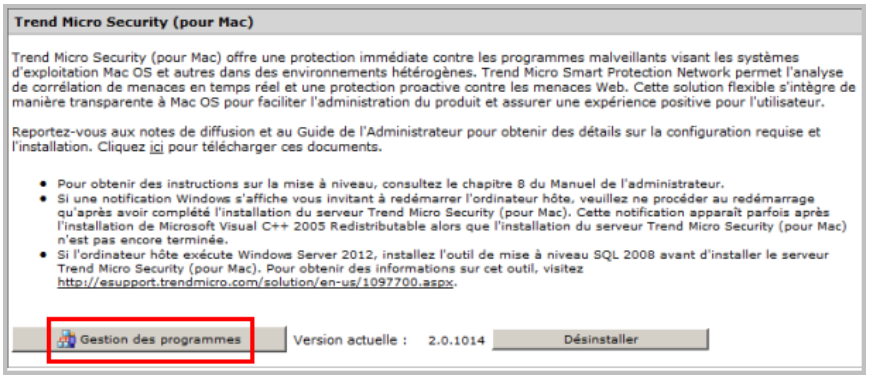
6. Surveillez la progression de l'installation. Après l'installation, l'écran Plug-in Manager se recharge.

Activation du produit pour la première fois

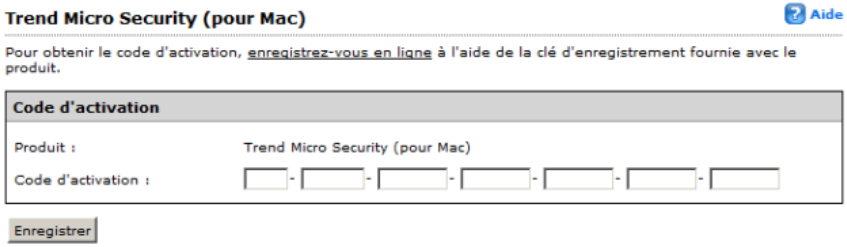
Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Plug-in Manager** dans le menu principal.

2. Accédez à la section **Trend Micro Security (pour Mac)**, puis cliquez sur **Gestion des programmes**.



3. Saisissez le code d'activation du produit (sensible à la casse), puis cliquez sur **Enregistrer**. .



Si vous ne connaissez pas le code d'activation, cliquez sur le lien **Enregistrement en ligne** pour accéder au site Web d'enregistrement de Trend Micro. Une fois l'enregistrement terminé, Trend Micro envoie un e-mail contenant le code d'activation. Vous pouvez ensuite poursuivre l'activation.

Si vous avez activé une licence de version d'évaluation, veillez à effectuer une mise à niveau vers la version complète avant l'expiration de la licence.

4. Dans la fenêtre Détails de la licence qui s'affiche, cliquez sur **Installer** pour ouvrir la console Web.

5. Cliquez sur **Installer** pour ouvrir la console Web.

Tâches à effectuer sur le serveur après l'installation

Procédure

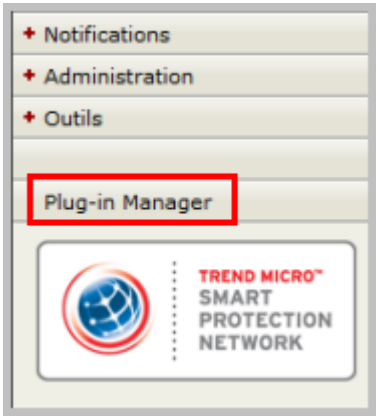
1. Vérifiez que les services suivants s'affichent sur la console d'administration Microsoft :
   - **ActiveMQ pour Trend Micro Security**
   - **SQL Server (TMSM)**
   - **Trend Micro Security (pour Mac)**
2. Vérifiez que le processus suivant est en cours d'exécution dans le gestionnaire des tâches Windows : **TMSMMainService.exe**
3. Vérifiez que la clé de Registre suivante existe dans l'éditeur du Registre : `HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_TMSM`

4. Vérifiez que les fichiers du serveur Trend Micro Security (pour Mac) figurent sous le <*Server installation folder*>..

Désinstallation du serveur Trend Micro Security (pour Mac)

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Plug-in Manager** dans le menu principal.



2. Accédez à la section **Trend Micro Security (pour Mac)**, puis cliquez sur **Désinstaller**.

3. Surveillez la progression de la désinstallation. Vous pouvez naviguer dans une autre fenêtre pendant l'opération. Une fois la désinstallation terminée, le serveur Trend Micro Security (pour Mac) est de nouveau disponible pour installation.

Remarque

Le pack de désinstallation ne supprime pas Java Runtime Environment (JRE), qui est utilisé par Trend Micro Security (pour Mac). Vous pouvez supprimer JRE si aucune autre application ne l'utilise.

Chapitre 3

Démarrage

Ce chapitre décrit la procédure de démarrage de Trend Micro Security (pour Mac) ainsi que les paramètres de configuration initiale.

Console Web

La console Web est le point central permettant de surveiller les agents Trend Micro Security (pour Mac) et de configurer les paramètres à déployer sur les agents. Elle présente des paramètres et des valeurs par défaut que vous pouvez configurer en fonction de vos spécifications et exigences de sécurité.

Utilisez la console Web pour effectuer les opérations suivantes :

- gérer les agents installés sur des ordinateurs Mac ;
- organiser les agents par groupes logiques pour permettre de les configurer et de les gérer tous ensemble ;
- définir des profils de scan et exécuter un scan sur un ou plusieurs ordinateurs ;
- configurer les notifications relatives aux risques de sécurité et afficher les journaux envoyés par les agents ;
- configurer les critères et notifications en matière d'épidémie.

Ouverture de la console Web

Avant de commencer

Ouvrez la console Web à partir d'un ordinateur en réseau équipé des ressources suivantes :

- Écran avec résolution 800 x 600 pixels, 256 couleurs minimum
- Microsoft™ Internet Explorer™ 7.0 ou version ultérieure. Si l'ordinateur exécute une plate-forme x64, utilisez la version 32 bits d'Internet Explorer.

Procédure

1. Dans un navigateur Web, saisissez l'URL du serveur OfficeScan.
2. Saisissez le nom d'utilisateur et le mot de passe pour la connexion au serveur OfficeScan.
3. Dans le menu principal, cliquez sur **Plug-in Manager**.

4. Accédez à la section **Trend Micro Security (pour Mac)**, puis cliquez sur **Gestion des programmes**.

Résumé de sécurité

L'écran Résumé s'affiche lorsque vous ouvrez la console Web de Trend Micro Security (pour Mac) ou cliquez sur **Résumé** dans le menu principal.

Conseil

Actualisez l'écran régulièrement pour obtenir les informations les plus récentes.

Agents

La section **Agents** affiche les informations suivantes :

- L'état de la connexion entre tous les agents et le serveur Trend Micro Security (pour Mac). Le fait de cliquer sur un lien ouvre l'arborescence des agents, dans laquelle vous pouvez configurer les paramètres des agents.
- Le nombre de risques de sécurité et de menaces Web détectés
- Le nombre d'ordinateurs sur lesquels ont été détectés des risques de sécurité et des menaces Web. Le fait de cliquer sur un chiffre ouvre l'arborescence des agents, qui affiche la liste des ordinateurs présentant des risques de sécurité ou des menaces Web. Dans l'arborescence des agents, effectuez les tâches suivantes :
  - Sélectionnez un ou plusieurs agents, cliquez sur **Journaux** > **Journaux de risques de sécurité**, puis spécifiez les critères des journaux. Dans l'écran qui s'affiche, vérifiez la colonne **Résultats** pour voir si les actions de scan sur les risques de sécurité ont été correctement effectuées. Consultez la rubrique *Résultats du scan à la page 6-29* pour obtenir la liste des résultats de scan.
  - Sélectionnez un ou plusieurs agents, cliquez sur **Journaux** > **Journaux de réputation de sites Web**, puis spécifiez les critères des journaux. Sur l'écran qui s'affiche, vérifiez la liste des sites Web bloqués. Vous pouvez ajouter les sites Web que vous ne souhaitez pas bloquer à la liste des URL approuvées.

Pour obtenir des informations détaillées, consultez la rubrique *Configuration de la liste des URL approuvées à la page 7-6*.

État de la mise à jour

Le tableau **État de la mise à jour** contient des informations sur les composants de Trend Micro Security (pour Mac) et le programme de l'agent qui protège les ordinateurs Mac contre les risques de sécurité.

Tâches présentées dans ce tableau :

- Mettez à jour les composants obsolètes immédiatement. Pour obtenir des informations détaillées, consultez la rubrique *Lancement de la mise à jour des agents à partir de l'écran Résumé à la page 5-12*.
- Mettez à niveau les agents vers la version la plus récente du programme si vous avez récemment mis à niveau le serveur. Consultez la rubrique *Mise à niveau du serveur et des agents à la page 8-2* pour obtenir des instructions de mise à niveau des agents.

L'arborescence agent

L'arborescence agent Trend Micro Security (pour Mac) affiche tous les agents que le serveur gère actuellement et qui appartiennent à un certain groupe. Utilisez les éléments de menu situés au-dessus de l'arborescence agent pour configurer, gérer et appliquer simultanément la même configuration à tous les agents appartenant à un groupe.

Tâches générales de l'arborescence agent

Les tâches générales suivantes peuvent être effectuées lorsque l'arborescence agent s'affiche :

Procédure

- Cliquez sur l'icône racine () pour sélectionner tous les groupes et agents. Lorsque vous sélectionnez l'icône racine puis choisissez une tâche située au-dessus de l'arborescence agent, un écran de configuration des paramètres s'affiche. Dans l'écran, choisissez les options générales suivantes :

- **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un groupe existant/futur. Les groupes futurs sont des groupes qui ne sont pas encore créés au moment de la configuration des paramètres.

- **Appliquer aux groupes futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux groupes futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un groupe existant.

- Pour sélectionner plusieurs groupes ou agents se trouvant à la suite, cliquez sur le premier groupe ou agent de la liste, maintenez la touche MAJ enfoncée et cliquez sur le dernier groupe ou agent de la liste.

- Pour sélectionner plusieurs groupes ou agents n'étant pas à la suite les uns des autres, maintenez enfoncée la touche CTRL et cliquez sur les groupes ou agents souhaités.

- Recherchez un agent à gérer en spécifiant son nom complet ou partiel dans le champ **Rechercher les ordinateurs**. La liste des agents correspondants apparaît dans l'arborescence agent.

Remarque

Les adresses IPv6 ou IPv4 ne peuvent pas être spécifiées lors de la recherche d'agents spécifiques.

- Triez les agents en fonction des informations de colonne en cliquant sur le nom de la colonne.

- Affichez le nombre total d'agents sous l'arborescence agent.

Tâches spécifiques de l'arborescence agent

Des éléments de menu situés au-dessus de l'arborescence agent permettent d'effectuer les tâches suivantes :

BOUTON DE MENU	TÂCHE
Tâches	• Mettre à jour les composants de l'agent. Pour obtenir des informations détaillées, consultez la rubrique *Mises à jour des agents à la page 5-8*. • Exécuter Scanner maintenant sur les ordinateurs Mac clients. Pour obtenir des informations détaillées, consultez la rubrique *Scanner maintenant à la page 6-9*.

Paramètres	• Configurez les paramètres de scan.
	  • *Scan manuel à la page 6-7*
	  • *Scan en temps réel à la page 6-6*
	  • *Scan programmé à la page 6-8*
	  • *Exclusions de scan à la page 6-18*
	  • *Paramètres de cache des scans à la page 6-22*
	• Configurer les paramètres de réputation de sites Web. Pour obtenir des informations détaillées, consultez la rubrique *Configuration des paramètres de réputation de sites Web à la page 7-3*.
	• Configurer les paramètres de scan. Pour obtenir des informations détaillées, consultez la rubrique *Configuration des paramètres de mise à jour des agents à la page 5-10*.

Journaux	Affichez les journaux. • *Consultation des journaux de risques de sécurité à la page 6-28* • *Consultation des journaux de réputation de sites Web à la page 7-7*
Gérer l'arborescence agent	Gérer les groupes Trend Micro Security (pour Mac). Pour obtenir des informations détaillées, consultez la rubrique *Groupes à la page 3-7*.

Groupes

Un groupe figurant dans Trend Micro Security (pour Mac) est un ensemble d'agents partageant une configuration commune et exécutant des tâches similaires. En regroupant vos agents, vous pouvez configurer, gérer et appliquer simultanément la même configuration à tous les agents appartenant aux groupes.

Pour une gestion plus simple, regroupez les agents en fonction du service auquel ils appartiennent ou des fonctions qu'ils exécutent. Vous pouvez aussi regrouper les agents exposés à un risque d'infection plus élevé afin de leur appliquer simultanément une configuration plus sécurisée. Vous pouvez ajouter ou renommer les groupes, déplacer les agents vers un autre groupe ou supprimer les agents définitivement. Un agent supprimé de l'arborescence agent n'est pas automatiquement désinstallé de l'ordinateur agent. L'agent peut toujours effectuer des tâches dépendant du serveur, telles que la mise à jour des composants. Le serveur n'est cependant pas informé de la présence de l'agent et ne peut donc pas lui envoyer de configurations ni de notifications.

Si l'agent a été désinstallé de l'ordinateur Mac, il n'est pas automatiquement supprimé de l'arborescence agent et son état de connexion est « Hors ligne ». Supprimez manuellement l'agent de l'arborescence agent.

Ajout d'un groupe

Procédure

1. Accédez à **Gestion des agents**.
2. Cliquez sur **Gérer l'arborescence agent** > **Ajouter groupe**.
3. Saisissez un nom pour le groupe que vous souhaitez ajouter.
4. Cliquez sur **Ajouter**.

   Le nouveau groupe s'affiche dans l'arborescence agent.

Suppression d'un groupe ou d'un agent

Avant de commencer

Avant de supprimer un groupe, vérifiez s'il existe des agents appartenant au groupe, puis déplacez-les vers un autre groupe. Pour obtenir des informations détaillées sur le déplacement des agents, consultez la rubrique *Déplacement d'un agent à la page 3-9*.

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence agent, sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Gérer l'arborescence agent** > **Supprimer groupe/agent**.
4. Cliquez sur **OK** pour confirmer la suppression.

Changement de nom d'un groupe

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence agent, sélectionnez les groupes à renommer.
3. Cliquez sur **Gérer l'arborescence agent** > **Renommer groupe**.
4. Saisissez un nouveau nom pour le groupe.
5. Cliquez sur **Renommer**.

   Le nouveau nom du groupe s'affiche dans l'arborescence agent.

Déplacement d'un agent

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence agent, sélectionnez un ou plusieurs agents appartenant au groupe.
3. Cliquez sur **Gérer l'arborescence agent** > **Déplacer agent**.
4. Sélectionnez le groupe vers lequel déplacer l'agent.
5. Décidez d'appliquer ou non les paramètres du nouveau groupe à l'agent.

Conseil

Conseil : vous pouvez également utiliser la fonction glisser-déposer pour déplacer un agent vers un autre groupe dans l'arborescence agent.

6. Cliquez sur **Déplacer**.

Widgets

Vous pouvez gérer les widgets Trend Micro Security (pour Mac) à partir du tableau de bord OfficeScan. Les widgets sont disponibles après avoir activé Trend Micro Security (pour Mac).

Pour afficher les widgets, assurez-vous que la version d'OfficeScan est la version 10.6 ou ultérieure et que la version de Plug-in Manager est la version 2.0 ou ultérieure.

Pour obtenir des informations détaillées sur l'utilisation des widgets, consultez la documentation d'OfficeScan.

Widget de connectivité des agents (Mac)

Le widget de connectivité des agents (Mac) affiche l'état de la connexion des agents avec le serveur Trend Micro Security (pour Mac). Les données sont consultables sous forme

de tableau et de graphique à secteurs. Vous pouvez passer de l'un à l'autre en cliquant sur les icônes d'affichage ( ).

Widget de connectivité des agents (Mac) présenté sous forme de tableau

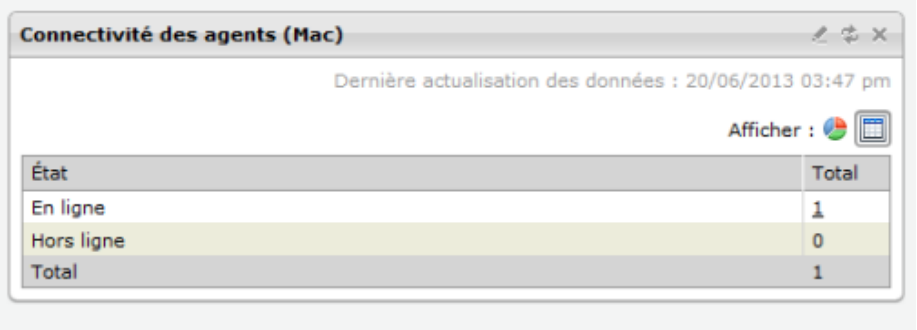


FIGURE 3-1. Widget de connectivité des agents (Mac) affiché sous forme de tableau

Si au moins 1 agent se trouve dans un état donné, vous pouvez cliquer sur le chiffre indiqué afin d'afficher ces agents dans l'arborescence des agents de Trend Micro Security (pour Mac). Vous pouvez lancer des tâches sur ces agents ou modifier leurs paramètres.

Widget de connectivité des agents (Mac) présenté sous forme de graphique à secteurs

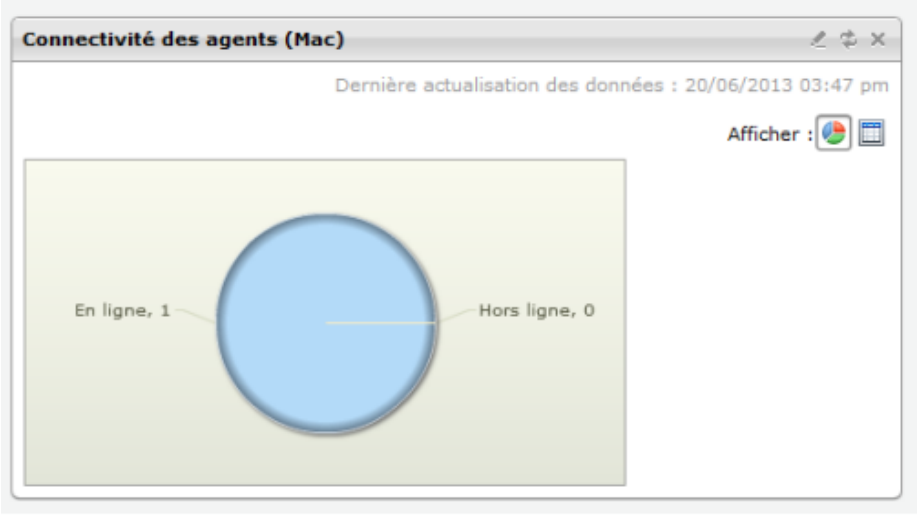


FIGURE 3-2. Widget de connectivité des agents (Mac) affiché sous forme de graphique à secteurs

Le graphique à secteurs indique le nombre d'agents se trouvant dans chaque état, mais ne fournit pas de liens vers l'arborescence des agents de Trend Micro Security (pour Mac). Vous pouvez cliquer sur un état pour le séparer du reste du graphique ou l'y reconnecter.

Widget de mise à jour des agents (Mac)

Le widget de mise à jour des agents (Mac) indique les composants et les programmes protégeant les ordinateurs Mac des risques de sécurité.

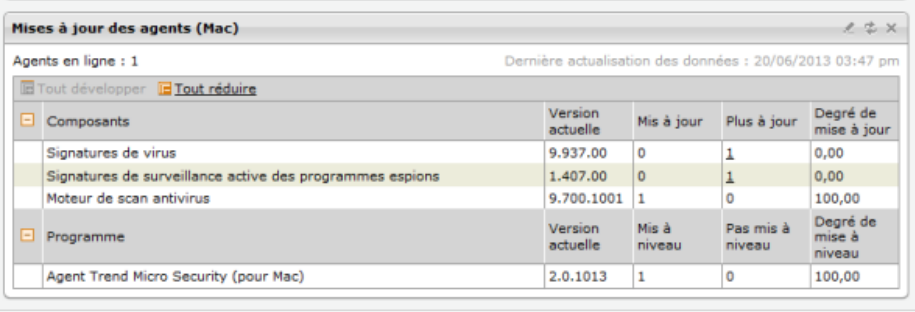


FIGURE 3-3. Widget de mise à jour des agents (Mac)

Dans ce widget, vous pouvez :

- Afficher la version actuelle de chaque composant.
- Afficher le nombre d'agents dont les composants sont obsolètes, sous la colonne **Plus à jour**. Si certains agents nécessitent une mise à jour, cliquez sur le chiffre, qui est un lien, pour lancer la mise à jour.
- Pour le programme des agents, affichez les agents n'ayant pas bénéficié d'une mise à jour via un clic sur le chiffre faisant effet de lien.

Remarque

Les liens ouvrent la console du serveur Trend Micro Security (pour Mac), à partir de laquelle vous pouvez effectuer des tâches supplémentaires.

Widget de détection des risques de sécurité (Mac)

Le widget de détection des risques de sécurité (Mac) indique le nombre risques de sécurité et de menaces Web.

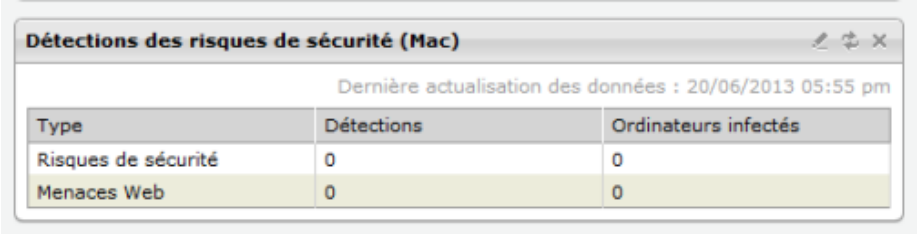


FIGURE 3-4. Widget de détection des risques de sécurité (Mac)

Si au moins 1 ordinateur est infecté, vous pouvez cliquer sur le chiffre indiqué afin d'afficher ces agents dans l'arborescence des agents de Trend Micro Security (pour Mac). Vous pouvez lancer des tâches sur ces agents ou modifier leurs paramètres.

Trend Micro Smart Protection

Trend Micro Smart Protection est une infrastructure de sécurité du contenu cloud-client de dernière génération, conçue pour protéger nos clients des risques de sécurité et des menaces Web. Elle est au cœur de solutions aussi bien locales qu'hébergées, ayant pour but de protéger les utilisateurs lorsqu'ils sont sur un réseau, chez eux, sur leur lieu de travail ou en déplacement. Cela est possible grâce à des clients peu encombrants permettant d'accéder à une combinaison unique de technologies cloud centrées sur la réputation des e-mails, du Web et de fichiers, ainsi que de bases de données de menaces. La protection des clients est automatiquement mise à jour et renforcée via l'accès au réseau par un nombre toujours croissant de produits, de services et d'utilisateurs, ce qui crée un service de protection communautaire en temps réel.

Services Smart Protection

Les services Smart Protection incluent Services de File Reputation, Services de réputation de sites Web et Smart Feedback.

Dans cette version, les agents Trend Micro Security (pour Mac) utilisent les *Services de réputation de sites Web à la page 7-2* pour déterminer le niveau de sécurité des sites Web auxquels un utilisateur accède via un ordinateur Mac.

Sources Smart Protection

Les Services de réputation de sites Web sont fournis par **des sources Smart Protection**, à savoir le réseau **Trend Micro Smart Protection Network** et des serveurs **Smart Protection Server**.

Le réseau Trend Micro Smart Protection Network est une infrastructure à l'échelle mondiale, basée sur Internet, conçue pour les utilisateurs ne disposant pas d'un accès direct à leur réseau d'entreprise.

Les serveurs Smart Protection Server sont destinés aux utilisateurs ayant accès à leur réseau local d'entreprise. Les serveurs locaux adaptent les services Smart Protection au réseau d'entreprise afin d'optimiser son rendement.

Source Smart Protection pour agents externes

Des agents externes, qui ne peuvent pas maintenir une connexion fonctionnelle avec le serveur Trend Micro Security (pour Mac), envoient des requêtes d'évaluation de réputation de sites Web au réseau Smart Protection Network. Une connexion Internet est requise pour assurer l'envoi de telles requêtes.

Accédez à l'écran Services de réputation de sites Web et activez la stratégie Réputation de sites Web pour les agents externes. Pour obtenir des instructions détaillées, consultez la rubrique *Configuration des paramètres de réputation de sites Web à la page 7-3*.

Source Smart Protection pour agents internes

Des agents internes, qui maintiennent une connexion fonctionnelle avec le serveur Trend Micro Security (pour Mac), peuvent envoyer des requêtes au serveur Smart Protection Server ou au réseau Smart Protection Network.

SOURCE	DÉTAILS
Serveurs Smart Protection Server	Configurez les serveurs Smart Protection Server en tant que source si vous avez des inquiétudes concernant la confidentialité et souhaitez conserver les requêtes d'évaluation de réputation de sites Web au sein du réseau de l'entreprise.

SOURCE	DÉTAILS
Smart Protection Network	Configurez le réseau Smart Protection Network en tant que source si vous ne disposez pas des ressources nécessaires pour configurer et gérer des serveurs Smart Protection Server.

Serveurs Smart Protection Server en tant que source pour agents internes

Lorsque cette option est sélectionnée, les agents Trend Micro Security (pour Mac) envoient des requêtes à des serveurs Smart Protection Server configurés pour des clients OfficeScan.

Cette option est uniquement disponible pour les versions 10.5 et ultérieures d'OfficeScan. OfficeScan 10, qui est pris en charge par cette version de Trend Micro Security (pour Mac), n'est pas compatible avec les serveurs Smart Protection Server fournissant des Services de réputation de sites Web.

Si votre serveur Trend Micro Security (pour Mac) est installé avec OfficeScan 10, mettez à niveau votre version d'OfficeScan vers la version 10.5 ou une version ultérieure. Si la mise à niveau d'OfficeScan est impossible, sélectionnez le réseau Smart Protection Network en tant que source.

Si votre version d'OfficeScan est la version 10.5 ou une version ultérieure, suivez les instructions ci-dessous afin de permettre aux agents d'envoyer correctement des requêtes aux serveurs Smart Protection Server :

1. Si ce n'est déjà fait, configurez l'environnement Smart Protection. Pour obtenir des instructions et des conseils sur la configuration de l'environnement, consultez les documents suivants :

   - Pour OfficeScan 10.5, consultez le chapitre 3 de la documentation, téléchargeable à l'adresse :

     http://docs.trendmicro.com/all/ent/officescan/v10.5/en-us/osce_10.5_gsg.pdf

   - Pour OfficeScan 10.6, consultez la page Web suivante :

     http://docs.trendmicro.com/all/ent/officescan/v10.6/fr-fr/osce_10.6_olhsrv/ohelp/smart/stusmps.htm

2. Sur la console Web su serveur Trend Micro Security (pour Mac), accédez à l'écran Paramètres de réputation de sites Web et activez l'option **Envoyer les requêtes aux Smart Protection Servers**. Pour obtenir des instructions détaillées, consultez la rubrique *Configuration des paramètres de réputation de sites Web à la page 7-3*.

Important

Cette option ne peut pas être activée si le serveur Trend Micro Security (pour Mac) est installé avec OfficeScan 10. Si cette option est activée depuis la gestion des stratégies de Control Manager, puis déployée sur un serveur Trend Micro Security (pour Mac) installé avec OfficeScan 10, ce paramètre ne prendra pas effet et l'option restera désactivée.

3. Assurez-vous que les Smart Protection Servers sont disponibles. Si tous les Smart Protection Servers sont indisponibles, les agents n'envoient pas de requêtes à Smart Protection Network, laissant ainsi les ordinateurs vulnérables aux menaces.

4. Veillez à mettre à jour régulièrement les Smart Protection Servers afin que cette protection reste actualisée.

Réseau Smart Protection Network en tant que source pour agents internes

Une connexion Internet est requise pour assurer l'envoi de requêtes au réseau Smart Protection Network.

Pour configurer le réseau Smart Protection Network en tant que source pour les agents internes, accédez à l'écran Services de réputation de sites Web et activez la stratégie Réputation de sites Web pour les agents internes. Assurez-vous de ne pas sélectionner l'option **Envoyer les requêtes aux Smart Protection Servers**. Pour obtenir des instructions détaillées, consultez la rubrique *Configuration des paramètres de réputation de sites Web à la page 7-3*.

Chapitre 4

Installation de l'agent

Ce chapitre décrit la configuration requise et les procédures d'installation de l'agent Trend Micro Security (pour Mac).

Pour plus de détails sur la mise à niveau de l'agent, consultez la rubrique *Mise à niveau du serveur et des agents à la page 8-2*.

Configuration minimale requise pour l'installation de l'agent

La configuration minimale suivante est requise pour l'installation de l'agent Trend Micro Security (pour Mac) sur un ordinateur Mac.

TABLEAU 4-1. Configuration minimale requise pour l'installation de l'agent

RESSOURCE	CONFIGURATION MINIMALE REQUISE
Système d'exploitation	• OS X™ Mountain Lion 10.8.3 ou version ultérieure • Mac OS X™ X Lion 10.7.5 ou version ultérieure • Mac OS X Snow Leopard™ 10.6.8 ou version ultérieure • Mac OS X Leopard™ 10.5.8 ou version ultérieure
Matériel	• **Processeur** : Intel™ • **Mémoire vive** : 256 Mo minimum • **Espace disque disponible** : 30 Mo minimum

Remarque

La version de ce produit ne prend plus en charge Mac OS X Tiger™ 10.4.11 et les processeurs PowerPC™. Si des agents sont installés sous Mac OS X Tiger et/ou s'exécutent depuis un processeur PowerPC, ne mettez pas à niveau ces agents et assurez vous qu'un serveur Trend Micro Security (pour Mac) 1.x peut gérer ces agents.

Méthodes et fichiers d'installation de l'agent

Il existe deux façons d'installer l'agent Trend Micro Security (pour Mac) :

- installation sur un seul ordinateur en lançant le pack d'installation (`tmsminstall.zip`) sur l'ordinateur Mac ;
- installation sur plusieurs ordinateurs en lançant le pack d'installation (`tmsminstall.mpkg.zip`) depuis Apple Remote Desktop.

Remarque

Pour mettre à niveau les agents, consultez la rubrique *Mise à niveau du serveur et des agents à la page 8-2*.

Récupérez le pack d'installation de l'agent nécessaire depuis le serveur Trend Micro Security (for Mac) et copiez-le sur l'ordinateur Mac.

Il existe deux façons de récupérer le pack :

- dans la console Web de Trend Micro Security (pour Mac), accédez à **Administration** > **Fichiers d'installation de l'agent**, puis cliquez sur un lien sous **Fichier d'installation de l'agent** ;

  Remarque

  les liens vers les packs d'installation de l'agent sont également disponibles sur cet écran. Utilisez ces packs pour supprimer le programme agent des ordinateurs Mac. Choisissez le pack en fonction de la version du programme agent que vous souhaitez supprimer. Pour plus d'informations sur la désinstallation de l'agent Trend Micro Security (pour Mac), consultez la rubrique *Désinstallation de l'agent à la page 4-14*.

- Accédez à <*Server installation folder*>`\TMSM_HTML\ClientInstall`.

Installation sur un seul ordinateur Mac

Le processus d'installation de l'agent Trend Micro Security (pour Mac) sur un seul ordinateur est semblable au processus d'installation des autres logiciels Mac.

Lors de l'installation, les utilisateurs peuvent être invités à autoriser les connexions à **iCoreService**, ce qui permet d'enregistrer l'agent auprès du serveur. Demandez aux utilisateurs d'autoriser la connexion lorsqu'ils y sont invités.

Procédure

1. Recherchez et désinstallez tous les logiciels de sécurité présents sur l'ordinateur Mac.
2. Récupérez le pack d'installation de l'agent `tmsminstall.zip`.

Pour plus d'informations sur l'obtention du pack, consultez la rubrique *Méthodes et fichiers d'installation de l'agent à la page 4-2*.

3. Copiez `tmsminstall.zip` sur l'ordinateur Mac puis lancez-le avec un outil d'archivage intégré tel qu'Utilitaire d'archive.

AVERTISSEMENT!

Les fichiers inclus à `tmsminstall.zip` peuvent être endommagés si les utilisateurs le lancent à l'aide d'outils d'archivage autres que ceux intégrés au Mac.

Pour lancer `tmsminstall.zip` depuis Terminal, utilisez la commande suivante :

```
ditto -xk <chemin d'accès au fichier tmsminstall.zip>
<dossier de destination>
```

Par exemple :

```
ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/Desktop
```

Cette opération permet de créer un nouveau dossier `tmsminstall`.

4. Ouvrez le dossier `tmsminstall` et lancez `tmsminstall.pkg`.

5. Lorsqu'un message vous invite à poursuivre l'installation, cliquez sur **Continuer**.

6. Dans l'écran Introduction, cliquez sur **Continuer** pour poursuivre.

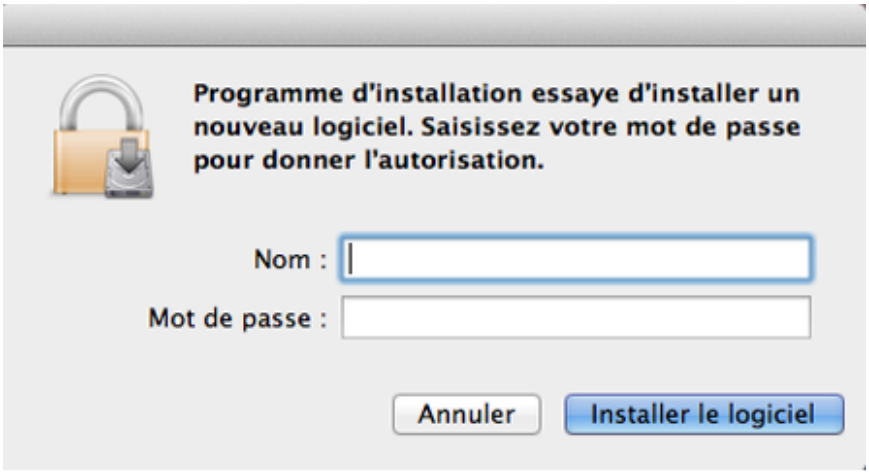
7. Consultez les rappels et cliquez sur **Continuer**.

8. Dans l'écran Type d'installation, cliquez sur **Installer**.

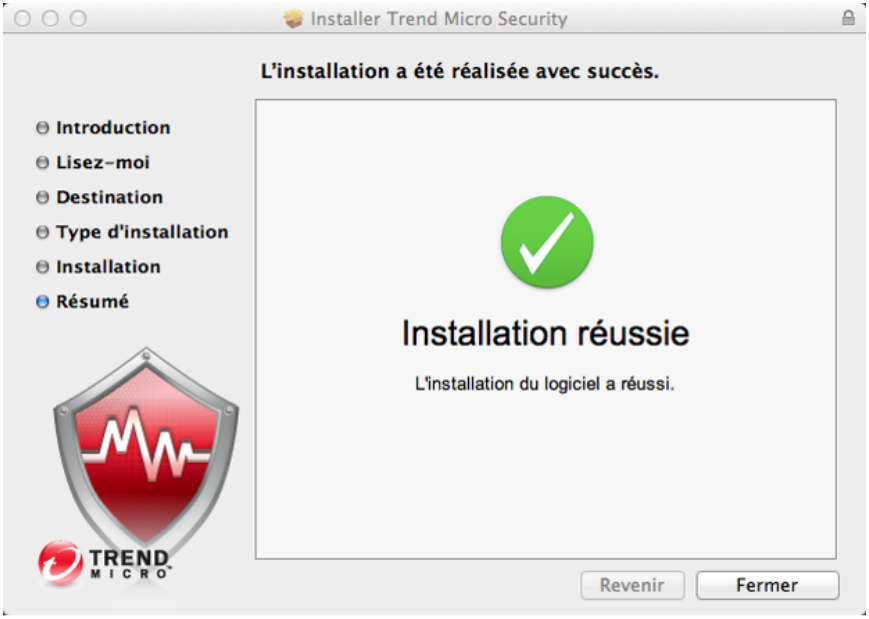
9. Renseignez les champs **Nom** et **Mot de passe** pour commencer le processus d'installation.

Remarque

Spécifiez le nom et le mot de passe d'un compte disposant de droits d'administration sur l'ordinateur Mac.



10. Si l'installation s'est correctement déroulée, cliquez sur **Fermer** pour terminer le processus d'installation.



L'agent s'enregistre automatiquement auprès du serveur à partir duquel le pack d'installation de l'agent a été obtenu. L'agent se met également à jour pour la première fois.

Que faire ensuite

Passez aux tâches à effectuer après l'installation de l'agent. Pour obtenir des informations détaillées, consultez la rubrique *Après l'installation de l'agent à la page 4-12*.

Installation sur plusieurs ordinateurs Mac

Le processus d'installation de l'agent Trend Micro Security (pour Mac) sur plusieurs ordinateurs peut être simplifié via Apple Remote Desktop.

Remarque

Si les ordinateurs Mac ne disposent que d'une adresse IPv6, consultez les limitations IPv6 pour le déploiement de l'agent Apple Remote Desktop dans *Limitations pour agent en IPv6 pur à la page A-3*.

Procédure

1. Recherchez et désinstallez tous les logiciels de sécurité présents sur l'ordinateur Mac.
2. Obtenez le pack d'installation de l'agent `tmsminstall.mpkg.zip`. Pour plus d'informations sur l'obtention du pack, consultez la rubrique *Méthodes et fichiers d'installation de l'agent à la page 4-2*.
3. Copiez `tmsminstall.mpkg.zip` sur l'ordinateur Mac avec Apple Remote Desktop puis lancez-le avec un outil d'archivage intégré tel qu'Utilitaire d'archive.

AVERTISSEMENT!

Les fichiers inclus à l'archive `tmsminstall.mpkg.zip` peuvent être endommagés si les utilisateurs le lancent à l'aide d'outils d'archivage autres que ceux intégrés au Mac.

Pour lancer `tmsminstall.mpkg.zip` depuis Terminal, utilisez la commande suivante :

```
ditto -xk <chemin d'accès au fichier tmsminstall.mpkg.zip>
<dossier de destination>
```

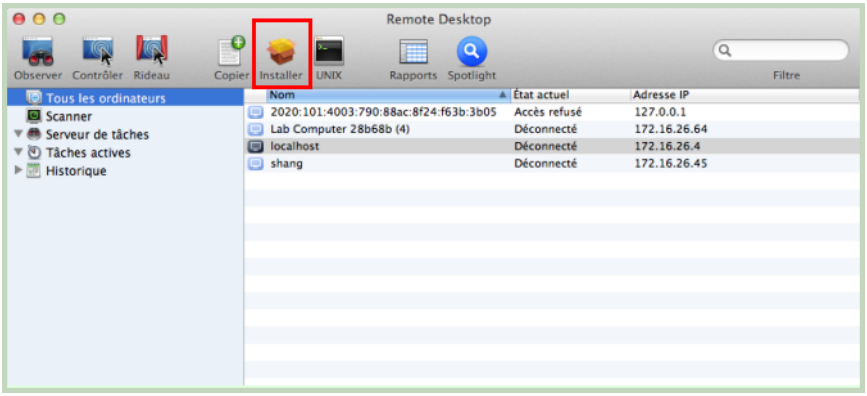
Par exemple :

```
ditto -xk users/mac/Desktop/tmsminstall.mpkg.zip users/mac/
Desktop
```

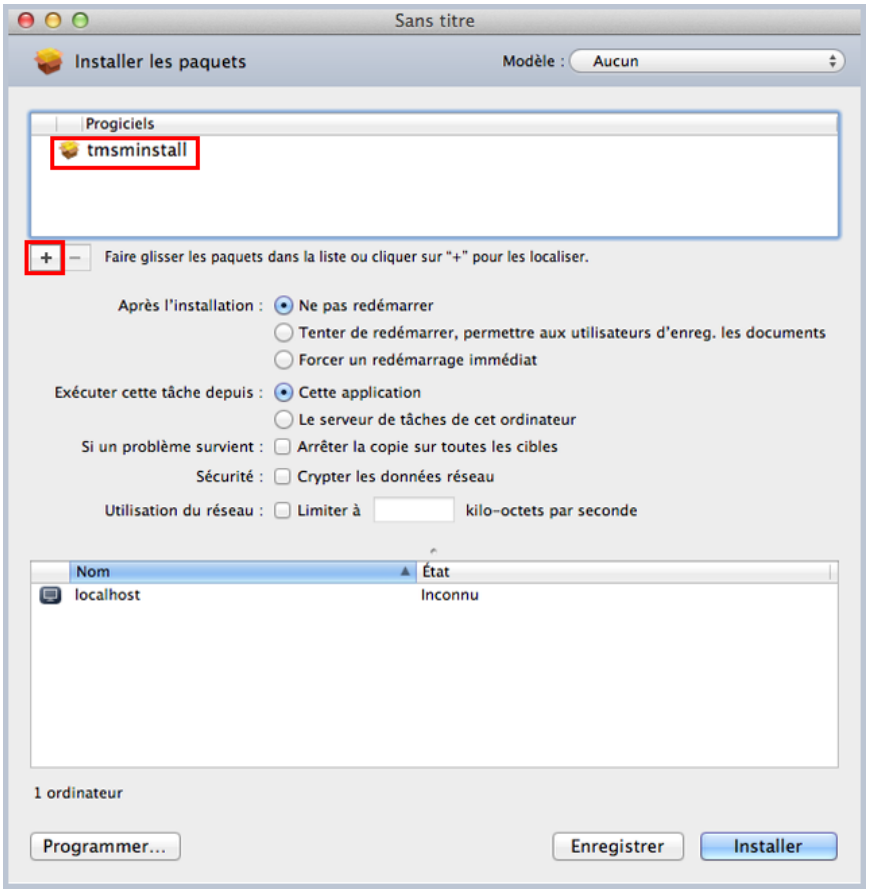
Cette opération permet d'extraire le fichier `tmsminstall.mpkg`.

4. Ouvrez Apple Remote Desktop sur l'ordinateur Mac.

5. Sélectionnez les ordinateurs vers lesquels installer l'agent Trend Micro Security (pour Mac), puis cliquez sur **Installer**.



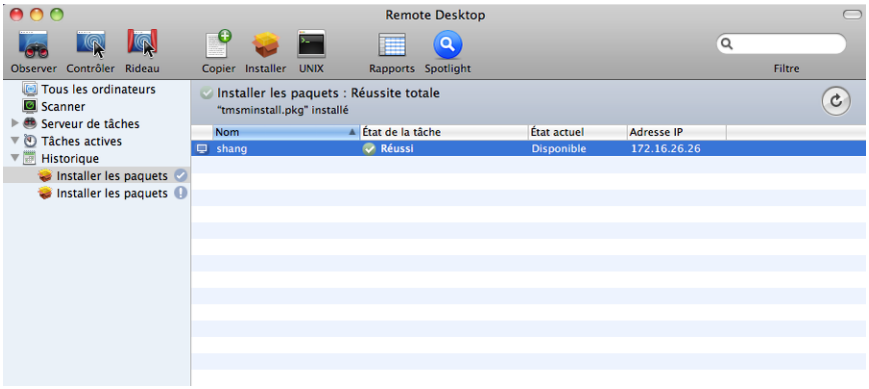
6. Dans l'écran Installer les paquets, faites glisser le pack d'installation ou cliquez sur « + » pour le localiser.



7. (Facultatif) Cliquez sur **Enregistrer** pour exécuter automatiquement la tâche d'installation sur les nouveaux ordinateurs Mac connectés au réseau.

8. Cliquez sur **Installer**.

   Apple Remote Desktop commence l'installation de l'agent sur les ordinateurs sélectionnés. Si l'installation s'est déroulée correctement sur tous les ordinateurs, le message `Installer les paquets : Réussite totale` s'affiche. Sinon, `Réussite` s'affiche sous **État de la tâche** pour chaque ordinateur sur lequel l'installation a abouti.



Les agents s'enregistrent automatiquement auprès du serveur à partir duquel le pack d'installation de l'agent a été obtenu. Ils se mettent également à jour pour la première fois.

Que faire ensuite

Passez aux tâches à effectuer après l'installation de l'agent. Pour obtenir des informations détaillées, consultez la rubrique *Après l'installation de l'agent à la page 4-12*.

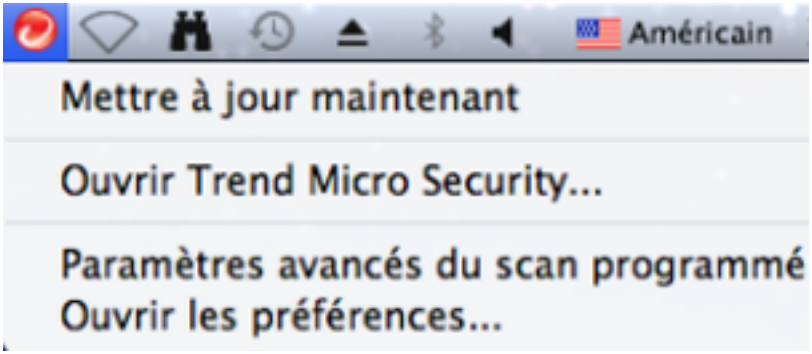
Après l'installation de l'agent

Procédure

1. Vérifiez ce qui suit :

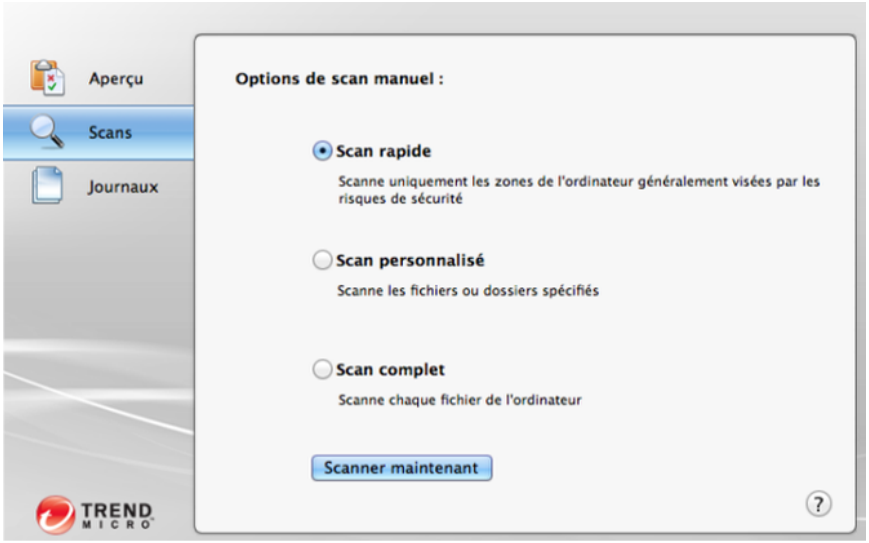
   - L'icône ( ) de l'agent Trend Micro Security (pour Mac) s'affiche dans la barre de menus de l'ordinateur Mac.
   - Les fichiers de l'agent Trend Micro Security (pour Mac) figurent sous le <*dossier d'installation de l'agent*>.
   - L'agent s'affiche dans l'arborescence agent de la console Web. Pour accéder à l'arborescence agent, cliquez sur **Gestion des agents** dans le menu principal.

2. Mise à jour des composants de Trend Micro Security (pour Mac). Le client télécharge les composants à partir du serveur Trend Micro Security (pour Mac). Consultez la rubrique *Mises à jour des agents à la page 5-8* pour obtenir des informations détaillées.



Si l'agent ne peut pas se connecter au serveur, il télécharge les mises à jour directement à partir du serveur ActiveUpdate de Trend Micro. Une connexion Internet est requise pour accéder au serveur ActiveUpdate.

3. Lancez l'opération Scanner maintenant sur l'ordinateur Mac ou demandez à l'utilisateur d'exécuter un scan manuel.



Que faire ensuite

Si des problèmes avec l'agent surviennent après l'installation, essayez de le désinstaller puis de le réinstaller.

Désinstallation de l'agent

Désinstallez le programme agent uniquement si vous rencontrez des problèmes avec lui. Réinstallez-le immédiatement pour que l'ordinateur soit protégé contre les risques de sécurité.

Procédure

1. Obtenez le pack de désinstallation de l'agent (`tmsmuninstall.zip`) du serveur Trend Micro Security (pour Mac). Dans la console Web de Trend Micro Security (pour Mac), accédez à **Administration** > **Fichiers d'installation du client**, puis cliquez sur le lien sous **Fichier de désinstallation de l'agent**.
2. Copiez et lancez le pack sur l'ordinateur Mac.

3. Renseignez les champs **Nom** et **Mot de passe** pour commencer le processus de désinstallation.

Remarque

Spécifiez le nom et le mot de passe d'un compte disposant de droits d'administration sur l'ordinateur Mac.

4. Si la désinstallation s'est déroulée correctement, cliquez sur **Fermer** pour terminer le processus de désinstallation.

Que faire ensuite

Annulez l'enregistrement de l'agent auprès du serveur.

1. Dans la console Web, cliquez sur **Gestion des agents**, puis sélectionnez l'agent qui a été désinstallé.
2. Cliquez sur **Gérer l'arborescence agent** > **Supprimer groupe/agent**.

Chapitre 5

Mise à jour de la protection

Ce chapitre décrit les composants et les procédures de mise à jour de Trend Micro Security (pour Mac).

Composants

Les composants permettent de protéger les ordinateurs agents contre les risques de sécurité les plus récents. Pour les mettre à jour, exécutez des mises à jour manuelles ou programmées.

Outre ces composants, les agents Trend Micro Security (pour Mac) reçoivent également des fichiers de configuration mis à jour du serveur Trend Micro Security (pour Mac), qui leur permettent d'appliquer de nouveaux paramètres. À chaque fois que vous modifiez les paramètres de Trend Micro Security (pour Mac) via la console Web, les fichiers de configuration sont modifiés.

Signatures de virus

Le fichier de signatures de virus contiennent des informations qui permettent à Trend Micro Security (pour Mac) d'identifier les virus/programmes malveillants les plus récents et les attaques mixtes. Trend Micro crée et publie de nouvelles versions des signatures de virus plusieurs fois par semaine et chaque fois qu'un virus/programme malveillant particulièrement ravageur est détecté.

Signatures de surveillance active des spywares

Les signatures de surveillance active des spywares contiennent des informations qui permettent à Trend Micro Security (pour Mac) d'identifier les programmes espions et les graywares.

Moteur de scan antivirus

Initialement développé pour faire face aux premiers virus de fichier, le moteur de scan est la partie centrale de tous les produits Trend Micro. Il est devenu un outil exceptionnellement sophistiqué et capable de détecter différents types de risques de sécurité, notamment les programmes espions. Il détecte également les virus contrôlés qui sont développés et utilisés à des fins de recherche.

Mise à jour du moteur de scan

Grâce à l'enregistrement des informations à durée de vie critique dans les fichiers de signatures, Trend Micro minimise le nombre de mises à jour du moteur de scan, tout en maintenant la protection à jour. Néanmoins, Trend Micro met régulièrement à disposition de nouvelles versions du moteur de scan, notamment dans les circonstances suivantes :

- Intégration de nouvelles technologies de scan et de détection au logiciel
- Découverte d'un nouveau risque de sécurité potentiellement dangereux que le moteur de scan n'est pas capable de traiter
- Optimisation des performances du scan
- Ajout de formats de fichiers, de langages de script, de formats de chiffrement et/ou de compression

Programme agent

Le programme agent Trend Micro Security (pour Mac) offre une protection effective contre les risques de sécurité.

Présentation des mises à jour

Toutes les mises à jour des composants proviennent du serveur Trend Micro ActiveUpdate. Lorsque des mises à jour sont disponibles, le serveur Trend Micro Security (pour Mac) télécharge les composants mis à jour.

Vous pouvez configurer le serveur Trend Micro Security (pour Mac) pour qu'il soit mis à jour à partir d'une source autre que le serveur Trend Micro ActiveUpdate. Pour ce faire, vous devez configurer une source de mise à jour personnalisée. Pour obtenir de l'aide au sujet de la configuration de celle-ci, contactez votre fournisseur d'assistance.

Le tableau suivant décrit les différentes options de mise à jour des composants pour le serveur et les agents Trend Micro Security (pour Mac) :

TABLEAU 5-1. Options de mise à jour serveur-agents

OPTION DE MISE À JOUR	DESCRIPTION
Serveur ActiveUpdate  Serveur Trend Micro Security (pour Mac)  Agents	Le serveur Trend Micro Security (pour Mac) reçoit les composants mis à jour à partir du serveur Trend Micro ActiveUpdate (ou d'une autre source de mise à jour si une source personnalisée a été configurée), puis les déploie sur les agents.
Serveur ActiveUpdate  Agents	Les agents Trend Micro Security (pour Mac) reçoivent les composants mis à jour directement du serveur ActiveUpdate s'ils ne peuvent pas se connecter au serveur Trend Micro Security (pour Mac).

Mise à jour du serveur

Le serveur Trend Micro Security (pour Mac) télécharge les composants suivants avant de les déployer sur les agents :

- Signatures de virus
- Signatures de surveillance active des spywares
- Moteur de scan antivirus

Affichez les versions actuelles des composants sur l'écran Résumé de la console Web, puis déterminez le nombre d'agents contenant des composants mis à jour et obsolètes.

Si vous utilisez un serveur proxy pour vous connecter à Internet, utilisez les paramètres proxy appropriés pour réussir le téléchargement des mises à jour.

Configuration de la source de mise à jour du serveur

Configurez le serveur Trend Micro Security (pour Mac) pour qu'il télécharge les composants à partir du serveur Trend Micro ActiveUpdate ou d'une autre source.

Remarque

Si le serveur dispose uniquement d'une adresse IPv6, consultez les limitations relatives mises à jour du serveur liées à IPv6 à la rubrique *Limitations pour serveur en IPv6 pur à la page A-3*.

Une fois que le serveur a téléchargé les mises à jour disponibles, il avertit automatiquement les agents afin que ceux-ci mettent à jour leurs composants. Si cette mise à jour s'avère capitale, faites en sorte que le serveur envoie une notification immédiate aux agents en accédant à **Gestion des agents** > **Tâches** > **Mise à jour**.

Procédure

1. Accédez à **Mises à jour du serveur** > **Source de mise à jour**.
2. Sélectionnez l'emplacement à partir duquel vous souhaitez télécharger les mises à jour de composants.
   - Si vous choisissez le serveur ActiveUpdate :
     - Assurez-vous que le serveur Trend Micro Security (pour Mac) dispose d'une connexion à Internet.
     - Si vous utilisez un serveur proxy, testez l'établissement de la connexion à Internet à l'aide des paramètres proxy. Pour obtenir des informations détaillées, consultez la rubrique *Configuration des paramètres proxy pour les mises à jour du serveur à la page 5-6*.
   - Si vous avez choisi une source de mise à jour personnalisée :
     - Configurez l'environnement et les ressources de mise à jour appropriées pour cette source de mise à jour.
     - Assurez-vous qu'il existe une connexion opérationnelle entre le serveur et cette source de mise à jour. Pour obtenir de l'aide au sujet de la

configuration d'une source de mise à jour, contactez votre fournisseur d'assistance.

- Vous pouvez obtenir des mises à jour depuis Control Manager en saisissant son adresse HTTP.

3. Cliquez sur **Enregistrer**.

Configuration des paramètres proxy pour les mises à jour du serveur

Configurez le serveur Trend Micro Security (pour Mac) afin qu'il utilise des paramètres proxy lors du téléchargement de mises à jour à partir du serveur Trend Micro ActiveUpdate.

Remarque

Si le serveur dispose uniquement d'une adresse IPv6, consultez les limitations relatives aux paramètres proxy liées à IPv6 à la rubrique *Limitations pour serveur en IPv6 pur à la page A-3*.

Procédure

1. Accédez à **Administration** > **Paramètres de proxy externe**.
2. Cochez la case pour permettre l'utilisation d'un serveur proxy.
3. Indiquez le nom ou l'adresse IPc4/IPv6 du serveur proxy, ainsi que le numéro de port.
4. Si le serveur proxy requiert une authentification, saisissez le nom d'utilisateur et le mot de passe dans les champs prévus à cet effet.
5. Cliquez sur **Enregistrer**.

Méthodes de mise à jour du serveur

Mettez à jour les composants du serveur Trend Micro Security (pour Mac) manuellement ou en configurant une mise à jour programmée.

- **Mise à jour manuelle** : Lorsqu'une mise à jour est capitale, effectuez-la de façon manuelle afin que le serveur puisse obtenir les mises à jour immédiatement. Consultez la rubrique *Mise à jour manuelle du serveur à la page 5-8* pour obtenir des informations détaillées.
- **Mise à jour programmée** : Le serveur Trend Micro Security (pour Mac) se connecte à la source de mise à jour aux jour et heure programmés pour obtenir les composants les plus récents. Consultez la rubrique *Programmation des mises à jour du serveur à la page 5-7* pour obtenir des informations détaillées.

Une fois que le serveur a terminé une mise à jour, il notifie immédiatement les agents afin que ceux-ci procèdent également à la mise à jour.

Programmation des mises à jour du serveur

Configurez le serveur Trend Micro Security (pour Mac) afin qu'il vérifie régulièrement la source de mise à jour et télécharge automatiquement les mises à jour disponibles. La mise à jour programmée est un moyen simple et efficace de garantir que votre protection contre les risques de sécurité est mise à jour en permanence.

Une fois que le serveur a terminé une mise à jour, il notifie les agents afin que ceux-ci procèdent également à la mise à jour.

Procédure

1. Accédez à **Mises à jour du serveur** > **Mise à jour programmée**.
2. Sélectionnez les composants à mettre à jour.
3. Programmez les mises à jour.

   Pour des mises à jour quotidiennes, hebdomadaires et mensuelles, la période correspond au nombre d'heures pendant lesquelles Trend Micro Security (pour Mac) exécute la mise à jour. Trend Micro Security (pour Mac) procède à la mise à jour à tout moment pendant cette période.

Si vous avez sélectionné le 29, le 30 ou le 31 pour les mises à jour mensuelles, Trend Micro Security (pour Mac) exécute la mise à jour le dernier jour du mois lorsque le mois est plus court.

4. Cliquez sur **Enregistrer**.

Mise à jour manuelle du serveur

Mettez à jour manuellement les composants sur le serveur Trend Micro Security (pour Mac) après l'installation ou la mise à niveau du serveur et à l'occasion d'une épidémie.

Procédure

1. Accédez à **Mises à jour du serveur** > **Mise à jour manuelle**.
2. Sélectionnez les composants à mettre à jour.
3. Cliquez sur **Mise à jour**.

   Le serveur télécharge les composants mis à jour.

   Une fois que le serveur a terminé une mise à jour, il notifie immédiatement les agents afin que ceux-ci procèdent également à la mise à jour.

Mises à jour des agents

Pour garantir le maintien de la protection des agents contre les risques de sécurité les plus récents, procédez à une mise à jour régulière des composants des agents, notamment lorsque les agents possèdent des composants particulièrement obsolètes, ainsi qu'à l'occasion d'une épidémie. Les composants deviennent particulièrement obsolètes lorsque l'agent ne parvient pas à les mettre à jour à partir du serveur Trend Micro Security (pour Mac) ou du serveur ActiveUpdate pendant une période prolongée.

Méthodes de mise à jour des agents

Il existe plusieurs méthodes de mise à jour des agents.

MÉTHODE DE MISE À JOUR	DESCRIPTION
Mise à jour manuelle lancée par un administrateur	Lancez une mise à jour à partie de l'un des écrans de la console Web suivants : • écran Gestion des agents. Pour obtenir des informations détaillées, consultez la rubrique *Lancement de la mise à jour des agents à partir de l'écran Gestion des agents à la page 5-12*. • écran Résumé. Pour obtenir des informations détaillées, consultez la rubrique *Lancement de la mise à jour des agents à partir de l'écran Résumé à la page 5-12*.
Mise à jour automatique	• Une fois que le serveur a terminé une mise à jour, il notifie immédiatement les agents afin que ceux-ci procèdent également à la mise à jour. • Les mises à jour peuvent être effectuées selon une programmation configurée par vos soins. Vous pouvez configurer et appliquer une programmation concernant un ou plusieurs agents et domaines, ou bien tous les agents gérés par le serveur. Pour obtenir des informations détaillées, consultez la rubrique *Configuration des paramètres de mise à jour des agents à la page 5-10*.
Mise à jour manuelle lancée par un utilisateur	Les utilisateurs lancent la mise à jour à partir de leurs ordinateurs Mac.

Source de mise à jour des agents

Par défaut, les agents téléchargent des composants à partir du serveur Trend Micro Security (pour Mac). Outre ces composants, les agents Trend Micro Security (pour Mac) reçoivent également des fichiers de configuration mis à jour lors des mises à jour effectuées à partir du Trend Micro Security (pour Mac), qui leur permettent d'appliquer de nouveaux paramètres. À chaque fois que vous modifiez les paramètres de Trend Micro Security (pour Mac) sur la console Web, les fichiers de configuration sont modifiés.

Avant de mettre à jour les agents, vérifiez que le serveur Trend Micro Security (pour Mac) dispose des composants les plus récents. Pour plus d'informations sur la façon de mettre à jour le serveur Trend Micro Security (pour Mac), consultez la rubrique *Mise à jour du serveur à la page 5-4*.

Configurez un agent, plusieurs d'entre eux ou l'ensemble des agents afin qu'ils effectuent des téléchargements à partir du serveur Trend Micro ActiveUpdate lorsque le serveur Trend Micro Security (pour Mac) est indisponible. Pour obtenir des informations détaillées, consultez la rubrique *Configuration des paramètres de mise à jour des agents à la page 5-10*.

Remarque

Si un agent dispose uniquement d'une adresse IPv6, consultez les limitations relatives à la mise à jour des agents liées à IPv6 à la rubrique *Limitations pour agent en IPv6 pur à la page A-3*.

Remarques et rappels relatifs à la mise à jour des agents

- Les agents Trend Micro Security (pour Mac) peuvent utiliser des paramètres proxy lors d'une mise à jour. Ceux-ci sont configurés sur la console de l'agent.
- Lors d'une mise à jour, l'icône Trend Micro Security (pour Mac) de la barre des menus de l'ordinateur Mac indique que le produit est en cours de mise à jour. Si une mise à niveau du programme de l'agent est disponible, les agents procèdent à une mise à jour, puis à une mise à niveau vers la version du programme la plus récente. Les utilisateurs ne peuvent pas exécuter de tâches à partir de la console avant la fin de la mise à jour.
- Accédez à l'écran Résumé pour vérifier que tous les agents ont été mis à jour.

Configuration des paramètres de mise à jour des agents

Pour obtenir des explications détaillées sur les mises à jour des agents, consultez la rubrique *Mises à jour des agents à la page 5-8*.

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine () afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de mise à jour**.

4. Cochez la case pour permettre aux agents de télécharger les mises à jour à partir du serveur Trend Micro ActiveUpdate.

Remarque

Si un agent dispose uniquement d'une adresse IPv6, consultez les limitations relatives à la mise à jour des agents liées à IPv6 à la rubrique *Limitations pour agent en IPv6 pur à la page A-3*.

---

5. Configurez des mises à jour programmées.

   a. Sélectionnez **Activer la mise à jour programmée**.

   b. Configurez la programmation.

   c. Si vous sélectionnez **Quotidienne** ou **Hebdomadaire**, indiquez le moment de la mise à jour et la période pendant laquelle le serveur Trend Micro Security (pour Mac) notifie les agents de la nécessité de mise à jour de composants. Par exemple, si l'heure de début est midi et que la période est de 2 heures, le serveur notifie de manière aléatoire tous les agents en ligne afin qu'ils mettent à jour leurs composants entre midi et 14 h. Ce paramètre évite que tous les agents en ligne se connectent simultanément au serveur à l'heure de début indiquée, ce qui réduit considérablement le trafic en direction du serveur.

6. Si vous avez sélectionné des groupes ou des agents dans l'arborescence des agents, cliquez sur **Enregistrer** pour appliquer les paramètres aux groupes ou aux agents. Si vous avez sélectionné l'icône racine (), choisissez l'une des options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un groupe existant/futur. Les groupes futurs sont des groupes qui ne sont pas encore créés au moment de la configuration des paramètres.

   - **Appliquer aux groupes futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux groupes futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un groupe existant.

Lancement de la mise à jour des agents à partir de l'écran Résumé

Consultez la rubrique *Mises à jour des agents à la page 5-8* pour découvrir les autres méthodes de mise à niveau des agents.

Procédure

1. Dans le menu principal, cliquez sur **Résumé**.
2. Accédez à la section **État de la mise à jour** et cliquez sur le lien qui se trouve sous la colonne **Plus à jour**.

   L'arborescence des agents s'ouvre et affiche tous les agents nécessitant une mise à jour.
3. Sélectionnez les agents que vous souhaitez mettre à jour.
4. Cliquez sur **Tâches** > **Mise à jour**.

   Les agents recevant la notification commencent à se mettre à jour. Sur les ordinateurs Mac, l'icône Trend Micro Security (pour Mac) de la barre des menus indique que le produit est en cours de mise à jour. Les utilisateurs ne peuvent pas exécuter de tâches à partir de la console avant la fin de la mise à jour.

Lancement de la mise à jour des agents à partir de l'écran Gestion des agents

Consultez la rubrique *Mises à jour des agents à la page 5-8* pour découvrir les autres méthodes de mise à niveau des agents.

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine du domaine () afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.

3. Cliquez sur **Tâches** > **Mise à jour**.

   Les agents recevant la notification commencent à se mettre à jour. Sur les ordinateurs Mac, l'icône Trend Micro Security (pour Mac) de la barre des menus indique que le produit est en cours de mise à jour. Les utilisateurs ne peuvent pas exécuter de tâches à partir de la console avant la fin de la mise à jour.

Chapitre 6

Protection des ordinateurs Mac contre les risques de sécurité

Ce chapitre décrit comment protéger vos ordinateurs des risques de sécurité à l'aide de scans basés sur des fichiers.

À propos des risques de sécurité

Les virus, les programmes malveillants, les programmes espions et les graywares représentent des risques de sécurité. Trend Micro Security (pour Mac) protège les ordinateurs des risques de sécurité en scannant les fichiers, puis en effectuant une action spécifique pour chaque risque de sécurité détecté. Un nombre important de risques de sécurité détectés sur une courte période signale une épidémie. Pour la contenir, Trend Micro Security (pour Mac) applique des stratégies de prévention d'épidémie et isole les ordinateurs infectés jusqu'à ce qu'ils soient inoffensifs. Les notifications et les journaux vous permettent de suivre les risques de sécurité et vous alertent lorsque vous devez effectuer une action immédiate.

Virus et programmes malveillants

Il existe des dizaines de milliers de virus/programmes malveillants et de nouveaux sont créés chaque jour. Les virus informatiques de notre époque peuvent provoquer des dommages importants en exploitant les failles de sécurité des réseaux d'entreprise, des systèmes de messagerie électronique et des sites Web.

Trend Micro Security (pour Mac) protège les ordinateurs contre les types de virus/programmes malveillants suivants :

TYPES DE VIRUS/ PROGRAMMES MALVEILLANTS	DESCRIPTION
Programme canular	Un programme canular est un programme similaire à un virus, qui manipule souvent l'apparence des éléments affichés sur l'écran d'un ordinateur.
cheval de Troie	Un cheval de Troie est un programme exécutable qui ne se multiplie pas mais recourt à des ordinateurs pour effectuer des opérations malveillantes telles que l'ouverture des ports aux pirates. Un tel programme utilise souvent des ports ouverts par des chevaux de Troie pour accéder à des ordinateurs. Sous prétexte d'éradiquer des virus sur un ordinateur, les chevaux de Troie peuvent par exemple y introduire de nouveaux virus.

TYPES DE VIRUS/ PROGRAMMES MALVEILLANTS	DESCRIPTION
Virus	Un virus est un programme qui se réplique. Pour ce faire, le virus doit s'attacher à d'autres fichiers programmes et s'exécuter chaque fois que le programme hôte est lancé. • **Virus du secteur d'amorçage** : virus qui infecte le secteur d'amorçage d'une partition ou d'un disque. • **Code malveillant Java** : virus indépendant du système d'exploitation écrit ou incorporé dans Java • **Virus de macro** : virus chiffré comme application macro qui est souvent inclus dans un document • **Virus VBScript, JavaScript ou HTML** : virus qui réside sur des pages Web et est téléchargé via un navigateur. • **Ver** : programme automatique ou ensemble de programmes qui peut répandre des copies fonctionnelles de lui-même ou de ses segments dans d'autres ordinateurs, souvent par e-mail
Virus de test :	Un virus de test est un fichier inerte pouvant être détecté par les logiciels antivirus. Utilisez des virus de test, tels que le script de test EICAR, afin de vérifier que le scan de l'installation antivirus fonctionne correctement.
Utilitaire de compression	Les utilitaires de compression sont des programmes exécutables compressés et/ou chiffrés Windows ou Linux™, souvent sous forme de cheval de Troie. La compression de fichiers exécutables rend les utilitaires de compression plus difficiles à détecter par les logiciels antivirus.
Virus/programmes malveillants potentiels	Les fichiers suspects ayant certaines des caractéristiques d'un virus/programme malveillant sont classés sous ce type de virus/ programme malveillant. Pour obtenir des informations détaillées sur les virus/programmes malveillants potentiels, consultez la page suivante de l'Encyclopédie des virus en ligne de Trend Micro : http://www.trendmicro.com/vinfo/fr/virusencyclo/default.asp

Types de virus/ programmes malveillants	Description
Autres	« Autres » inclut les virus/programmes malveillants n'entrant dans aucune des catégories de types de virus/programmes malveillants.

Programmes espions et graywares

Les termes « grayware » et « programmes espions » se rapportent aux applications ou aux fichiers non classés en tant que virus ou programmes malveillants mais qui peuvent toutefois avoir un effet négatif sur les performances des ordinateurs de votre réseau. Les programmes espions et les graywares font courir à votre entreprise un risque significatif en termes de sécurité, de confidentialité et en termes juridiques. Ils réalisent souvent des actions variées non souhaitées et menaçantes qui irritent les utilisateurs avec des fenêtres pop-up, enregistrent les séquences de frappe des touches du clavier et exposent les failles de l'ordinateur à des attaques.

Trend Micro Security (pour Mac) protège les ordinateurs contre les types de programmes espions/graywares suivants :

Types de programmes espions/graywares	Description
Programme espion	Les programmes espions récoltent des données, telles que des noms d'utilisateur de compte, de mots de passe, des numéros de cartes de crédit et d'autres informations confidentielles pour les transmettre à des tiers.
Adware	Les adwares affichent des publicités et récoltent des données, telles que des préférences de navigation, pouvant être utilisées à des fins publicitaires.

Types de programmes espions/graywares	Description
Composeur de numéros	Un composeur de numéros modifie les paramètres Internet et oblige un ordinateur à composer des numéros de téléphone préconfigurés à l'aide d'un modem. Ce sont souvent des numéros de services téléphoniques facturés à l'utilisation (pay-per-call) ou internationaux qui peuvent entraîner une dépense significative pour votre entreprise.
Outil de piratage	Un outil de piratage aide les pirates informatiques à s'infiltrer dans les ordinateurs.
Outil d'accès à distance	Un outil d'accès à distance permet aux pirates de s'infiltrer et de contrôler un ordinateur à distance.
Application de craquage de mots de passe	Ce type d'application aide à déchiffrer des noms d'utilisateurs et des mots de passe.
Autres	« Autres » inclut les programmes malveillants potentiels n'entrant dans aucune des catégories de types de programmes espions/graywares.

Types de scans

Trend Micro Security (pour Mac) fournit les types de scans suivants pour protéger les ordinateurs Mac contre les risques de sécurité :

Type de scan	Description
Scan en temps réel	Scanne automatiquement un fichier reçu, ouvert, téléchargé, copié ou modifié Consultez la rubrique *Scan en temps réel à la page 6-6*.
Scan manuel	Lancé par l'utilisateur : scanne un fichier ou un ensemble de fichiers Consultez la rubrique *Scan manuel à la page 6-7*.

TYPE DE SCAN	DESCRIPTION
Scan programmé	Scanne automatiquement les fichiers de l'ordinateur en fonction de la programmation configurée par l'administrateur Consultez la rubrique *Scan programmé à la page 6-8*.
Scanner maintenant	Lancé par l'administrateur : scanne les fichiers sur un ou plusieurs ordinateurs cibles Consultez la rubrique *Scanner maintenant à la page 6-9*.

Scan en temps réel

Le scan en temps réel s'effectue en continu. À chaque réception, ouverture, téléchargement, copie ou modification d'un fichier, le scan en temps réel recherche les risques de sécurité dans le fichier. Si Trend Micro Security (pour Mac) ne détecte aucun risque de sécurité, le fichier est conservé au même emplacement et reste accessible. Si un risque de sécurité est détecté, Trend Micro Security (pour Mac) affiche un message de notification indiquant le nom du fichier infecté et le risque spécifique lié à la sécurité.

Configurez et appliquez les paramètres de scan en temps réel à un ou plusieurs agents et groupes, ou à tous les agents gérés par le serveur.

Configuration des paramètres de scan en temps réel

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine ( ) afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de scan en temps réel**.
4. Configurez les critères de scan suivants :
   - *Action des utilisateurs sur les fichiers à la page 6-11*
   - *Paramètres de scan à la page 6-12*

5. Cliquez sur l'onglet **Action** pour configurer les actions de scan que Trend Micro Security (pour Mac) effectue sur les risques de sécurité détectés. Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Options d'action de scan et paramètres supplémentaires à la page 6-15*.

6. Si vous avez sélectionné des groupes ou des agents dans l'arborescence des agents, cliquez sur **Enregistrer** pour appliquer les paramètres aux groupes ou aux agents. Si vous avez sélectionné l'icône racine (), choisissez l'une des options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un groupe existant/futur. Les groupes futurs sont des groupes qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux groupes futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux groupes futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un groupe existant.

Scan manuel

Le scan manuel est un scan à la demande qui démarre immédiatement après avoir été lancé dans la console de l'agent. Sa durée dépend du nombre de fichiers spécifiés et des ressources matérielles de l'ordinateur Mac.

Configurez et appliquez les paramètres de scan manuel à un ou plusieurs agents et groupes, ou à tous les agents gérés par le serveur.

Configuration des paramètres de scan manuel

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine () afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de scan manuel**.

4. Configurez les critères de scan suivants :
   - *Paramètres de scan à la page 6-12*
   - *Utilisation du processeur à la page 6-13*
5. Cliquez sur l'onglet **Action** pour configurer les actions de scan que Trend Micro Security (pour Mac) effectue sur les risques de sécurité détectés. Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Options d'action de scan et paramètres supplémentaires à la page 6-15*.
6. Si vous avez sélectionné des groupes ou des agents dans l'arborescence des agents, cliquez sur **Enregistrer** pour appliquer les paramètres aux groupes ou aux agents. Si vous avez sélectionné l'icône racine (), choisissez l'une des options suivantes :
   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un groupe existant/futur. Les groupes futurs sont des groupes qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux groupes futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux groupes futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un groupe existant.

Scan programmé

Le scan programmé démarre automatiquement aux date et heure programmées. Il permet d'automatiser les scans de routine sur l'agent et d'améliorer l'efficacité de votre gestion des scans.

Configurez et appliquez les paramètres de scan programmé à un ou plusieurs clients agents et groupes, ou à tous les agents gérés par le serveur.

Configuration des paramètres de scan programmé

Procédure

1. Accédez à **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône de la racine () afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de scan programmé**.
4. Cochez la case pour activer le scan programmé.
5. Configurez les critères de scan suivants :
   - *Programmation à la page 6-13*
   - *Cible du scan à la page 6-11*
   - *Paramètres de scan à la page 6-12*
   - *Utilisation du processeur à la page 6-13*
6. Cliquez sur l'onglet **Action** pour configurer les actions de scan que Trend Micro Security (pour Mac) effectue sur les risques de sécurité détectés. Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Options d'action de scan et paramètres supplémentaires à la page 6-15*.
7. Si vous avez sélectionné des groupes ou des agents dans l'arborescence des agents, cliquez sur **Enregistrer** pour appliquer les paramètres aux groupes ou aux agents. Si vous avez sélectionné l'icône racine (), choisissez l'une des options suivantes :
   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un groupe existant/futur. Les groupes futurs sont des groupes qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux groupes futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux groupes futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un groupe existant.

Scanner maintenant

Le scan immédiat est lancé à distance par un administrateur Trend Micro Security (pour Mac) via la console Web. Il peut être exécuté sur un ou plusieurs ordinateurs Mac.

Lancez le scan immédiat sur les ordinateurs susceptibles d'être infectés.

Lancement d'un scan immédiat

Avant de commencer

Tous les paramètres de scan programmé, à l'exception de la programmation en elle-même, sont utilisés lors du scan immédiat. Pour configurer les paramètres avant de lancer un scan immédiat, suivez les étapes de la rubrique *Configuration des paramètres de scan programmé à la page 6-8*.

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine () afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Tâches** > **Scan immédiat**.

Paramètres communs à tous les types de scans

Pour chaque type de scan, configurez trois ensembles de paramètres : critères de scan, exclusions de scan et actions de scan. Déployez ces paramètres sur un ou plusieurs agents et groupes, ou sur tous les agents gérés par le serveur.

Critères de scan

Spécifiez les fichiers qu'un type de scan spécifique doit scanner à l'aide des attributs de fichiers, tels que le type et l'extension. Spécifiez également les conditions qui déclencheront le scan. Par exemple, configurez le scan en temps réel pour qu'il s'exécute à chaque téléchargement d'un fichier sur l'ordinateur.

Action des utilisateurs sur les fichiers

Choisissez des actions sur les fichiers qui déclencheront le scan en temps réel. Sélectionnez l'une des options suivantes :

- **Scanner les fichiers en cours de création/modification** : Scanne les nouveaux fichiers présents sur l'ordinateur (par exemple, après leur téléchargement) ou les fichiers en cours de modification
- **Scanner les fichiers en cours de récupération** : Scanne les fichiers lors de leur ouverture
- **Scanner les fichiers en cours de création/modification et de récupération**

Par exemple, si la troisième option est sélectionnée, un nouveau fichier téléchargé sur l'ordinateur sera scanné et ne sera pas déplacé si aucun risque de sécurité n'est détecté. Le fichier sera scanné lors de son ouverture ou, s'il a été modifié, avant l'enregistrement des modifications.

Cible du scan

Sélectionnez l'une des options suivantes :

- **Tous les fichiers scannables** : Scanne tous les fichiers
- **Types de fichier scannés par IntelliScan** : Scanne uniquement les fichiers susceptibles de contenir du code malveillant, y compris ceux dissimulés sous une extension inoffensive. Consultez la rubrique *IntelliScan à la page B-2* pour obtenir des informations détaillées.
- **Nom du fichier ou du dossier accompagné du chemin complet** : Scanne uniquement le ou les fichiers se trouvant dans un dossier spécifique.

  1. Saisissez un chemin d'accès complet à un fichier ou à un répertoire, puis cliquez sur **Ajouter**.

     - Exemple de chemin d'accès complet à un fichier : `/Users/username/temp.zip`
     - Exemple de chemin d'accès à un répertoire : `/Users/username`

2. Pour supprimer un chemin d'accès complet à un fichier ou à un répertoire, sélectionnez-le, puis cliquez sur **Supprimer**.

Paramètres de scan

Trend Micro Security (pour Mac) peut scanner les fichiers inclus dans des fichiers compressés et prend en charge les types de compressions suivants :

EXTENSION	TYPE
.zip	Archive créée avec Pkzip
.rar	Archive créée avec RAR
.tar	Archive créée avec Tar
.arj	Archive compressée ARJ
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/Fichiers compressés 16 bits
.bin	MacBinary
.cab	Fichier Microsoft Cabinet
Microsoft Compressed/ MSCOMP	
.eml; .mht	MIME
.td0	Format Teledisk
.bz2	Fichier compressé avec Unix BZ2 et Bzip
.uu	UUEncode
.ace	WinAce

Utilisation du processeur

Trend Micro Security (pour Mac) peut s'interrompre entre deux fichiers scannés. Ce paramètre est utilisé lors du scan manuel, du scan programmé et du scan immédiat.

Sélectionnez l'une des options suivantes :

- **Élevé** : Aucune interruption entre les fichiers lors des scans
- **Faible** : Interruption entre les fichiers lors des scans

Programmation

Configurez la fréquence (quotidienne, hebdomadaire ou mensuelle) ainsi que l'heure d'exécution du scan programmé.

Si vous avez sélectionné le 29, le 30 ou le 31 pour les scans programmés mensuels, Trend Micro Security (pour Mac) exécute le scan programmé le dernier jour du mois lorsque le mois est plus court.

Actions de scan

Spécifiez l'action effectuée par Trend Micro Security (pour Mac) lorsqu'un type de scan particulier détecte un risque de sécurité.

L'action que Trend Micro Security (pour Mac) effectue dépend du type de scan qui a détecté le risque de sécurité. Par exemple, lorsque Trend Micro Security (pour Mac) détecte un risque de sécurité lors d'un scan manuel (type de scan), il nettoie (action) le fichier infecté.

Les actions suivantes contre les risques de sécurité peuvent être effectuées par Trend Micro Security (pour Mac) :

Actions de scan	Détails
Supprimer	Trend Micro Security (pour Mac) supprime le fichier infecté de l'ordinateur.

ACTIONS DE SCAN	DÉTAILS
Quarantaine	Trend Micro Security (pour Mac) renomme puis déplace le fichier infecté vers le répertoire de quarantaine sur l'ordinateur agent situé dans <*dossier d'installation de l'agent*>`/common/lib/vsapi/quarantine`. Une fois dans le répertoire de quarantaine, Trend Micro Security (pour Mac) peut effectuer une action supplémentaire sur le fichier en quarantaine, en fonction de l'action spécifiée par l'utilisateur. Trend Micro Security (pour Mac) peut supprimer, nettoyer ou restaurer le fichier. L'opération de restauration correspond au déplacement du fichier vers son emplacement d'origine sans effectuer d'action. Les utilisateurs peuvent restaurer le fichier s'il est réellement inoffensif. Le nettoyage correspond à la suppression du risque de sécurité du fichier en quarantaine, puis à son transfert vers son emplacement d'origine si le nettoyage est réussi.
Nettoyer	Trend Micro Security (pour Mac) supprime le risque de sécurité présenté par un fichier infecté avant d'autoriser les utilisateurs à y accéder. Si le fichier n'est pas nettoyable, Trend Micro Security (pour Mac) effectue une seconde action qui peut être l'une des actions suivantes : Quarantaine, Supprimer et Ignorer. Pour configurer la deuxième action, accédez à **Gestion des agents** > **Paramètres** > **{Type de scan}** et cliquez sur l'onglet **Action**.

Actions de scan	Détails
Ignorer	Trend Micro Security (pour Mac) n'effectue pas d'action sur le fichier infecté mais consigne le risque de sécurité détecté dans les journaux. Le fichier reste à son emplacement. Trend Micro Security (pour Mac) « ignore » toujours les fichiers infectés avec de type virus/programmes malveillants potentiels, afin de réduire le risque de faux positifs. Si une analyse plus poussée confirme que le virus/programme malveillant potentiel constitue effectivement un risque de sécurité, un nouveau fichier de signatures est publié pour permettre à Trend Micro Security (pour Mac) d'entreprendre l'action de scan appropriée. S'il se révèle inoffensif, le virus/programme malveillant potentiel ne sera plus détecté. Par exemple : Trend Micro Security (pour Mac) détecte « virus_potentiel_x » sur un fichier nommé « 123.pdf » et n'entreprend aucune action lors de la détection. Trend Micro confirme ensuite que « virus_potentiel_x » est un cheval de Troie et publie une nouvelle version du fichier de signatures. Après le chargement du nouveau fichier de signatures, Trend Micro Security (pour Mac) détecte que « virus_potentiel_x » est un cheval de Troie et, si l'action prévue contre un tel programme est « Supprimer », supprime « 123.pdf ».

Options d'action de scan et paramètres supplémentaires

Lors de la configuration de l'action de scan, sélectionnez l'une des options suivantes :

Option	Détails
Utiliser ActiveAction	ActiveAction est un ensemble d'actions de scan préconfigurées pour différents types de risques de sécurité. Si vous ignorez quelle action est la mieux adaptée à un type de risque de sécurité, l'utilisation de l'outil ActiveAction est recommandée. Les paramètres ActiveAction sont constamment mis à jour dans les fichiers de signatures pour protéger les ordinateurs contre les risques de sécurité et les méthodes d'attaques les plus récents.

OPTION	DÉTAILS
Utiliser la même action pour tous les types de risques de sécurité	Sélectionnez cette option si vous voulez que la même action soit effectuée sur tous les types de risques de sécurité, sauf les virus/programmes malveillants potentiels. Pour les virus/programmes malveillants potentiels, l'action est toujours « Ignorer ». Si vous choisissez « Nettoyer » en tant que première action, sélectionnez une seconde action que Trend Micro Security (pour Mac) effectue en cas d'échec du nettoyage. Si la première action n'est pas « Nettoyer », aucune seconde action n'est configurable. Pour obtenir des informations détaillées sur les actions de scan, consultez la rubrique *Actions de scan à la page 6-13*.

Paramètres supplémentaires de scan en temps réel

PARAMÈTRE	DÉTAILS
Afficher une notification lorsqu'un risque de sécurité est détecté	Lorsque Trend Micro Security (pour Mac) détecte un risque de sécurité lors d'un scan en temps réel, il peut afficher un message de notification informant l'utilisateur de la détection.

Privilèges du scan programmé

Si un scan programmé est activé sur l'ordinateur Mac, les utilisateurs peuvent reporter et ignorer/arrêter le scan programmé.

Privilège	Détails
Différer le scan programmé	Les utilisateurs disposant du privilège « Différer le scan programmé » peuvent effectuer les actions suivantes : • Différer le scan programmé avant son exécution, puis indiquer la durée du report. Un scan programmé ne peut être différé qu'une seule fois. • Si un scan programmé est en cours, les utilisateurs peuvent arrêter le scan et le redémarrer ultérieurement. Les utilisateurs peuvent alors indiquer la durée d'attente avant le redémarrage du scan. Lorsque le scan redémarre, tous les fichiers précédemment scannés sont à nouveau scannés. Un scan programmé ne peut être arrêté et redémarré qu'une seule fois. Configurer le nombre d'heures et de minutes, ce qui correspond à : • La durée maximale de report • La durée d'attente maximale avant le redémarrage du scan
Ignorer ou arrêter le scan programmé	Ce privilège permet aux utilisateurs d'effectuer les actions suivantes : • Ignorer le scan programmé, avant son exécution • Arrêter le scan programmé, lorsqu'il est en cours

Paramètres supplémentaires de scan programmé

Paramètre	Détails
Afficher une notification avant l'exécution du scan programmé	Lorsque vous activez cette option, un message de notification s'affiche sur l'ordinateur Mac quelques minutes avant l'exécution du scan programmé. Les utilisateurs sont informés de la programmation du scan (date et heure) et des privilèges de scan programmé dont ils disposent, tels que reporter, ignorer ou arrêter un scan programmé. Configurez le moment de l'affichage du message de notification, en minutes.

Paramètre	Détails
Arrêter automatiquement le scan programmé lorsque celui-ci dure plus de __ heures et __ minutes	L'agent arrête le scan lorsque la durée indiquée s'est écoulée, même si le scan n'est pas terminé. L'agent avertit immédiatement les utilisateurs de tout risque de sécurité détecté lors du scan.

Exclusions de scan

Configurez les exclusions de scan afin d'accroître les performances du scan et d'ignorer les fichiers inoffensifs.. Lorsqu'un type de scan spécifique s'exécute, Trend Micro Security (pour Mac) vérifie la liste des exclusions de scan pour déterminer les fichiers présents sur l'ordinateur qui seront exclus du scan.

Liste des exclusions de scan	Détails
Fichiers	Trend Micro Security (pour Mac) exclut un fichier du scan si : • Ce fichier se trouve dans le répertoire indiqué dans la liste des exclusions de scan • Ce fichier correspond au chemin de fichier complet (chemin du répertoire et nom du fichier) indiqué dans la liste des exclusions de scan
Extensions de fichiers	Trend Micro Security (pour Mac) ne scanne pas les fichiers dont l'extension correspond à l'une des extensions présentes dans la liste des exclusions.

Configuration des listes d'exclusion de scan

Pour obtenir des informations détaillées sur les listes des exclusions de scan, consultez la rubrique *Exclusions de scan à la page 6-18*.

Procédure

1. Accédez à **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône de la racine () afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres d'exclusion de scan**.
4. Cochez la case pour activer l'exclusion de scan.
5. Pour configurer la **Liste des exclusions de scan (fichiers)** :
   a. Saisissez un chemin d'accès complet à un fichier ou à un répertoire et cliquez sur **Ajouter**.

      Rappels :

      - Il est impossible de saisir uniquement un nom de fichier.
      - Vous pouvez définir au maximum 64 chemins. Reportez-vous au tableau ci-dessous pour obtenir des exemples.

CHEMIN	DÉTAILS	EXEMPLES
Chemin d'accès complet au fichier	Exclut un fichier spécifique sur l'ordinateur	• Exemple 1 : `/file.log` • Exemple 2 : `/System/file.log`

CHEMIN	DÉTAILS	EXEMPLES
Chemin d'accès à un répertoire	Exclut tous les fichiers situés dans un dossier spécifique ainsi que tous ses sous-dossiers	• Exemple 1 : `/System/` Exemples de fichiers exclus des scans : • `/System/file.log` • `/System/Library/file.log` Exemples de fichiers inclus dans les scans : • `/Applications/file.log` • Exemple 2 : `/System/Library` Exemples de fichiers exclus des scans : • `/System/Library/file.log` • `/System/Library/Filters/file.log` Exemples de fichiers inclus dans les scans : • `/System/file.log`

- Utilisez un astérisque (*) au lieu des noms de dossiers.

  Reportez-vous au tableau ci-dessous pour obtenir des exemples.

CHEMIN	EXEMPLES D'UTILISATION DE CARACTÈRES GÉNÉRIQUES
Chemin d'accès complet au fichier	`/Users/Mac/*/file.log` Exemples de fichiers exclus des scans : • `/Users/Mac/Desktop/file.log` • `/Users/Mac/Movies/file.log` Exemples de fichiers inclus dans les scans : • `/Users/file.log` • `/Users/Mac/file.log`

Chemin d'accès à un répertoire	• Exemple 1 :
	`/Users/Mac/*`
	Exemples de fichiers exclus des scans :
	• `/Users/Mac/doc.html`
	• `/Users/Mac/Documents/doc.html`
	• `/Users/Mac/Documents/Pics/pic.jpg`
	Exemples de fichiers inclus dans les scans :
	• `/Users/doc.html`
	• Exemple 2 :
	`/*/Components`
	Exemples de fichiers exclus des scans :
	• `/Users/Components/file.log`
	• `/System/Components/file.log`
	Exemples de fichiers inclus dans les scans :
	• `/file.log`
	• `/Users/file.log`
	• `/System/Files/file.log`

- Les correspondances partielles des noms de fichiers ne sont pas prises en charge. Par exemple, il est impossible de saisir `/Users/*user/temp` afin d'exclure les fichiers se trouvant dans des dossiers dont les noms se terminent par `user`, tels que `end_user` ou `new_user`.

b. Pour supprimer un chemin, sélectionnez-le, puis cliquez sur **Supprimer**.

6. Pour configurer la **Liste des exclusions de scan (extensions de fichier)** :

   a. Saisissez une extension de fichier, sans point (.), et cliquez sur **Ajouter**. Par exemple, saisissez `pdf`. Vous pouvez définir au maximum 64 extensions de fichiers.

   b. Pour supprimer une extension de fichier, sélectionnez-la, puis cliquez sur **Supprimer**.

7. Si vous avez sélectionné des groupes ou des agents dans l'arborescence des agents, cliquez sur **Enregistrer** pour appliquer les paramètres aux groupes ou aux agents. Si vous avez sélectionné l'icône racine (), choisissez l'une des options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un groupe existant/futur. Les groupes futurs sont des groupes qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux groupes futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux groupes futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un groupe existant.

Paramètres de cache des scans

Lors de chaque exécution du scan, l'agent vérifie le **cache des fichiers modifiés** afin de savoir si un fichier a été modifié depuis le dernier démarrage de l'agent.

- Si un fichier a en effet été modifié, l'agent le scanne et l'ajoute au **cache des fichiers scannés**.
- Dans le cas d'un fichier non modifié, l'agent vérifie que ce fichier se trouve dans le cache des fichiers scannés.

- Si le fichier se trouve bien dans le cache des fichiers scannés, l'agent ne procède pas au scan du fichier.
- Si le fichier ne se trouve pas dans le cache des fichiers scannés, l'agent vérifie le **cache des fichiers approuvés**.

Remarque

Le cache des fichiers approuvés contient des fichiers jugés comme étant de confiance par Trend Micro Security (pour Mac). Les fichiers de confiance ont été scannés par les versions successives du fichier de signatures et déclarés dépourvus de menaces à chaque fois. Il peut également s'agir de fichiers ne contenant pas de menaces et n'ayant pas été modifiés depuis un certain temps.

- Si le fichier se trouve bien dans le cache des fichiers approuvés, l'agent ne procède pas au scan du fichier.
- Si le fichier ne se trouve pas dans le cache des fichiers approuvés, l'agent le scanne et l'ajoute au cache des fichiers scannés.

Certains caches (ou tous les caches) sont vidés lorsque le moteur de scan ou le fichier de signatures est mis à jour.

Si des scans sont exécutés fréquemment et que de nombreux fichiers sont envoyés vers les caches, la durée de scan s'en trouve significativement réduite.

Si des scans sont rarement exécutés, désactivez les caches, afin que chaque scan analyse les fichiers à la recherche des menaces potentielles.

Configuration des paramètres de cache des scans

Pour obtenir des détails sur le cache de scan à la demande, consultez la rubrique *Paramètres de cache des scans à la page 6-22*.

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine () afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Paramètres de cache des scans**.

4. Sélectionnez **Activer le cache de scan à la demande**.

5. Si vous avez sélectionné des groupes ou des agents dans l'arborescence des agents, cliquez sur **Enregistrer** pour appliquer les paramètres aux groupes ou aux agents. Si vous avez sélectionné l'icône racine (), choisissez l'une des options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un groupe existant/futur. Les groupes futurs sont des groupes qui ne sont pas encore créés au moment de la configuration des paramètres.

   - **Appliquer aux groupes futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux groupes futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un groupe existant.

Notifications et journaux de risques de sécurité

Trend Micro Security (pour Mac) est fourni avec un ensemble de messages de notification par défaut qui informent les utilisateurs ainsi que les administrateurs de la détection d'un risque de sécurité ou d'une épidémie.

Trend Micro Security (pour Mac) crée des journaux lorsqu'il détecte des risques de sécurité.

Configuration des paramètres de notification aux administrateurs

En cas de détection de risques de sécurité ou d'épidémie, les administrateurs de Trend Micro Security (pour Mac) peuvent recevoir des notifications par e-mail.

Procédure

1. Accédez à **Notifications** > **Paramètres généraux**.
2. Dans le champ **Serveur SMTP**, saisissez une adresse IPv4/IPv6 ou un nom d'ordinateur.
3. Saisissez un numéro de port compris entre 1 et 65535.
4. Saisissez l'adresse électronique de l'expéditeur dans le champ **De**.
5. Cliquez sur **Enregistrer**.

Configuration des notifications de risques de sécurité aux administrateurs

Configurez Trend Micro Security (pour Mac) pour qu'il envoie une notification lorsqu'un risque de sécurité est détecté ou uniquement lorsque l'action entreprise contre le risque échoue et qu'une intervention de votre part s'impose en conséquence.

Vous pouvez recevoir des notifications par e-mail. Configurez les paramètres de notification aux administrateurs pour permettre à Trend Micro Security (pour Mac) d'envoyer des notifications via e-mail. Pour obtenir des informations détaillées, consultez la rubrique *Configuration des paramètres de notification aux administrateurs à la page 6-24*.

Procédure

1. Accédez à **Notifications** > **Notifications standard**.
2. Sous l'onglet **Critères**, déterminez si des notifications doivent être envoyées à chaque fois que Trend Micro Security (pour Mac) détecte un risque de sécurité, ou uniquement lorsque l'action effectuée sur les risques de sécurité échoue.
3. Cliquez sur **Enregistrer**.
4. Sous l'onglet **E-mail** :
   a. Autorisez l'envoi de notifications par e-mail.

b. Spécifiez les destinataires des e-mails, puis acceptez ou modifiez l'objet par défaut.

Les variables de jeton sont utilisées afin de représenter les données dans le champ **Message**.

VARIABLE	DESCRIPTION
%v	Nom du risque de sécurité
%s	Ordinateur sur lequel le risque de sécurité a été détecté
%m	Groupe de l'arborescence des agents auquel appartient l'ordinateur
%p	Emplacement du risque de sécurité
%y	Date et heure de la détection

5. Cliquez sur **Enregistrer**.

Configuration des notifications d'épidémies pour les administrateurs

Définissez les critères d'épidémie en fonction du nombre de risques de sécurité détectés et de la période de détection. Configurez ensuite Trend Micro Security (pour Mac) pour vous notifier, ainsi qu'aux autres administrateurs Trend Micro Security (pour Mac), d'une épidémie afin que vous puissiez y apporter une réponse immédiate.

Vous pouvez recevoir des notifications par e-mail. Configurez les paramètres de notification aux administrateurs pour permettre à Trend Micro Security (pour Mac) d'envoyer des notifications via e-mail. Pour obtenir des informations détaillées, consultez la rubrique *Configuration des paramètres de notification aux administrateurs à la page 6-24*.

Procédure

1. Accédez à **Notifications** > **Notifications d'épidémies**.
2. Sous l'onglet **Critères**, spécifiez ce qui suit :

- Nombre de sources uniques de risques de sécurité
- Nombre de détections
- Période de détection

Conseil

Trend Micro recommande d'accepter les valeurs par défaut dans cet écran.

Trend Micro Security (pour Mac) déclare une épidémie et envoie un message de notification lorsque le nombre de détections est dépassé. Par exemple, si vous spécifiez 100 détections, Trend Micro Security (pour Mac) envoie la notification après avoir détecté la 101e instance d'un risque de sécurité.

3. Cliquez sur **Enregistrer**.
4. Sous l'onglet **E-mail** :
   a. Autorisez l'envoi de notifications par e-mail.
   b. Spécifiez les destinataires des e-mails, puis acceptez ou modifiez l'objet par défaut.

      Les variables de jeton sont utilisées afin de représenter les données dans le champ **Message**.

VARIABLE	DESCRIPTION
%CV	Nombre total de risques de sécurité détectés
%CC	Nombre total d'ordinateurs affectés par des risques de sécurité

5. Sélectionnez les informations supplémentaires que vous souhaitez inclure dans l'e-mail, Par exemple, le nom de l'agent/groupe, le nom du risque de sécurité, le chemin d'accès du fichier infecté, la date et l'heure de la détection, ainsi que le résultat du scan.
6. Cliquez sur **Enregistrer**.

Consultation des journaux de risques de sécurité

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine () afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Journaux** > **Journaux de risques de sécurité**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux comprennent les informations suivantes :
   - Date et heure de la détection du risque de sécurité
   - Ordinateur affecté par un risque de sécurité
   - Nom du risque de sécurité
   - Source du risque de sécurité
   - Type de scan qui a détecté le risque de sécurité
   - Résultats de scan, qui indiquent si les actions de scan ont été correctement effectuées. Pour obtenir des informations détaillées sur les résultats de scan, consultez la rubrique *Résultats du scan à la page 6-29*.
   - Plate-forme
6. Pour enregistrer les journaux en tant que fichiers au format CSV, cliquez sur **Exporter**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Remarque

Si vous exportez un grand nombre de journaux, attendez que la tâche d'exportation soit achevée. Si vous fermez la page avant la fin de la tâche d'exportation, le fichier .csv ne sera pas créé.

Que faire ensuite

Pour éviter que les journaux n'occupent trop d'espace sur le disque dur, supprimez-les manuellement ou configurez une programmation de suppression des journaux. Consultez la rubrique *Gestion des journaux à la page 8-6* pour obtenir des informations complémentaires sur la gestion des journaux.

Résultats du scan

Les résultats de scan suivants s'affichent dans les journaux relatifs aux virus/programmes malveillants :

- **Supprimé**
  - La première action est Supprimer et le fichier infecté a été supprimé.
  - La première action est Nettoyer, mais le nettoyage a échoué. La seconde action est Supprimer et le fichier infecté a été supprimé.
- **En quarantaine**
  - La première action est Quarantaine et le fichier infecté a été mis en quarantaine.
  - La première action est Nettoyer, mais le nettoyage a échoué. La seconde action est Quarantaine et le fichier infecté a été mis en quarantaine.
- **Nettoyé**

  Un fichier infecté a été nettoyé.
- **Ignoré**
  - La première action est Ignorer. Trend Micro Security (pour Mac) n'a entrepris aucune action sur le fichier infecté.
  - La première action est Nettoyer, mais le nettoyage a échoué. La deuxième action est Ignorer. De ce fait, Trend Micro Security (pour Mac) n'a entrepris aucune action sur le fichier infecté.
- **Impossible de nettoyer le fichier ou de le mettre en quarantaine**

La première action est Nettoyer. La seconde action est Quarantaine. Ces deux actions ont échoué.

Solution : Consultez la section « Impossible de mettre le fichier en quarantaine » ci-dessous.

- **Impossible de nettoyer ou de supprimer le fichier**

  La première action est Nettoyer. La seconde action est Supprimer. Ces deux actions ont échoué.

  Solution : Consultez la section « Impossible de supprimer le fichier » ci-dessous.

- **Impossible de mettre le fichier en quarantaine**

  Le fichier infecté est peut-être verrouillé par une autre application, est en cours d'exécution ou se trouve sur un CD. Trend Micro Security (pour Mac) mettra le fichier en quarantaine une fois que l'application aura terminé de traiter le fichier ou après son exécution.

  Solution

  Dans le cas de fichiers infectés sur un CD, envisagez de ne pas utiliser celui-ci car le virus peut se propager sur d'autres ordinateurs du réseau.

- **Impossible de supprimer le fichier**

  Le fichier infecté est peut-être verrouillé par une autre application, est en cours d'exécution ou se trouve sur un CD. Trend Micro Security (pour Mac) supprimera le fichier une fois que l'application aura terminé de traiter le fichier ou après son exécution.

  Solution

  Dans le cas de fichiers infectés sur un CD, envisagez de ne pas utiliser celui-ci car le virus peut se propager sur d'autres ordinateurs du réseau.

- **Impossible de nettoyer le fichier**

  Le fichier est peut-être non nettoyable. Pour obtenir des informations détaillées et des solutions, consultez la rubrique *Fichiers non nettoyables à la page B-2*.

Chapitre 7

Protection des ordinateurs Mac contre les menaces Web

Ce chapitre décrit les menaces Web et comment utiliser Trend Micro Security (pour Mac) pour protéger votre réseau et vos ordinateurs de telles menaces.

Menaces Web

Les menaces Internet comprennent un large éventail de menaces provenant du Web. Les menaces Internet emploient des méthodes très sophistiquées : au lieu d'utiliser une seule approche ou un seul fichier, elles associent plusieurs techniques et fichiers. Les auteurs de menaces Internet modifient par exemple constamment la version ou la variante utilisée. Étant donné qu'une menace Internet se trouve à un emplacement défini sur un site Web plutôt que sur un ordinateur infecté, l'auteur de cette menace Internet modifie constamment son code pour éviter qu'elle ne soit détectée.

De nos jours, les pirates informatiques, les auteurs de virus, les spammeurs et les développeurs de programmes espions sont regroupés sous le nom de « cyber-criminels ». Les menaces Web aident ces individus à atteindre un objectif précis. L'un de ces objectifs est de voler des informations à des fins de revente. Il en résulte une fuite des informations confidentielles sous la forme de perte d'identité. L'ordinateur infecté peut également servir de vecteur pour la transmission d'attaques de hameçonnage ou d'autres activités de capture d'informations. En outre, cette menace est susceptible de briser la confiance dans le commerce électronique ainsi que dans les transactions Internet. Le second objectif est de pirater la puissance du processeur de l'utilisateur afin de mener des activités lucratives, par exemple l'envoi de spam ou l'extorsion sous la forme d'attaques de refus de service distribuées ou d'activités de paiement au clic.

Réputation de sites Web

Trend Micro Security (pour Mac) exploite les bases de données de sécurité Web de Trend Micro pour vérifier la réputation des sites Web auxquels les utilisateurs tentent d'accéder. La réputation du site Web est mise en corrélation avec la stratégie de réputation de sites Web appliquée sur l'ordinateur. En fonction de la stratégie utilisée, Trend Micro Security (pour Mac) bloque ou autorise l'accès au site Web. Les stratégies sont appliquées en fonction de l'emplacement de l'agent.

Configuration des paramètres de réputation de sites Web

Les paramètres de réputation de sites Web incluent des stratégies qui indiquent à Trend Micro Security (pour Mac) de bloquer ou d'autoriser l'accès à un site Web donné. Pour déterminer la stratégie appropriée à utiliser, Trend Micro Security (pour Mac) vérifie l'emplacement de l'agent. L'emplacement de l'agent est « interne » s'il peut se connecter au serveur Trend Micro Security (pour Mac). Dans le cas contraire, l'emplacement de l'agent est « externe ».

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine ( ) afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètre de réputation de sites Web**.
4. Pour configurer une stratégie pour les agents externes :
   a. Cliquez sur l'onglet **Agents externes**.
   b. Sélectionnez **Activer la stratégie de réputation de sites Web**.

      Lorsque la stratégie est activée, les agents externes envoient des requêtes d'évaluation de la réputation de sites Web au réseau Smart Protection Network.

      Remarque

      Si un agent dispose uniquement d'une adresse IPv6, consultez les limitations relatives aux requêtes d'évaluation de réputation de sites Web liées à IPv6 à la rubrique *Limitations pour agent en IPv6 pur à la page A-3*.

      ---

   c. Sélectionnez un niveau de sécurité pour la fonction de réputation de sites Web : **Élevé**, **Moyen** ou **Faible**

Remarque

Les niveaux de sécurité déterminent si Trend Micro Security (pour Mac) autorise ou bloque l'accès à une URL. Par exemple, si vous définissez le niveau de sécurité sur Faible, Trend Micro Security (pour Mac) ne bloque que les URL constituant des menaces Web connues. Lorsque vous définissez un niveau de sécurité supérieur, le taux de détection des menaces Web s'améliore mais la possibilité de détecter des faux positifs augmente également.

d. Pour envoyer des commentaires relatifs à la réputation de sites Web, cliquez sur l'URL fournie. Le système d'évaluation de réputation de sites Web de Trend Micro ouvre une nouvelle fenêtre de navigateur.

5. Pour configurer une stratégie pour les agents internes :

a. Cliquez sur l'onglet **Agents internes**.

b. Sélectionnez **Activer la stratégie de réputation de sites Web**.

Lorsque la stratégie est activée, les agents internes envoient des requêtes d'évaluation de la réputation de sites Web aux entités suivantes :

- aux serveurs Smart Protection Server si l'option **Envoyer les requêtes aux Smart Protection Servers** est activée.
- au réseau Smart Protection Network si l'option **Envoyer les requêtes aux Smart Protection Servers** est désactivée.

Remarque

Si un agent dispose uniquement d'une adresse IPv6, consultez les limitations relatives aux requêtes d'évaluation de réputation de sites Web liées à IPv6 à la rubrique *Limitations pour agent en IPv6 pur à la page A-3*.

c. Sélectionnez **Envoyer les requêtes aux Smart Protection Servers** si vous souhaitez que les agents internes envoient des requêtes de réputation de sites Web à des serveurs Smart Protection Server.

- Si vous activez cette option, les agents utilisent la même liste de sources Smart Protection que celle utilisée par les agents OfficeScan pour déterminer les serveurs Smart Protection Server auxquels envoyer leurs requêtes.

Important

Avant d'activer cette option, consultez les directives fournies à la rubrique *Trend Micro Smart Protection à la page 3-13*.

Cette option ne peut pas être activée si le serveur Trend Micro Security (pour Mac) est installé avec OfficeScan 10. Si cette option est activée depuis la gestion des stratégies de Control Manager, puis déployée sur un serveur Trend Micro Security (pour Mac) installé avec OfficeScan 10, ce paramètre ne prendra pas effet et l'option restera désactivée.

- Si vous désactivez cette option, les agents envoient des requêtes d'évaluation de la réputation de sites Web au réseau Smart Protection Network. Les ordinateurs Mac doivent disposer d'une connexion Internet pour réussir à envoyer des requêtes.

d. Sélectionnez un niveau de sécurité pour la fonction de réputation de sites Web : **Élevé**, **Moyen** ou **Faible**

Remarque

Les niveaux de sécurité déterminent si Trend Micro Security (pour Mac) autorise ou bloque l'accès à une URL. Par exemple, si vous définissez le niveau de sécurité sur Faible, Trend Micro Security (pour Mac) ne bloque que les URL constituant des menaces Web connues. Lorsque vous définissez un niveau de sécurité supérieur, le taux de détection des menaces Web s'améliore mais la possibilité de détecter des faux positifs augmente également.

Les agents ne bloquent pas les sites Web non testés, quel que soit le niveau de sécurité.

e. Pour envoyer des commentaires relatifs à la réputation de sites Web, cliquez sur l'URL fournie. Le système d'évaluation de réputation de sites Web de Trend Micro ouvre une nouvelle fenêtre de navigateur.

f. Décidez si les agents sont autorisés à envoyer des journaux de réputation de sites Web au serveur. Autorisez les agents à envoyer des journaux si vous souhaitez analyser les URL bloquées par Trend Micro Security (pour Mac), puis entreprendre l'action appropriée sur les URL dont vous estimez l'accès sécurisé.

6. Si vous avez sélectionné des groupes ou des agents dans l'arborescence des agents, cliquez sur **Enregistrer** pour appliquer les paramètres aux groupes ou aux agents. Si vous avez sélectionné l'icône racine (), choisissez l'une des options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un groupe existant/futur. Les groupes futurs sont des groupes qui ne sont pas encore créés au moment de la configuration des paramètres.
   - **Appliquer aux groupes futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux groupes futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un groupe existant.

Configuration de la liste des URL approuvées

Les URL approuvées contournent les stratégies de réputation de sites Web. Trend Micro Security (pour Mac) ne bloque pas ces URL même si la stratégie de réputation de sites Web est configurée pour les bloquer. Ajoutez les URL que vous estimez être sures à la liste des URL approuvées.

Procédure

1. Accédez à **Administration** > **Liste des URL approuvées par l'évaluation de réputation des sites Web**.
2. Saisissez une URL dans la zone de texte. Vous pouvez insérer un caractère générique (*) dans l'URL.

   Exemples :

   - `www.trendmicro.com/*` signifie que toutes les pages situées dans le domaine www.trendmicro.com seront approuvées.
   - `*.trendmicro.com/*` signifie que toutes les pages des sous-domaines de trendmicro.com seront approuvées.

Vous pouvez saisir des URL contenant des adresses IP. Si une URL contient une adresse IPv6, placez cette adresse entre crochets.

3. Cliquez sur **Ajouter**.
4. Pour supprimer une entrée, cliquez sur l'icône en regard d'une URL approuvée.
5. Cliquez sur **Enregistrer**.

Consultation des journaux de réputation de sites Web

Avant de commencer

Configurez les agents internes afin qu'ils envoient les journaux de réputation de sites Web au serveur. Procédez ainsi si vous souhaitez analyser les URL bloquées par Trend Micro Security (pour Mac) et entreprendre les actions appropriées pour les URL auxquelles vous estimez pouvoir accéder en toute sécurité.

Procédure

1. Accédez à **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône de la racine () afin d'inclure tous les agents ou bien sélectionnez des groupes ou des agents spécifiques.
3. Cliquez sur **Journaux** > **Journaux de réputation de sites Web**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux comprennent les informations suivantes :
   - Date/heure à laquelle Trend Micro Security (pour Mac) a bloqué l'URL
   - Ordinateur depuis lequel l'utilisateur a accédé à l'URL
   - URL bloquée
   - Niveau de risque de l'URL

- Lien vers le système de requête de l'évaluation de la réputation de sites Web de Trend Micro qui fournit de plus amples informations sur l'URL bloquée

6. Pour enregistrer les journaux en tant que fichiers au format `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Remarque

Si vous exportez un grand nombre de journaux, attendez que la tâche d'exportation soit achevée. Si vous fermez la page avant la fin de la tâche d'exportation, le fichier .csv ne sera pas créé.

Que faire ensuite

Pour éviter que les journaux n'occupent trop d'espace sur le disque dur, supprimez-les manuellement ou configurez une programmation de suppression des journaux. Consultez la rubrique *Gestion des journaux à la page 8-6* pour obtenir des informations complémentaires sur la gestion des journaux.

Chapitre 8

Gestion du serveur et des agents

Ce chapitre décrit la gestion et les configurations supplémentaires des serveurs et agents Trend Micro Security (pour Mac).

Mise à niveau du serveur et des agents

La console Plug-in Manager affiche toute nouvelle version de Trend Micro Security (pour Mac).

Mettez à niveau le serveur et les agents dès qu'une nouvelle version est disponible.

Avant de procéder à la mise à niveau, assurez-vous que le serveur et les agents disposent des ressources nécessaires, comme indiqué dans les rubriques *Configuration minimale requise pour l'installation du serveur à la page 2-2* et *Configuration minimale requise pour l'installation de l'agent à la page 4-2*.

Mise à niveau du serveur

Avant de commencer

Trend Micro recommande d'effectuer une sauvegarde des fichiers de programme et de la base de données du serveur, ce qui permet d'effectuer une restauration en cas de problème lors de la mise à niveau.

- Fichiers de programme
  - Chemin d'accès par défaut :

    `C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM`

    Ou

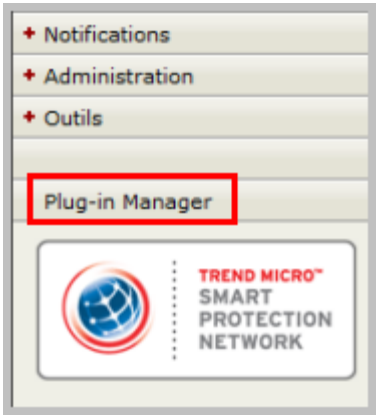
    `C:\Program Files (x86)\Trend Micro\OfficeScan\Addon\TMSM`
  - Fichiers à sauvegarder :
    - `..\apache-activemq\conf\activemq.xml`
    - `..\apache-activemq\conf\broker.pem`
    - `..\apache-activemq\conf\broker.ks`
    - `..\apache-activemq\bin\win32\wrapper.conf`
    - `..\apache-activemq\bin\win64\wrapper.conf`

- `..\ServerInfo.plist`

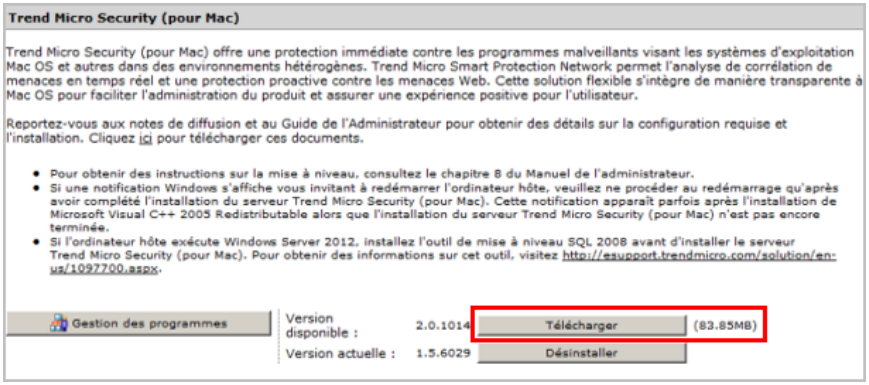
- Fichiers de base de données. Consultez la rubrique *Sauvegarde de la base de données du serveur à la page 8-8*.

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Plug-in Manager** dans le menu principal.



2. Accédez à la section **Trend Micro Security (pour Mac)**, puis cliquez sur **Télécharger**.

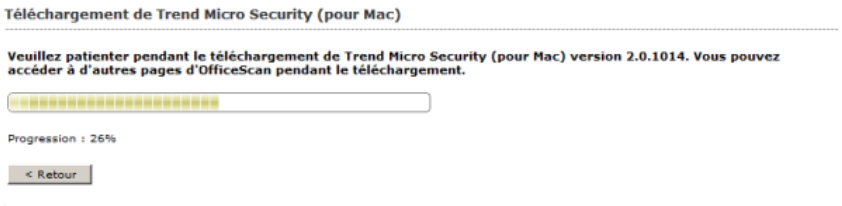


La taille du fichier à télécharger s'affiche à côté du bouton **Télécharger**.

Plug-in Manager télécharge le pack vers `<OfficeScan server installation folder>\PCCSRV\Download`.

`<OfficeScan server installation folder>` est généralement `C:\Program Files\Trend Micro\OfficeScan`.

3. Surveillez la progression du téléchargement.



Vous pouvez naviguer dans une autre fenêtre pendant le téléchargement.

Si vous rencontrez des problèmes lors du téléchargement du pack, consultez les journaux de mise à jour du serveur sur la console Web OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Journaux de mise à jour du serveur**.

4. Pour effectuer immédiatement la mise à niveau de Trend Micro Security (pour Mac), cliquez sur **Mise à niveau immédiate**. Pour effectuer l'installation ultérieurement, procédez comme suit :

   a. Cliquez sur **Mise à niveau ultérieure**.

   b. Ouvrez l'écran Plug-in Manager.

   c. Accédez à la section **Trend Micro Security (pour Mac)**, puis cliquez sur **Mettre à niveau**.

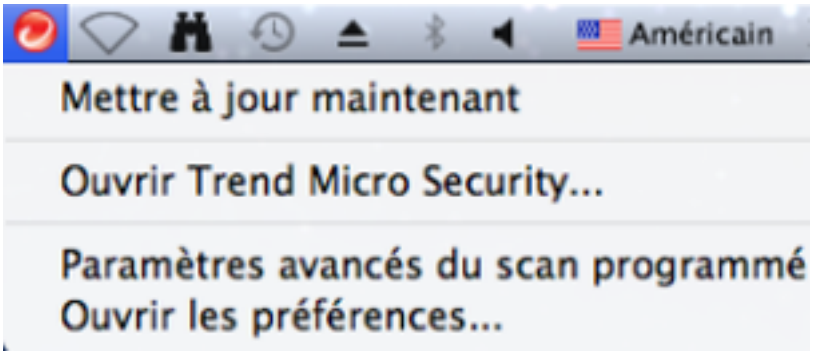
5. Surveillez la progression de la mise à niveau. Une fois la mise à niveau terminée, l'écran Plug-in Manager est actualisé.

Mise à niveau des agents

Procédure

1. Effectuez l'une des opérations suivantes :

   - Effectuez une mise à jour manuelle. Veillez à sélectionner **Agent Trend Micro Security (pour Mac)** dans la liste des composants.
   - Sous l'arborescence des agents, sélectionnez les agents à mettre à niveau, puis cliquez sur **Tâches** > **Mise à jour**.
   - Si la mise à jour programmée a été activée, veillez à sélectionner **Agent Trend Micro Security (pour Mac)**.
   - Demandez aux utilisateurs de cliquer sur **Mettre à jour maintenant** à partir de la console de l'agent.



   Les agents recevant la notification commencent à se mettre à niveau. Sur un ordinateur Mac, l'icône Trend Micro Security (pour Mac) de la barre des menus indique que le produit est en cours de mise à jour. Les utilisateurs ne peuvent pas exécuter de tâches à partir de la console avant la fin de la mise à niveau.

2. Vérifiez l'état de la mise à niveau.

   a. Cliquez sur Résumé dans le menu principal et accédez à la section **Agents**.

   b. Cliquez sur le lien sous la colonne **Pas mis à niveau**. L'arborescence des agents s'ouvre et affiche tous les agents qui n'ont pas été mis à niveau.

c. Pour mettre à niveau ces agents, cliquez sur **Tâches** > **Mise à jour**.

Gestion des journaux

Trend Micro Security (pour Mac) met à votre disposition des journaux complets concernant les détections de risques de sécurité et les URL bloqués. Ceux-ci permettent d'évaluer l'efficacité des stratégies de protection de votre entreprise et d'identifier les agents présentant un risque plus élevé d'infection ou d'attaque.

Pour éviter que les journaux n'occupent trop d'espace sur le disque dur, supprimez-les manuellement ou configurez une programmation de suppression des journaux à partir de la console Web.

Procédure

1. Accédez à **Administration** > **Maintenance des journaux**.
2. Sélectionnez **Activer la suppression programmée des journaux**.
3. Spécifiez si tous les types de journaux doivent être supprimés ou uniquement ceux antérieurs à un certain nombre de jours.
4. Spécifiez la fréquence et l'heure de suppression des journaux.
5. Cliquez sur **Enregistrer**.

Gestion des licences

Affichez, activez et renouvelez la licence Trend Micro Security (pour Mac) sur la console Web.

L'état de la licence du produit détermine les fonctionnalités disponibles aux utilisateurs. Pour plus d'informations, reportez-vous au tableau ci-dessous.

TYPE ET ÉTAT DE LA LICENCE	FONCTIONNALITÉS			
	SCAN EN TEMPS RÉEL	SCAN MANUEL/ PROGRAMMÉ	RÉPUTATION DE SITES WEB	MISE À JOUR DES SIGNATURES
Version complète et activée	Activé	Activé	Activé	Activé
Version d'évaluation et ayant été activée	Activé	Activé	Activé	Activé
Version complète et ayant expiré	Activé	Activé	Désactivé	Désactivé
Version d'évaluation et ayant expiré	Désactivé	Désactivé	Désactivé	Désactivé
Non activé	Désactivé	Désactivé	Désactivé	Désactivé

Remarque

Si le serveur ne dispose que d'une adresse IPv6, consultez les limitations IPv6 pour les mises à jour de licence dans la rubrique *Limitations pour serveur en IPv6 pur à la page A-3*.

Procédure

1. Accédez à **Administration** > **Licence du produit**.
2. Affichez les informations de licence. Pour obtenir des informations actualisées concernant les licences, cliquez sur **Mettre à jour les informations**.

   La section relative aux **informations de licence** vous fournit les informations suivantes :

   - **État** : affiche « Activé » ou « Expiré »
   - **Version** : affiche la version « Complète » ou d'« Évaluation ». Si vous utilisez une version d'évaluation, vous pouvez effectuer à tout moment une mise à niveau vers la version complète. Pour obtenir des instructions sur la mise à niveau, cliquez sur **Afficher les instructions de mise à niveau de la licence**.

- **Postes** : nombre maximum d'installations agents que la licence prend en charge
- **Date d'expiration du contrat de licence** : date d'expiration de la licence
- **Code d'activation** : code d'activation de la licence

3. Pour spécifier un nouveau code d'activation, cliquez sur **Nouveau code d'activation**.
4. Dans l'écran qui s'affiche, saisissez le code d'activation, puis cliquez sur **Enregistrer**.

   Cet écran inclut également un lien pointant vers le site Web de Trend Micro, sur lequel vous pouvez consulter des informations détaillées sur votre licence.

Sauvegarde de la base de données du serveur

Procédure

1. Arrêtez les services suivants depuis la console d'administration Microsoft :
   - **ActiveMQ pour Trend Micro Security**
   - **Trend Micro Security (pour Mac)**
2. Ouvrez SQL Server Management Studio (par exemple, depuis **Menu Démarrer de Windows** > **Programmes** > **Microsoft SQL Server {version}** > **SQL Server Management Studio**.
3. Recherchez `db_TMSM` puis utilisez la fonction **backup** dans SQL Server Management Studio afin de sauvegarder les fichiers de la base de données.

   Consultez la documentation de SQL Server Management Studio pour obtenir des informations détaillées.
4. Démarrez les services que vous aviez arrêtés.

Restauration de la base de données du serveur

Avant de commencer

Préparez la sauvegarde des fichiers de la base de données créés pendant la sauvegarde. Pour obtenir des informations détaillées, consultez la rubrique *Sauvegarde de la base de données du serveur à la page 8-8*.

Procédure

1. Arrêtez les services suivants depuis la console d'administration Microsoft :
   - **ActiveMQ pour Trend Micro Security**
   - **Trend Micro Security (pour Mac)**
2. Ouvrez SQL Server Management Studio (par exemple, depuis **Menu Démarrer de Windows** > **Programmes** > **Microsoft SQL Server {version}** > **SQL Server Management Studio**.
3. Recherchez `db_TMSM` puis utilisez la fonction **detach** dans SQL Server Management Studio afin de détacher les fichiers actuels de la base de données.

   Consultez la documentation de SQL Server Management Studio pour obtenir des informations détaillées.
4. Utilisez l'option **attach** afin d'attacher la sauvegarde des fichiers de le base de données.
5. Démarrez les services que vous aviez arrêtés.

Trend Micro Control Manager

Trend Micro Control Manager est une console d'administration centralisée qui permet de gérer les produits et services Trend Micro à différents niveaux : passerelle, serveur de messagerie, serveur de fichiers et postes de travail d'entreprise. La console d'administration Web de Control Manager offre un point de contrôle unique pour les produits et services gérés sur l'ensemble du réseau.

Control Manager permet aux administrateurs système de surveiller les activités telles que les infections, les violations de sécurité et les points d'entrée de virus, ainsi que de créer des rapports à partir de ces données. Les administrateurs système peuvent télécharger et déployer des composants sur l'ensemble du réseau, ce qui leur permet de garantir une protection cohérente et constamment à jour. Control Manager offre la possibilité d'effectuer des mises à jour manuelles et préprogrammées. Pour plus de flexibilité, il permet également de configurer et de gérer des produits individuellement ou par groupes.

Intégration de Control Manager dans cette version

Cette version de Trend Micro Security (pour Mac) prend en charge Control Manager 6.0. Dans cette version, vous pouvez créer, gérer et déployer des stratégies pour Trend Micro Security (pour Mac) depuis Control Manager.

Voici les configurations de stratégies disponibles dans Control Manager :

- Paramètres de scan manuel
- Paramètres de scan en temps réel
- Paramètres d'exclusion de scan
- Paramètres de cache des scans
- Paramètres de scan programmé
- Paramètres de mise à jour
- Paramètres de réputation de sites Web

Consultez la documentation de Control Manager pour obtenir des informations détaillées.

Remarque

Vous pouvez également spécifier Control Manager comme source de mise à jour pour le serveur Trend Micro Security (pour Mac). Pour obtenir des informations détaillées, consultez la rubrique *Configuration de la source de mise à jour du serveur à la page 5-5*.

Configuration des paramètres de communication agent-serveur

Les agents identifient le serveur qui les gère par son nom ou son adresse IPv4/IPv6. Lors de l'installation du serveur Trend Micro Security (pour Mac) le programme d'installation identifie les adresses IP du serveur, qui s'affichent sur l'écran Communications agent-serveur de la console Web.

Le serveur communique avec les agents par le biais du port d'écoute, qui est le port 61617 par défaut.

Remarques et rappels :

- Si vous modifiez le numéro de port, assurez-vous qu'il n'est pas actuellement utilisé pour empêcher des conflits avec d'autres applications et des problèmes de communication agent-serveur.
- Si un pare-feu est exécuté sur le serveur, veillez à ce qu'il ne bloque pas la communication agent-serveur sur le port d'écoute. Par exemple, si le pare-feu de l'agent OfficeScan a été activé sur l'ordinateur, ajoutez une exception qui autorise le trafic entrant et sortant sur le port d'écoute.
- Vous pouvez configurer les agents pour qu'ils se connectent au serveur via un serveur proxy. Ce dernier n'est toutefois généralement pas requis pour les connexions agent-serveur au sein du réseau de l'entreprise.
- Si vous envisagez de mettre à jour ou de remplacer l'ensemble des noms de serveur et adresses IPv4/IPv6 existants ou de changer le port d'écoute ou les paramètres proxy, faites-le avant d'installer des agents. Si vous avez installé des agents et effectué des changements, la connexion avec le serveur sera perdue et la seule façon de la rétablir sera de redéployer les agents.

Procédure

1. Accédez à **Administration** > **Communication agent-server**.
2. Saisissez le nom ou les adresses IPv4/IPv6 du serveur, ainsi que le port d'écoute.

Remarque

Si le champ **Nom de serveur (ou adresse IP)** inclut plusieurs entrées, l'agent en sélectionne une au hasard. Veillez à ce que la connexion agent-serveur puisse être établie à l'aide de toutes les entrées.

3. Indiquez si les agents se connectent au serveur via un serveur proxy.
   a. Sélectionnez le protocole du serveur proxy.
   b. Saisissez le nom ou l'adresse IPv4/IPv6 du serveur proxy, ainsi que le numéro de port.
   c. Si le serveur proxy requiert une authentification, saisissez le nom d'utilisateur et le mot de passe dans les champs prévus à cet effet.
4. Cliquez sur **Enregistrer**.
5. Si vous êtes invité à redémarrer les services Trend Micro Security (pour Mac) pour que les paramètres prennent effet, procédez comme suit :
   a. Accédez à <*Dossier d'installation du serveur*>.
   b. Double-cliquez sur `restart_TMSM.bat`.
   c. Attendez que tous les services redémarrent.

Icônes des agents

Les icônes de la barre d'état de l'ordinateur Mac indiquent l'état de l'agent et la tâche en cours d'exécution.

ICÔNE	COULEUR	DESCRIPTION
	Rouge	L'agent est en cours d'exécution et il est connecté au serveur parent. En outre : • La licence du produit a été activée. • La licence du produit (version d'évaluation ou complète) a été activée mais a expiré. Certaines fonctionnalités de l'agent ne seront pas disponibles si la licence a expiré. Pour obtenir des informations détaillées, consultez la rubrique *Gestion des licences à la page 8-6*.
	Gris	L'agent est en cours d'exécution, mais il est déconnecté du serveur parent.
	Rouge	L'agent recherche les risques de sécurité et il est connecté au serveur parent.
	Gris	L'agent recherche les risques de sécurité, mais il est déconnecté du serveur parent. Si l'agent détecte des risques de sécurité lors du scan, il n'enverra les résultats au serveur que lorsque la connexion aura été restaurée.
	Rouge	L'agent est en train de mettre à jour les composants à partir du serveur parent.
	Gris	L'agent est en train de mettre à jour les composants à partir du serveur ActiveUpdate de Trend Micro car il ne peut pas se connecter au serveur parent.

ICÔNE	COULEUR	DESCRIPTION
	Gris	Cette icône indique ce qui suit : • L'agent a été enregistré auprès du serveur parent, mais la licence du produit n'a pas été activée. Certaines fonctionnalités de l'agent ne seront pas disponibles si la licence n'a pas été activée. Pour obtenir des informations détaillées, consultez la rubrique *Gestion des licences à la page 8-6*. • L'agent n'a pas été enregistré auprès du serveur parent. La licence du produit peut avoir été ou non activée. Si un agent n'est pas enregistré auprès du serveur parent : ◦ Le scan en temps réel est activé, mais l'action sur les risques de sécurité est toujours « Ignorer ». ◦ Le scan manuel, le scan programmé, la réputation de sites Web et les mises à jour des signatures sont désactivés. • L'agent a été enregistré auprès du serveur parent. La licence du produit correspond à une version d'évaluation du produit et a été activée. Toutefois, la licence de la version d'évaluation a expiré. Certaines fonctionnalités de l'agent ne seront pas disponibles si la licence a expiré. Pour obtenir des informations détaillées, consultez la rubrique *Gestion des licences à la page 8-6*.

Chapitre 9

Obtenir de l'aide

Ce chapitre décrit les principaux problèmes pouvant apparaître et comment contacter l'assistance technique.

Dépannage

Accès à la console Web

Problème :

La console Web est inaccessible.

Procédure

1. Vérifiez que l'ordinateur est conforme à la configuration minimale requise pour installer et exécuter le serveur Trend Micro Security (pour Mac). Pour obtenir des informations détaillées, consultez la rubrique *Configuration minimale requise pour l'installation du serveur à la page 2-2*.

2. Vérifiez si les services suivants ont été démarrés :

   - **ActiveMQ pour Trend Micro Security**
   - **OfficeScan Plug-in Manager**
   - **SQL Server (TMSM)**
   - **Trend Micro Security (pour Mac)**

3. Rassemblez les journaux de débogage. Utilisez « erreur » ou « échec » comme mot clé lors de la recherche dans les journaux.

   - **Journaux d'installation** : `C:\TMSM*.log`
   - **Journaux de débogage général** : <*Dossier d'installation du serveur*> `\debug.log`
   - **Journaux de débogage OfficeScan** : `C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Log\ofcdebug.log`

     a. Si le fichier n'existe pas, activez la journalisation du débogage. Dans la bannière de la console Web OfficeScan, cliquez sur le premier « c » du mot « OfficeScan », spécifiez les paramètres du journal de débogage, puis cliquez sur **Enregistrer**.

b. Reproduisez les étapes ayant mené au problème d'accès à la console Web.

c. Obtenez les journaux de débogage.

4. Vérifiez les clés de Registre de Trend Micro Security (pour Mac) en accédant à `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMSM`.

5. Vérifiez les fichiers de base de données et les clés de registre.

   a. Vérifiez que les fichiers suivants existent sous `C:\Program Files \Microsoft SQL Server\MSSQL.x\MSSQL\Data\` :

      - `db_TMSM.mdf`
      - `db_TMSM_log.LDF`

   b. Vérifiez que l'instance de base de données de Trend Micro Security (pour Mac) sur la clé de Registre du serveur Microsoft SQL existe :

      - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\Noms d'instance`
      - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.x\MSSQLServer\CurrentVersion`

6. Envoyez les éléments suivants à Trend Micro :

   - Fichiers du registre

     a. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Microsoft SQL server\TMSM`.

     b. Cliquez sur **Fichier** > **Exporter**, puis enregistrez la clé de Registre dans un fichier portant l'extension `.reg`.

   - Informations sur le serveur
     - Nom et version de votre système d'exploitation
     - Espace disque disponible
     - Mémoire vive disponible
     - Si d'autres plugiciels, tels qu'Intrusion Defense Firewall, sont installés

7. Redémarrez les services Trend Micro Security (pour Mac).

   a. Accédez à <*Dossier d'installation du serveur*>.

   b. Double-cliquez sur `restart_TMSM.bat`.

   c. Attendez que tous les services redémarrent.

8. Le service Trend Micro Security (pour Mac) doit toujours être en cours d'exécution. Dans le cas contraire, un problème peut survenir avec le service ActiveMQ.

   a. Sauvegardez les données ActiveMQ dans `C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM\apache-activemq\data\*.*`.

   b. Supprimez les données ActiveMQ.

   c. Essayez de redémarrer le service Trend Micro Security (pour Mac) en double-cliquant sur `restart_TMSM.bat`.

   d. Tentez de nouveau d'accéder à la console Web pour vérifier que le problème d'accès a été résolu.

Désinstallation du serveur

Problème :

Le message suivant s'affiche :

```
Impossible de désinstaller le plugiciel. La commande de
désinstallation du plugiciel ne figure pas dans la clé de
Registre.
```

Procédure

1. Ouvrez l'éditeur du Registre et accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`.

2. Redéfinissez la valeur sur `1.0.1000`.

3. Supprimez la clé de Registre du plugiciel, par exemple : `HKEY_LOCAL_MACHINE \SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx`.

4. Redémarrez le service OfficeScan Plug-in Manager.

5. Téléchargez, installez puis désinstallez le plugiciel.

Installation de l'agent

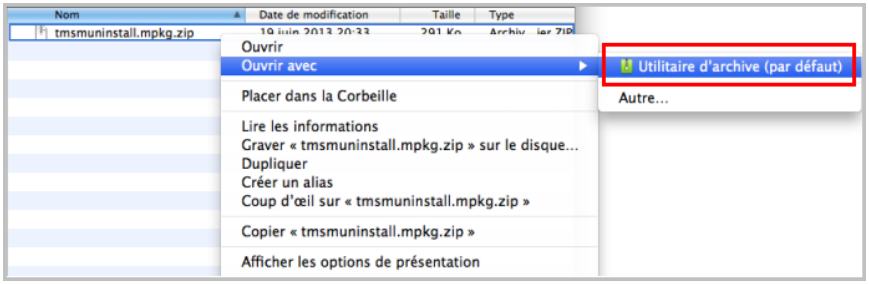
Problème :

Échec de l'installation. Le pack d'installation (`tmsminstall.zip` ou `tmsminstall.mpkg.zip`) a été lancé à l'aide d'un outil d'archivage autre que ceux intégrés au Mac ou via une commande non prise en charge (telle que `unzip`) émise à partir d'un outil de ligne de commande, ce qui a endommagé le dossier (`tmsminstall`) ou le fichier (`tmsminstall.mpkg`) extrait.

Procédure

1. Supprimez le dossier (`tmsminstall`) ou le fichier (`tmsminstall.mpkg`) extrait.

2. Relancer le pack d'installation à l'aide des outils d'archivage intégrés, tels que l'Utilitaire d'archive.



Vous pouvez également lancer le pack à l'aide de la commande suivante :

- Si le pack est `tmsminstall.zip` :

```
ditto -xk <chemin d'accès au fichier tmsminstall.zip>
<dossier de destination>
```

Par exemple :

```
ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/
Desktop
```

- Si le pack est `tmsminstall.mpkg.zip` :

  ```
  ditto -xk <chemin d'accès au fichier
  tmsminstall.mpkg.zip> <dossier de destination>
  ```

  Par exemple :

  ```
  ditto -xk users/mac/Desktop/tmsminstall.mpkg.zip
  users/mac/Desktop
  ```

Erreur générale de l'agent

Problème :

Une erreur ou un problème est survenu(e) sur l'agent.

Procédure

1. Ouvrez<*dossier d'installation de l'agent*>`/Tools`, puis lancez Trend Micro Debug Manager.
2. Suivez les instructions s'affichant à l'écran dans l'outil pour collecter correctement les données.

AVERTISSEMENT!

L'outil ne fonctionnera pas si un utilisateur le déplace vers un autre emplacement sur l'ordinateur Mac. Si l'outil a été déplacé, désinstallez puis installez l'agent Trend Micro Security (pour Mac).

Si l'outil a été copié vers un autre emplacement, supprimez la version copiée, puis exécutez l'outil à partir de son emplacement d'origine.

Base de connaissances Trend Micro

La base de connaissances Trend Micro, accessible à partir du site Web de Trend Micro, contient des réponses constamment actualisées aux questions relatives aux produits. Il est possible d'y poser une question si vous ne trouvez pas de réponse dans la documentation du produit. Accédez à la base de connaissances à l'adresse suivante :

http://esupport.trendmicro.com/en-us/business/default.aspx?locale=fr_FR

Trend Micro met à jour en permanence la base de connaissances et ajoute de nouvelles solutions quotidiennement. Cependant, si vous ne trouvez pas de réponse à une question, vous pouvez décrire le problème dans un e-mail et l'envoyer directement à un ingénieur d'assistance Trend Micro qui l'étudiera et le résoudra dès que possible.

Contacter l'assistance technique

Trend Micro fournit pendant un an une assistance technique, des téléchargements de fichiers de signatures et des mises à jour de programmes à tous les utilisateurs enregistrés. Au terme de cette période, un paiement sera exigé pour renouveler le service de maintenance. Si vous avez besoin d'aide ou si vous avez simplement une question, n'hésitez pas à nous contacter. Vos commentaires sont aussi toujours les bienvenus.

Centres d'assistance dans le monde entier :

http://esupport.trendmicro.com/

Documentation des produits Trend Micro :

http://docs.trendmicro.com/fr-fr/home.aspx

Optimisation de votre demande d'assistance

Lorsque vous contactez Trend Micro, rassemblez les informations suivantes pour accélérer la résolution de vos problèmes :

- Versions de Microsoft Windows et du Service Pack
- Type de réseau

- Marque de l'ordinateur, modèle et tout matériel complémentaire connecté à votre ordinateur
- Mémoire et espace disque disponibles sur votre ordinateur
- Description détaillée de l'environnement d'installation
- Texte exact du message d'erreur affiché
- Étapes permettant de reproduire le problème

Contact

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

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

Numéro gratuit : +1 (800) 228-5651 (ventes) Appel vocal : +1 (408) 257-1500 (ligne principale) Télécopie : +1 (408) 257-2003

Adresse Web : www.trendmicro.com

E-mail : support@trendmicro.com

Centre d'informations de sécurité

Des informations de sécurité complètes sont disponibles sur le site Web de Trend Micro :

- Liste des virus et des codes mobiles malveillants actuellement « en circulation » ou actifs
- Canulars informatiques
- Informations sur les menaces Web
- Rapport hebdomadaire sur les virus

- Encyclopédie virale contenant une liste complète des noms et des symptômes des virus et codes mobiles malveillants connus

  http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=fr&tab=malware

- Glossaire terminologique

TrendLabs

Les TrendLabs^{SM} constituent le centre d'assistance et de recherche antivirus mondial de Trend Micro. Présent sur trois continents, les TrendLabs emploient plus de 250 chercheurs et ingénieurs qui travaillent jour et nuit pour vous fournir service et assistance ainsi qu'à chaque client de Trend Micro.

Les TrendLabs fournissent les services après-vente suivants :

- Mises à jour régulières des fichiers de signatures pour tous les virus et codes malveillants connus, « en cage » et « en circulation »
- Aide d'urgence en cas d'épidémie virale
- Contact par e-mail avec les ingénieurs antivirus
- Base de connaissances de Trend Micro en ligne, répertoriant les problèmes techniques connus

Les TrendLabs ont obtenu la certification d'assurance qualité ISO 9002.

Commentaires relatifs à la documentation

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 Trend Micro, veuillez consulter le site suivant°:

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

Annexe A

Prise en charge IPv6 de Trend Micro Security (pour Mac)

L'annexe est un document incontournable pour les utilisateurs souhaitant déployer Trend Micro Security (pour Mac) dans un environnement qui prend en charge l'adressage IPv6. Cette annexe contient des informations sur les limites de la prise en charge d'IPv6 par Trend Micro Security (pour Mac).

Trend Micro suppose que le lecteur est familiarisé avec les concepts IPv6 et les tâches exigées lors de la mise en place d'un réseau prenant en charge l'adressage IPv6.

Prise en charge IPv6 des agents et du serveur Trend Micro Security (pour Mac)

Prise en charge IPv6 de Trend Micro Security (pour Mac) à partir de la version 2.0. Les versions plus anciennes de Trend Micro Security (pour Mac) ne prennent pas en charge l'adressage IPv6. La prise en charge d'IPv6 est automatique active après l'installation ou la mise à niveau d'agents ou de serveur Trend Micro Security (pour Mac) qui répondent aux exigences IPv6.

Configuration minimale requise pour un serveur Trend Micro Security (pour Mac) en IPv6 pur

Le serveur Trend Micro Security (pour Mac) doit être installé avec un serveur OfficeScan dont la version prend en charge IPv6.

IPv6 est pris en charge par OfficeScan à partir de la version 10.6. Les versions précédentes d'OfficeScan compatibles avec Trend Micro Security (pour Mac) (consultez la rubrique *Configuration minimale requise pour l'installation du serveur à la page 2-2*) ne prennent pas en charge l'adressage IPv6.

Consultez la documentation d'OfficeScan 10.6 ou version ultérieure pour obtenir des informations détaillées à propos de la prise en charge d'IPv6.

Configuration minimale requise pour un agent Trend Micro Security (pour Mac) en IPv6 pur

Toutes les versions de Mac OS X prises en charge par l'agent Trend Micro Security (pour Mac) prennent également en charge IPv6.

Il est préférable pour l'agent d'avoir à la fois des adresses IPv4 et IPv6 puisque certaines entités auxquelles il se connecte ne prennent en charge que l'adressage IPv4.

Limitations pour serveur en IPv6 pur

La table suivante énumère les limitations qui s'appliquent lorsque le serveur Trend Micro Security (pour Mac) ne possède qu'une adresse IPv6.

TABLEAU A-1. Limitations pour serveur en IPv6 pur

ÉLÉMENT	LIMITATION
Gestion des agents	Un serveur en IPv6 pur ne peut pas gérer d'agents en IPv4 pur.
Mises à jour et gestion centralisée	Un serveur en IPv6 pur ne peut se mettre à jour depuis des sources de mise à jour en IPv4 pur ou transmettre des données à des produits de gestion centrale en IPv4 pur, tels que : • serveur ActiveUpdate de Trend Micro • toute source de mise à jour personnalisée en IPv4 pur • Control Manager 6.0 en IPv4 pur
Enregistrement, activation et renouvellement d'un produit	Un serveur en IPv6 pur ne peut se connecter au serveur d'enregistrement en ligne Trend Micro afin d'enregistrer le produit, obtenir la licence et activer/renouveler la licence.
Connexion proxy	Un serveur en IPv6 pur ne peut se connecter via un serveur proxy en IPv4 pur.

La plupart de ces limitations peuvent être contournées en configurant un serveur proxy à double pile qui peut effectuer des conversions entre adresses IPv4 et IPv6 (tel que DeleGate). Placez le serveur proxy entre le serveur Trend Micro Security (pour Mac) et les entités auxquelles il se connecte ou qu'il traite.

Limitations pour agent en IPv6 pur

La table suivante énumère les limitations qui s'appliquent lorsque les agents ne possèdent qu'une adresse IPv6.

TABLEAU A-2. Limitations pour agent en IPv6 pur

ÉLÉMENT	LIMITATION
Serveur parent	Les agents en IPv6 pur ne peuvent être gérés par un serveur en IPv4 pur.
Mises à jour	Un agent en IPv6 pur ne peut se mettre à jour depuis des sources de mise à jour en IPv4 pur, telles que : • serveur ActiveUpdate de Trend Micro • un serveur Trend Micro Security (for Mac) en IPv4 pur
Requêtes de l'évaluation de la réputation de sites Web	Un agent en IPv6 pur ne peut envoyer de requêtes de l'évaluation de la réputation de sites Web à Trend Micro Smart Protection Network.
Connexion proxy	Un agent en IPv6 pur ne peut se connecter via un serveur proxy en IPv4 pur.
Déploiement de l'agent	Impossible pour Apple Remote Desktop de déployer l'agent vers des ordinateurs en IPv6 pur car ces ordinateurs apparaissent constamment hors ligne.

La plupart de ces limitations peuvent être contournées en configurant un serveur proxy à double pile qui peut effectuer des conversions entre adresses IPv4 et IPv6 (tel que DeleGate). Placez le serveur proxy entre les agents et les entités auxquelles ils se connectent.

Configuration d'adresses IPv6

La console Web vous permet de configurer une adresse IPv6 ou une plage d'adresses IPv6. Voici quelques instructions de configuration.

- Trend Micro Security (pour Mac) accepte les présentations standards d'adresses IPv6.

  Par exemple :

  ```
  2001:0db7:85a3:0000:0000:8a2e:0370:7334
  ```

  ```
  2001:db7:85a3:0:0:8a2e:370:7334
  ```

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```

- Trend Micro Security (pour Mac) accepte également les adresses IPv6 link-local, telles que :

  ```
  fe80::210:5aff:feaa:20a2
  ```

  AVERTISSEMENT!

  Soyez prudent lorsque vous spécifiez une adresse IPv6 link-local car, même si Trend Micro Security (pour Mac) accepte cette adresse, elle pourrait ne pas fonctionner comme prévu dans certaines circonstances. Par exemple, les agents ne peuvent pas se mettre à jour depuis une source de mise à jour si celle-ci se trouve sur un autre segment réseau et qu'elle est identifiée par son adresse IPv6 link-local.

- Lorsque l'adresse IPv6 fait partie d'une URL, placez l'adresse entre crochets.
- Pour les plages d'adresses IPv6, un préfixe et une longueur de préfixe sont généralement requis.

Écrans affichant des adresses IP

L'arborescence agent affiche les adresses IPv6 des agents sous la colonne **Adresse IPv6**.

Annexe B

Terminologie et concepts liés au produit

Les éléments contenus dans cette annexe fournissent plus d'informations à propos des produits et technologies Trend Micro.

IntelliScan

IntelliScan est une méthode d'identification des fichiers à scanner. Pour les fichiers exécutables (par exemple, `.exe`), le véritable type du fichier est déterminé en fonction de son contenu. Pour les fichiers non exécutables (au format `.txt` par exemple), le véritable type du fichier est déterminé en fonction de son en-tête.

IntelliScan offre les avantages suivants :

- Optimisation des performances : IntelliScan n'affecte pas les applications du point final car il exploite au minimum les ressources système de l'ordinateur.
- Durée de scan réduite : comme IntelliScan est capable d'identifier le type réel des fichiers, il ne scanne que les fichiers réellement vulnérables aux infections. La durée du scan s'en trouve considérablement réduite, puisque tous les fichiers ne sont pas concernés.

Fichiers non nettoyables

Le moteur de scan antivirus ne peut pas nettoyer les fichiers suivants :

Fichier non nettoyable	Explication et solution
Fichiers infectés par des vers	Un ver informatique est un programme (ou ensemble de programmes) autonome qui peut répandre des copies fonctionnelles de lui-même ou de ses segments au sein d'autres systèmes informatiques. La propagation se produit généralement par le biais de connexions réseau ou de pièces jointes d'e-mails. Les vers ne peuvent pas être nettoyés car le fichier constitue un programme autonome. **Solution** : Trend Micro recommande de supprimer les vers.
Fichiers infectés protégés en écriture	**Solution** : supprimez la protection en écriture pour autoriser l'agent Trend Micro Security (pour Mac) à nettoyer le fichier.

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
Fichiers protégés par mot de passe	Inclut les fichiers compressés ou les fichiers protégés par mot de passe. **Solution** : supprimez la protection par mot de passe pour autoriser l'agent Trend Micro Security (pour Mac) à nettoyer ces fichiers.
Fichiers de sauvegarde	Les fichiers possédant une extension RB0~RB9 sont des copies de sauvegarde des fichiers infectés. L'agent Trend Micro Security (pour Mac) crée une sauvegarde du fichier infecté au cas où le virus/programme malveillant l'endommagerait au cours du processus de nettoyage. **Solution** : si l'agent Trend Micro Security (pour Mac) a réussi à nettoyer le fichier infecté, vous n'avez pas besoin de conserver la copie de sauvegarde. Si l'ordinateur fonctionne correctement, vous pouvez supprimer le fichier de sauvegarde.

Index