TREND MICRO

10.0 Worry-Free™ Business Security Éditions Standard et Advanced

Service Pack 1

Manuel de l'administrateur

Securing Your Journey to the Cloud

Protected Cloud

Web Security

Document n° : WFEM108677/190617

Date de publication : Juin 2019

Protégé par le brevet américain n° : 5 951 698 et 7 188 369

Cette documentation présente les fonctionnalités principales du produit et/ou fournit les instructions d'installation pour un environnement de production. Lisez attentivement cette documentation avant d'installer ou d'utiliser le produit.

Pour plus d'informations concernant l'utilisation des fonctionnalités spécifiques de produit, consultez notre Trend Micro Centre d'aide en ligne et/ou notre Trend Micro base de connaissances.

Trend Micro cherche constamment 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.

Évaluez cette documentation sur le site Web suivant :

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

Table des matières

Préface

Chapitre 1: Présentation de Worry-Free Business Security Standard et Advanced

Chapitre 2: Mise en route

Chapitre 3: Installation des agents

Chapitre 4: Gestion des dispositifs

Chapitre 5: Gestion des paramètres de sécurité de base des agents Security Agent

Chapitre 6: Gestion des param. sécurité de base des MSA (Advanced uniq.)

Chapitre 7: Gestion des scans

Chapitre 8: Gestion des mises à jour

Chapitre 9: Utilisation de l'État actuel

Chapitre 10: Gestion des notifications

Chapitre 11: Gestion des paramètres généraux

Chapitre 12: Utilisation des journaux et des rapports

Chapitre 13: Exécution des tâches administratives

Chapitre 14: Utilisation des outils de gestion

Annexe A: Icône de Security Agent

Annexe B: Prise en charge d'IPv6 dans Worry-Free Business Security

Annexe C: Assistance technique

Annexe D: Terminologie et concepts du produit

Index

Préface

Préface

Bienvenue dans le *Manuel de l'administrateur* de Trend Micro™ Worry-Free™ Business Security. Ce document aborde les informations relatives au démarrage, les procédures d'installation des agents, ainsi que la gestion du serveur Security Server et de l'agent.

Documentation relative à Worry-Free Business Security

La documentation relative à Worry-Free Business Security inclut les éléments suivants :

TABLEAU 1. Documentation relative à Worry-Free Business Security

DOCUMENTATION	DESCRIPTION
Guide d'installation et de mise à niveau	document PDF qui aborde les éléments requis et les procédures d'installation du serveur Security Server, ainsi que les informations nécessaires pour la mise à niveau du serveur et des agents.
Manuel de l'administrateur	document PDF qui aborde les informations relatives au démarrage, les procédures d'installation client et l'administration du serveur Security Server et des agents.
Aide	Fichiers HTML compilés au format WebHelp ou CHM contenant des descriptions de procédures, des conseils d'utilisation et des informations relatives aux champs
Fichier Lisez-moi	Contient une liste des problèmes connus et les étapes d'installation de base. Il peut aussi contenir des informations relatives au produit qui n'ont pas pu être intégrées à temps à l'aide ou à la documentation imprimée.
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

Téléchargez la dernière version des documents PDF et du fichier Lisez-moi à l'adresse suivante:

http://docs.trendmicro.com/fr-fr/smb/worry-free-business-security.aspx

Public visé

La documentation relative à Worry-Free Business Security est destinée aux utilisateurs suivants :

- **Administrateurs de sécurité** : responsable de l'administration de Worry-Free Business Security, y compris de la gestion et de l'installation de Security Server 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 Security Agent sur leurs ordinateurs. Leur niveau de compétence informatique varie: débutant, expérimenté, etc.

Conventions typographiques du document

Pour faciliter la recherche et la compréhension des informations, la documentation relative à Worry-Free Business Security utilise les conventions suivantes :

TABLEAU 2. Conventions typographiques 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
<Texte>	Indique que le texte entre crochets doit être remplacé par les données réelles. Par exemple, `C:\Program Files \<file_name>` peut correspondre à `C:\Program Files \sample.jpg`.

Nomenclature	Description
 **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

Chapitre 1

Présentation de Worry-Free™ Business Security Standard et Advanced

Ce chapitre offre un aperçu de Worry-Free Business Security (Worry-Free Business Security).

Présentation de Trend Micro Worry-Free Business Security

Trend Micro Worry-Free Business Security (Worry-Free Business Security) protège les utilisateurs et actifs de PME-PMI contre le vol de données, l'usurpation d'identité, les sites Web dangereux et le spam (Advanced uniquement).

Ce document fournit des informations pour les versions Standard et Advanced de Worry-Free Business Security. Les sections et chapitres correspondant à la version Advanced sont signalés par « (Advanced uniquement) ».

Fonctionnant sous Trend Micro Smart Protection Network, Worry-Free Business Security est :

- **Plus sûr** : il empêche les virus, les spywares, les spams (Advanced uniquement) et les menaces Web d'atteindre les clients. Le filtrage d'URL bloque l'accès aux sites Web dangereux et contribue à améliorer la productivité de l'utilisateur.
- **Plus intelligent** : les scans rapides et les mises à jour continues bloquent les nouvelles menaces et minimisent l'impact sur les clients.
- **Plus simple** : facile à déployer et ne nécessitant aucune administration, Worry-Free Business Security détecte les menaces plus efficacement afin que vous puissiez vous concentrer sur vos activités et non sur la sécurité.

Nouveautés de cette version

Le tableau suivant décrit les nouvelles fonctionnalités et améliorations incluses dans cette version de Worry-Free Business Security.

Fonctionnalité/ amélioration	Description
Scan agressif	Worry-Free Business Security propose désormais une fonction de scan agressif pour une recherche et un nettoyage plus approfondis des points de terminaison infectés. Voir *Utilisation de l'arborescence de dispositifs à la page 4-2* et *Utilisation des commandes des dispositifs à la page 4-5* pour obtenir des informations supplémentaires.
Protection améliorée contre les programmes malveillants sans fichier	Worry-Free Business Security utilise désormais les technologies les plus récentes de prévention contre les programmes malveillants sans fichier afin de protéger vos endpoints contre les attaques sans fichier.
Prise en charge du système d'exploitation	Worry-Free Business Security prend désormais en charge l'installation de Security Server et de l'agent sur les systèmes d'exploitation suivants : • Mise à jour du 10 mai 2019 de Windows 10 • Windows Server 2019

Fonctionnalités et avantages principaux

Worry-Free Business Security fournit les fonctionnalités et avantages suivants :

Trend Micro™ Smart Protection Network™

Trend Micro™ Smart Protection Network™ est une infrastructure de sécurité du contenu en ligne de nouvelle génération conçue pour protéger les clients contre les risques de sécurité et les menaces Internet. Il repose sur des solutions à la fois sur site et Trend Micro hébergées pour protéger les utilisateurs, qu'ils se trouvent sur le réseau, chez eux ou en voyage. Smart Protection Network utilise des agents légers pour accéder à une combinaison unique de technologies en ligne de messagerie, de File Reputation et de sites Web, ainsi que de bases de données de menaces. La protection des clients est

automatiquement mise à jour et renforcée alors qu'un nombre croissant de produits, de services et d'utilisateurs accèdent au réseau, créant un service de protection qui offre à ses utilisateurs une surveillance ciblée en temps réel.

Pour plus d'informations relatives au Smart Protection Network, veuillez vous reporter à :

http://www.trendmicro.fr/technologie-innovation/notre-technologie/smart-protection-network/

Services de File Reputation

Les services de File Reputation vérifient la réputation de chaque fichier par rapport à une base de données en ligne étendue. Les informations concernant les programmes malveillants étant stockées en ligne, elles sont immédiatement disponibles pour tous les utilisateurs. Des réseaux d'acheminement de contenu hautement performants et des serveurs cache locaux garantissent une latence minimale lors du processus de vérification. L'architecture Internet-client offre une protection immédiate et élimine le fardeau que représente le déploiement de fichiers de signatures tout en réduisant de façon significative l'impact général sur le client.

Les agents Security Agent doivent être en mode Smart Scan pour utiliser les services de réputation de fichiers. Ces agents sont appelés **agents Smart Scan** dans le présent document. Les agents qui ne sont pas en mode Smart Scan n'utilisent pas les services de réputation de fichiers et sont appelés **agents de scan traditionnels**. Les administrateurs Worry-Free Business Security peuvent configurer tout ou partie des agents pour qu'ils soient en mode Smart Scan.

Services de réputation de sites Web

Dotée de l'une des plus grandes bases de données de réputation de domaine du monde, la technologie de réputation de sites Web de Trend Micro assure le suivi de la crédibilité des domaines Web en attribuant un score de réputation dépendant de facteurs tels que l'ancienneté du site Web concerné,

l'historique de ses changements d'emplacement et les indications d'activités suspectes mises en lumière par l'analyse de comportement des programmes malveillants. La réputation des sites Web continue ensuite à analyser les sites et à bloquer les utilisateurs tentant d'accéder à ceux qui sont infectés. Les fonctionnalités de réputation de sites Web permettent de garantir que les pages consultées par les utilisateurs sont sûres et exemptes de menaces Web, telles que les programmes malveillants, les spywares et les attaques de phishing visant à duper les utilisateurs afin de leur faire divulguer des informations personnelles. Pour une plus grande précision et une réduction des faux positifs, la technologie de réputation de sites Web de Trend Micro affecte des scores de réputation à des pages et liens spécifiques de chaque site, plutôt que de classer comme suspects des sites entiers ou de les bloquer. En effet, il arrive souvent que seule une portion d'un site légitime ait été piratée et les réputations peuvent changer de manière dynamique au fil du temps

Les agents soumis aux stratégies de réputation de sites Web utilisent les services de réputation de sites Web. Les administrateurs Worry-Free Business Security peuvent soumettre tout ou partie des agents aux stratégies de réputation de sites Web.

Réputation de messagerie (Advanced uniquement)

La technologie de réputation de messagerie de Trend Micro valide les adresses IP en les comparant aux sources de spam connues recensées dans une base de données de réputation et en utilisant un service dynamique pouvant accéder en temps réel à la réputation des expéditeurs de courrier électronique. Les évaluations de réputation sont améliorées grâce à une analyse continue du « comportement », du cadre d'activité et de l'historique des adresses IP. Les e-mails malveillants sont bloqués en ligne, en fonction de l'adresse IP de l'expéditeur, ce qui empêche les menaces (par exemple zombies et réseaux de zombies) d'atteindre le réseau ou le PC d'un utilisateur.

La technologie d'évaluation de la réputation de messagerie identifie le spam en fonction de la réputation du MTA d'origine. Cela permet de décharger Security Server de la tâche. Lorsque l'évaluation de la réputation de messagerie est activée, l'ensemble du trafic SMTP entrant est vérifié par les

bases de données IP pour vérifier si l'adresse IP d'origine est saine ou si elle a été désignée comme vecteur de spam connu.

L'évaluation de la réputation de messagerie propose les deux niveaux de service :

- **Standard** :le service standard utilise une base de données pour évaluer la réputation d'environ deux millions d'adresses IP. Les adresses IP ayant été correctement associées à la remise de messages de spam sont ajoutées à la base de données et rarement supprimées.
- **Avancé** : le service avancé est un service DNS reposant sur des demandes, comme le service standard. La clé de voûte de ce service est la base de données de réputation standard, associée à la base de données de réputation dynamique, en temps réel, qui bloque les messages des sources de spam connues et suspectes.

Lorsqu'un message électronique provenant d'une adresse IP bloquée ou suspecte est détecté, Email Reputation Services le bloque avant qu'il n'atteigne votre infrastructure de messagerie. Si les services ERS bloquent les messages électroniques d'une adresse IP que vous pensez sûre, ajoutez cette adresse à la liste des adresses IP approuvées.

Smart Feedback

Trend Micro Smart Feedback assure la communication permanente entre les produits Trend Micro et les centres et technologies de recherche des menaces de la société, opérationnels 24h sur 24 et 7 jours sur 7. Chaque nouvelle menace identifiée par un contrôle de réputation de routine d'un seul client met automatiquement à jour toutes les bases de données de menaces de Trend Micro, et empêche que cette menace ne survienne à nouveau chez un autre client.

Grâce à l'analyse constante des données de menaces collectées par son vaste réseau mondial de clients et de partenaires, Trend Micro assure une protection automatique et en temps réel contre les dernières menaces, offrant ainsi une sécurité « unifiée », très semblable à une surveillance de voisinage automatisée qui implique la communauté dans la protection de chacun. La confidentialité des informations personnelles ou

professionnelles d'un client est toujours protégée car les données sur les menaces qui sont collectées reposent sur la réputation de la source de communication et non sur le contenu de la communication en question.

Exemples d'informations envoyées à Trend Micro :

- Sommes de contrôle de fichiers
- les sites Web visités
- Informations sur les fichiers, notamment la taille et le chemin
- Noms des fichiers exécutables

Vous pouvez interrompre à tout moment votre participation au programme depuis la console Web.

Pour plus de détails, voir *Participation au programme Smart Feedback à la page 13-7*.

Conseil

Il n'est pas obligatoire de participer à Smart Feedback pour protéger vos points finaux. La participation de l'utilisateur est facultative et il peut y mettre fin à tout moment. Trend Micro recommande aux utilisateurs de participer à Smart Feedback afin d'assurer une meilleure protection globale à tous les clients Trend Micro.

Pour plus d'informations relatives au Smart Protection Network, veuillez vous reporter à :

http://www.trendmicro.fr/technologie-innovation/notre-technologie/smart-protection-network/

Filtrage d'URL

Le filtrage d'URL vous aide a contrôler l'accès aux sites Web pour réduire les périodes d'improductivité du personnel, diminuer l'utilisation de la bande passante et créer un environnement Internet plus sûr. Vous pouvez définir

un niveau de protection par filtrage URL ou personnaliser les types de sites Web que vous souhaitez surveiller.

Avantages de la protection

Le tableau suivant décrit comment les divers composants de Worry-Free Business Security protègent vos ordinateurs contre les menaces.

TABLEAU 1-1. Avantages de la protection

MENACE	PROTECTION
Virus/programmes malveillants. Virus, chevaux de Troie, vers, backdoors et rootkits **Spywares/graywares**. Spyware, numéroteurs, outils de piratage, applications de piratage de mots de passe, adware, canulars et enregistreurs de frappe	Scans basés sur fichier (scan en temps réel, scan manuel et scan programmé)
Menaces de sécurité transmises par e-mail	**Scan de la messagerie POP3** de Security Agent
Vers/virus de réseau et intrusions	Pare-feu de Security Agent
Sites Web/sites de phishing potentiellement dangereux	Réputation de sites Web et filtrage d'URL de Security Agent
Menaces de sécurité qui se répandent par l'intermédiaire des clés USB et autres dispositifs externes	Contrôle des dispositifs de Security Agent
Comportement malveillant	Surveillance des comportements de Security Agent
Logiciels de rançon ciblant des documents qui s'exécutent sur des endpoints	Surveillance des comportements et apprentissage automatique prédictif dans l'agent Security Agent

Description des menaces

Les entreprises ne disposant pas d'un personnel de sécurité dédiée et appliquant des stratégies de sécurité peu strictes sont de plus en plus exposées aux menaces, même si elles mettent en œuvre une infrastructure de sécurité de base. Lorsqu'elles sont détectées, ces menaces se sont peut-être déjà répandues à de nombreuses ressources informatiques et leur élimination complète est susceptible de demander un temps et des efforts considérables. Les coûts imprévus liés à l'élimination de ces menaces peuvent également s'avérer faramineux.

De données de sécurité réseau et les serveurs en ligne de Trend Micro composant Trend Micro Smart Protection Network permettent d'identifier les menaces de nouvelle génération et d'y répondre.

Virus et programmes malveillants

Il existe des dizaines de milliers de virus/programmes malveillants et de nouveaux sont créés chaque jour. Alors qu'à une époque, ils étaient plus courants dans DOS ou Windows, 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.

- **Canular** : Programme similaire aux virus qui manipule souvent l'apparence des éléments affichés sur l'écran de l'ordinateur.
- **Virus/programmes malveillants probables** : fichiers suspects ayant certaines des caractéristiques d'un virus/programme malveillant. Pour plus d'informations, consultez l'Encyclopédie des menaces de Trend Micro :

  http://about-threats.trendmicro.com/threatencyclopedia.aspx
- **Rootkit** : Un programme (ou un ensemble de programmes) qui installe et exécute un code sur un système à l'insu de l'utilisateur et sans son autorisation. Il utilise une technique de camouflage pour maintenir une présence persistante et indétectable sur la machine. Les rootkits

n'infectent pas les machines. Ils cherchent plutôt à fournir un environnement indétectable afin d'exécuter un code malveillant. Les rootkits sont installés sur les systèmes via un piratage psychologique, lors de l'exécution de programmes malveillants ou simplement en naviguant sur un site Web malveillant. Une fois installé, un pirate peut pratiquement effectuer n'importe quelle action sur le système, notamment l'accès à distance et l'espionnage. Il peut également masquer des processus, des fichiers, des clés de registre et des canaux de communication.

- **Cheval de Troie** : Ce type de menace utilise souvent les ports pour accéder aux ordinateurs ou aux programmes exécutables. Les programmes Cheval de Troie ne se répliquent pas, mais résident dans des systèmes pour effectuer des opérations malveillantes, telles que l'ouverture des ports aux pirates. Les solutions antivirus conventionnelles peuvent détecter et supprimer les virus, mais pas les chevaux de Troie, notamment ceux qui ont déjà pénétré votre système.
- **Virus**: 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.
  - **Code malveillant ActiveX** : Code résidant dans les pages Web qui exécutent des contrôles ActiveX™
  - **Virus du secteur d'amorçage** : virus qui infecte le secteur d'amorçage d'une partition ou d'un disque.
  - **Virus infectant les fichiers COM et EXE** : Programme exécutable avec extensions `.com` ou `.exe`
  - **Code malveillant Java** : Virus indépendant du système d'exploitation écrit ou imbriqué dans Java™.
  - **Virus de macro** : virus chiffré comme application macro qui est souvent inclus dans un document.
  - **Utilitaire de compression** : Programme exécutable compressé et/ou encodé Windows ou Linux™, souvent un cheval de Troie. La compression de fichiers exécutables rend l'utilitaire de compression plus difficile à détecter par les logiciels antivirus.

- **Virus de test** : Fichier inerte agissant comme un véritable virus et pouvant être détecté par les logiciels antivirus. Utilise des virus de test tels que le script de test EICAR afin de vérifier que le scan de votre installation antivirus fonctionne correctement.
- Virus **VBScript**, **JavaScript** ou **HTML** : Réside sur des pages Web et est téléchargé par un navigateur.
- **Vers** : Programme automatique ou ensemble de programmes qui peut répandre des copies fonctionnelles de lui-même ou de ses segments dans d'autres systèmes informatiques, souvent par e-mail.
- **Autres** : Virus/programmes malveillants n'entrant dans aucune des catégories de types de virus/programmes malveillants.

Programmes espions et graywares

Les Points finaux courent des risques liés à des menaces potentielles autres que les virus/programmes malveillants. Les spywares/graywares sont des applications ou fichiers non classés en tant que virus ou chevaux de Troie, mais qui peuvent toutefois avoir un effet négatif sur les performances des clients de votre réseau. Ils font courir un risque significatif à votre entreprise sur le plan de la sécurité et de la confidentialité et peuvent avoir des conséquences judiciaires. Les spywares/graywares 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 du client à des attaques.

Si vous découvrez une application ou un fichier que Worry-Free Business Security ne peut pas détecter comme étant un grayware, mais que vous jugez qu'il en est un, envoyez-le à Trend Micro à l'adresse suivante :

https://success.trendmicro.com/solution/1059565

Type	Description
Programme espion	rassemblent des données telles que des noms d'utilisateurs de comptes et des mots de passe pour les transmettre à des tiers.

Type	Description
Adware	affiche des publicités et rassemble des données telles que les préférences de navigation de l'utilisateur afin de cibler les publicités destinées à cet utilisateur via un navigateur Web.
Composeur de numéros	Modifie les paramètres Internet du client et peut l'obliger 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.
Canular	Entraîne un comportement anormal du client, comme la fermeture et l'ouverture du tiroir de CD-ROM et l'affichage de nombreuses boîtes de message.
Outil de piratage	aide les pirates informatiques à s'infiltrer sur les ordinateurs.
Outil d'accès à distance	aide les pirates informatiques à accéder à distance à plusieurs ordinateurs et à les contrôler.
Application de craquage de mots de passe	aide les pirates informatiques à déchiffrer des noms d'utilisateurs et des mots de passe.
Autres	Autres types de programmes potentiellement malveillants.

Spam

Les messages de spam sont des messages indésirables, souvent de nature commerciale, envoyés à l'aveugle à diverses listes de publipostage, à des individus ou à des groupes de discussion. Il existe deux types de spam : les messages électroniques commerciaux non sollicités ou les messages envoyés en nombre.

Intrusions

Les intrusions font référence à des entrées dans les réseaux ou les clients, de force ou sans autorisation. Elles peuvent également impliquer le contournement de la sécurité d'un réseau ou d'un client.

Comportement malveillant

Un comportement malveillant signifie que des modifications non autorisées sont apportées par un logiciel au système d'exploitation, aux entrées de registre, aux autres logiciels, aux fichiers et aux dossiers.

Points d'accès fictifs

Les points d'accès fictifs (également connus sous l'expression « Evil Twin ») représentent des points d'accès Wi-Fi corrompus qui semblent légitimes au départ, mais qui ont en fait été conçus par des pirates pour écouter les communications sans fil.

Incidents de type phishing

Le phishing est une forme de fraude se développant rapidement qui vise à duper les internautes en reproduisant à l'identique l'apparence de sites Web légitimes afin de divulguer des informations personnelles.

On rencontre généralement le cas suivant : un utilisateur non averti reçoit un e-mail manifestement urgent (et ayant l'air authentique) lui notifiant un problème relatif à son compte qu'il doit résoudre immédiatement sous peine de fermeture du compte. L'e-mail contient une URL permettant d'accéder à un site Web ressemblant en tout point au véritable site. il est facile de copier un message et un site Web légitimes, puis de modifier le serveur principal où sont collectées les données envoyées.

Le message invite l'utilisateur à se connecter au site et à confirmer des informations sur le compte. Un pirate reçoit les données fournies par l'utilisateur, par exemple, un identifiant, un mot de passe, un numéro de carte de crédit ou de sécurité sociale.

Ce genre de fraude est rapide, peu onéreux et simple d'exécution. C'est une méthode également relativement rentable pour les criminels qui la pratiquent. Le phishing est difficile à détecter même pour les utilisateurs avertis. Il en est de même pour les autorités judiciaires. Pire encore, il est quasiment impossible de poursuivre ses auteurs en justice.

Veuillez signaler à Trend Micro tout site Web susceptible de pratiquer des activités de phishing. Voir *Envoi de contenu suspect à Trend Micro à la page C-5* pour obtenir des informations complémentaires.

Attaques de publipostage

Les virus/programmes malveillants de messagerie ont la capacité de se propager via les messages électroniques en automatisant les clients de messagerie de l'ordinateur infecté ou en propageant eux-mêmes les virus/programmes malveillants. Le publipostage correspond à une situation dans laquelle une infection se propage rapidement dans un environnement Microsoft Exchange. Trend Micro propose un moteur de scan spécialement conçu pour détecter le comportement que présentent généralement ces virus. Ces comportements sont enregistrés dans le fichier de signatures de virus mis à jour à l'aide des serveurs ActiveUpdate de Trend Micro.

Vous pouvez activer Messaging Security Agent (Advanced uniquement) pour exécuter une action particulière dès qu'un comportement de publipostage est détecté. Cette action est prioritaire sur toute autre action. L'action par défaut définie pour les attaques de type publipostage massif est de supprimer le message entier.

Par exemple : vous pouvez configurer Messaging Security Agent pour placer des messages en quarantaine lorsqu'ils sont identifiés comme étant infectés par un vers ou un cheval de Troie. Vous avez également la possibilité d'activer l'option de détection des comportements de publipostage de masse et de paramétrer l'agent pour qu'il supprime tous les messages présentant ce comportement. L'agent peut par exemple recevoir un message contenant un ver comme une variante de MyDoom. Ce ver utilise son propre moteur de transport SMTP pour être transmis vers des adresses électroniques collectées dans l'ordinateur infecté. Lorsque l'agent détecte le comportement de publipostage du ver MyDoom, il supprime le message électronique contenant le ver contrairement à l'action de quarantaine configurée pour les vers ne présentant pas de comportement de publipostage.

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. Ainsi, les auteurs de menaces Internet modifient 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 client infecté, l'auteur de cette menace modifie constamment son code pour éviter qu'elle ne soit détectée.

De nos jours, les pirates informatiques, les auteurs de virus, les spammers 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. Le client infecté peut également devenir un vecteur pour transmettre des attaques de phishing ou d'autres activités d'interception d'informations. Entre autres conséquences, cette menace risque d'entamer la confiance dans le commerce sur Internet et dans les transactions qu'il nécessite. 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.

Chapitre 2

Mise en route

Ce chapitre explique comment installer et exécuter la solution Worry-Free Business Security.

Le réseau Worry-Free Business Security

Worry-Free Business Security comprend les éléments suivants :

Serveur Security Server

Security Server est au cœur de la solution Worry-Free Business Security. Le serveur Security Server héberge la console Web, la console Web de gestion centralisée pour la solution Worry-Free Business Security. Security Server installe les agents sur les clients du réseau et, avec ces agents, établit une relation agent-serveur. Security Server permet d'afficher les informations relatives à l'état de sécurité, d'afficher les agents, de configurer la sécurité système et de télécharger des composants à partir d'un emplacement centralisé. Security Server contient aussi une base de données dans laquelle il stocke les journaux des menaces Web détectées qui lui sont signalées par les agents.

Security Server exécute les tâches essentielles suivantes :

- Il installe, surveille et gère les agents.
- Il télécharge la plupart des composants dont les clients ont besoin. Par défaut, le serveur Security Server télécharge les composants depuis le serveur ActiveUpdate de Trend Micro, puis les distribue aux agents.

Serveur de scan

Le serveur Security Server possède un service dénommé Scan Server (Serveur de scan), qui est installé automatiquement lors de l'installation du serveur Security Server. Il n'est ainsi pas nécessaire de l'installer séparément. Le serveur de scan s'exécute sous le nom de processus `iCRCService.exe` et

s'affiche sous l'intitulé **Service Trend Micro Smart Scan** dans Microsoft Management Console.

Lorsque des agents Security Agent utilisent une méthode de scan dénommée **smart scan**, le serveur de scan optimise leur exécution. Le processus smart scan peut être décrit comme suit :

- L'agent Security Agent analyse la présence de menaces de sécurité sur le client à l'aide de **Signatures de l'agent Smart Scan**, une version légère du fichier de signatures de virus traditionnel. Signatures de l'agent Smart Scan contient la plupart des signatures de menaces présentes dans le fichier de signatures de virus.
- Un agent Security Agent dans l'impossibilité de déterminer le risque du fichier lors du scan vérifie ce risque en envoyant une requête au serveur de scan. Le serveur de scan vérifie le risque à l'aide de **Signatures Smart Scan**, qui contient les signatures de menaces non disponibles sur Signatures de l'agent Smart Scan.
- Security Agent met en mémoire cache le résultat de la requête fournie par le serveur de scan afin d'améliorer ses performances.

En hébergeant certaines des définitions de menaces, le serveur de scan permet de réduire la consommation de bande passante des agents Security Agent lors du téléchargement des composants. Au lieu de télécharger le fichier de signatures de virus, les agents Security Agent téléchargent signatures de l'agent Smart Scan, qui est d'une taille considérablement inférieure.

Lorsque les agents Security Agent ne peuvent pas se connecter au serveur de scan, ils envoient leurs requêtes de scan à Trend Micro Smart Protection Network, qui possède la même fonction que le serveur de scan.

Il est impossible de désinstaller le serveur de scan séparément du serveur Security Server. Si vous ne souhaitez pas utiliser le serveur de scan :

1. Sur l'ordinateur de Security Server, ouvrez Microsoft Management Console et désactivez **Service Trend Micro Smart Scan**.
2. Dans la console Web, basculez les agents Security Agent en mode de scan traditionnel en accédant à **Administration** > **Paramètres généraux**

> **Poste de travail/serveur** et en sélectionnant l'option **Désactiver le service Smart Scan**.

Agents

Les agents protègent les clients contre les menaces de sécurité. Les clients incluent les postes de travail, les serveurs et les serveurs Microsoft Exchange. Les agents Worry-Free Business Security sont :

TABLEAU 2-1. Agents Worry-Free Business Security

AGENT	DESCRIPTION
Security Agent	Protège les postes de travail et les serveurs des menaces de sécurité et des intrusions
Messaging Security Agent (Advanced uniquement)	Protège les serveurs Microsoft Exchange contre les menaces de sécurité liées à la messagerie

Un agent dépend du serveur Security Server à partir duquel il a été installé. L'agent envoie les informations relatives à l'état et aux événements en temps réel pour fournir à Security Server les informations les plus récentes concernant le client. Les agents signalent des événements tels que la détection d'une menace, le démarrage, l'arrêt, le lancement d'un scan et la réalisation d'une mise à jour.

Console Web

La console Web est le point central pour la surveillance des agents Security Agent sur le réseau de l'entreprise. Elle présente des paramètres et des valeurs par défaut que vous pouvez configurer en fonction de vos spécifications et exigences de sécurité. La console Web utilise des technologies Internet standard telles que Java, CGI, HTML et HTTP.

Utilisez la console Web pour :

- Déployer des agents sur les endpoints ;
- Organiser les agents par groupes logiques pour les configurer et les gérer tous ensemble ;
- Configurer les paramètres de produits et exécuter un scan manuel sur les endpoints ;
- Recevoir des notifications et consulter les journaux d'activité liées aux menaces ;
- Recevoir des notifications et envoyer des alertes d'épidémies par email lorsque des menaces sont détectées sur les endpoints.

Ouverture de la console Web

Ouvrez la console Web à partir d'un endpoint du réseau à l'aide d'un navigateur Web pris en charge. Pour plus d'informations sur la configuration requise du navigateur, consultez le document *Configuration minimale requise*.

Procédure

1. Sélectionnez l'une des options suivantes pour ouvrir la console Web :
   - Sur le point final qui héberge Security Server, naviguez jusqu'à Poste de travail et cliquez sur le raccourci Worry-Free Business Security.
   - Sur le point final qui héberge Security Server, cliquez sur le **menu Démarrer de Windows** > **Trend Micro Worry-Free Business Security** > **Worry-Free Business Security**.
   - Sur l'un des points finaux du réseau, ouvrez un navigateur Web et saisissez ce qui suit dans la barre d'adresse :

     `https://{Nom_Security_Server ou adresse IP}:{numéro de port}/SMB`

     Par exemple :

     `https://my-test-server:4343/SMB`

`https://192.168.0.10:4343/SMB`

`http://my-test-server:8059/SMB`

`http://192.168.0.10:8059/SMB`

Conseil

Si vous n'utilisez pas SSL, tapez `http` au lieu de `https`. Le port par défaut pour les connexions HTTP est le port 8059 ; pour les connexions HTTPS, il s'agit du port 4343.

Si l'environnement ne peut pas résoudre les noms de serveur par DNS, utilisez le nom du serveur au lieu de l'adresse IP.

L'écran de connexion à Worry-Free Business Security s'affiche dans le navigateur.

2. Saisissez votre mot de passe et cliquez sur **Connexion**.

   Le navigateur Web affiche l'écran **État actuel**.

Que faire ensuite

Si vous ne parvenez pas à accéder à la console Web, vérifiez ce qui suit.

ÉLÉMENTS À VÉRIFIER	DÉTAILS
Mot de passe	Si vous avez oublié votre mot de passe, réinitialisez-le à l'aide de l'outil de réinitialisation du mot de passe de la console. Pour accéder à cet outil sur le serveur Security Server, accédez au dossier Trend Micro Worry-Free Business Security du menu Démarrer de Windows. 

Éléments à vérifier	Détails
Cache du navigateur	Si vous avez procédé à une mise à niveau à partir d'une version antérieure de Worry-Free Business Security, les fichiers de mémoire cache du serveur proxy et du navigateur Web peuvent empêcher le chargement correct de la console Web. Videz la mémoire cache de votre navigateur et celle de tout serveur proxy situé entre Trend Micro Security Server et le point final que vous utilisez pour accéder à la console Web.
Certificat SSL	Vérifiez que votre serveur Web fonctionne correctement. Si vous utilisez SSL, assurez-vous que le certificat SSL est encore valide. Consultez la documentation de votre serveur Web pour plus d'informations.

ÉLÉMENTS À VÉRIFIER	DÉTAILS

Paramètres du répertoire virtuel	Il y a peut-être un problème avec les paramètres du répertoire virtuel si vous exécutez la console Web sur un serveur IIS et que le message suivant s'affiche :
	
	`Impossible d'afficher la page`
	
	`Erreur HTTP 403.1 - Interdit : l'accès en exécution est refusé.`
	
	`Internet Information Services (IIS)`
	
	Ce message peut s'afficher lorsque vous utilisez l'une des adresses suivantes pour accéder à la console :
	
	`http://{nom du serveur}/SMB/`
	
	`http://{nom du serveur}/SMB/default.htm`
	
	Toutefois, la console peut s'ouvrir sans problème avec l'adresse suivante :
	
	`http://{nom du serveur}/SMB/console/html/cgi/cgichkmasterpwd.exe`
	
	Pour résoudre ce problème, vérifiez les permissions d'exécution du répertoire virtuel SMB.
	
	Pour activer des scripts :
	
	1. Ouvrez le gestionnaire Internet Information Services (IIS).
	2. Dans le répertoire virtuel SMB, choisissez **Properties**.
	3. Sélectionnez l'onglet Virtual Directory et définissez les permissions d'exécution sur `Scripts` plutôt que sur `none`. Modifiez aussi les permissions d'exécution du répertoire virtuel d'installation du client.

Navigation dans la console Web

La console Web regroupe les principales sections suivantes :

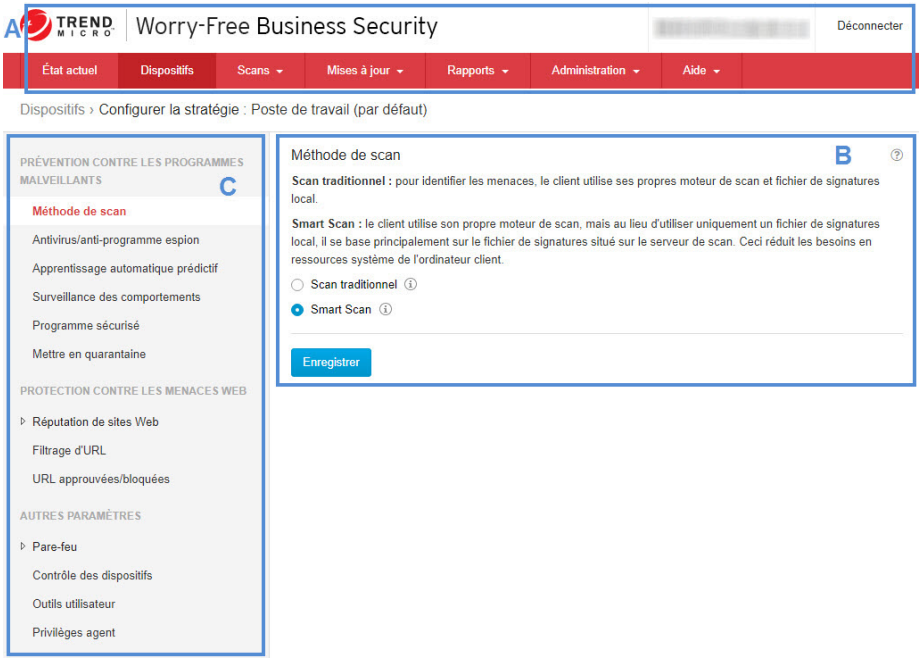


TABLEAU 2-2. Principales sections de la console Web

SECTION	DESCRIPTION
A. Menu principal	Dans la partie supérieure de la console Web se trouve le menu principal. Vous disposez également d'un lien **Déconnexion** qui vous permet de quitter la session en cours.

Section	Description
B. Zone de configuration	La zone de configuration se situe sous les éléments du menu principal. Utilisez cette zone pour sélectionner des options et configurer des paramètres en fonction de l'élément de menu sélectionné.
C. Barre latérale du menu (non disponible sur tous les écrans)	Lorsque vous choisissez un groupe d'agents Security Agent dans l'écran **Dispositifs** et que vous cliquez sur **Configurer la stratégie**, une barre de menus latérale s'affiche. Utilisez cette barre latérale pour configurer les paramètres de sécurité et les scans des postes de travail et des serveurs appartenant au groupe. Dans l'écran **Dispositifs**, lorsque vous choisissez un agent Messaging Security Agent (Advanced uniquement), vous pouvez utiliser la barre latérale pour configurer les paramètres de sécurité et les scans des serveurs Microsoft Exchange.

Tableau 2-3. Section Menu principal

Élément de menu	Description
État actuel	Surveillez l'état de sécurité de l'ensemble de vos agents Security Agent et l'état de fonctionnement du serveur Security Server.
Dispositifs	• Personnalisation des paramètres de sécurité pour agents • Réplication des paramètres entre les groupes
Scans	• Recherche de menaces sur les endpoints • Programmation du scan des clients
Mises à jour	• Consultation du serveur ActiveUpdate de Trend Micro (ou une source de mises à jour personnalisée) pour connaître les derniers composants mis à jour, y compris le fichier de signatures de virus, le moteur de scan, les composants de nettoyage et le programme de l'agent • Configuration de la source de mise à jour • Désignation d'agents Security Agent comme agents de mise à jour
Rapports	Générez des rapports pour garder le suivi des menaces et d'autres événements relatifs à la sécurité

Élément de menu	Description
Administration	• Configuration de notifications en cas d'événements anormaux liés à des menaces ou au système • Configuration de paramètres globaux pour faciliter la maintenance • Utilisation d'outils d'administration afin de gérer la sécurité sur le réseau et les clients • Affichage des informations de licence du produit, gestion du mot de passe de l'administrateur et préservation de l'environnement de l'entreprise pour l'échange d'informations numériques en rejoignant le programme Smart Feedback • Automatisation des mises à jour de produit et notification envoyée aux utilisateurs lorsqu'un nouveau package de mise à jour est disponible
Aide	• Rechercher un contenu particulier et des rubriques • Afficher le manuel de l'administrateur • Accéder aux informations les plus récentes dans la base de connaissances (KB) • Afficher les informations relatives à la sécurité, à la vente, à l'assistance et à la version.

Icônes de la console Web

Le tableau ci-dessous décrit les icônes affichées sur la console Web et explique leur utilisation.

Tableau 2-4. Icônes de la console Web

Icône	Description
	Icône d'aide. permet d'ouvrir l'aide en ligne.
	Icône Actualiser. permet d'actualiser l'affichage de l'écran.

Icône	Description
	Icône Développer/Réduire la section. permet d'afficher/de masquer les sections. Il est possible de ne développer qu'une section à la fois.
	Icône Informations. permet d'afficher les informations relatives à un élément particulier.
	Icône Personnaliser les notifications. Permet d'afficher les différentes options de notification.

Chapitre 3

Installation des agents

Ce chapitre explique les étapes nécessaires pour installer les agents Security Agent et Messaging Security Agent (Advanced uniquement). Il fournit également des informations sur la suppression de ces agents.

Installation de Security Agent

Effectuez une nouvelle installation de Security Agent sur les clients Windows (postes de travail et serveurs). Utilisez la méthode d'installation qui répond le mieux à vos besoins.

Fermez toutes les applications en cours d'exécution avant d'installer Security Agent. Si vous procédez à l'installation alors que d'autres applications sont en cours d'exécution, le processus d'installation peut prendre plus de temps.

Remarque

Pour plus d'informations sur la mise à niveau des agents Security Agent vers cette version, voir le *Guide d'installation et de mise à niveau*.

Configuration minimale requise pour l'installation de Security Agent

Visitez le site Web suivant pour obtenir la liste complète des configurations d'installation requises et des produits tiers compatibles :

http://docs.trendmicro.com/fr-fr/smb/worry-free-business-security.aspx

Considérations d'installation de Security Agent

Avant d'installer des agents Security Agent, tenez compte des éléments suivants :

- **Fonctionnalités de l'agent** : certaines fonctionnalités de Security Agent ne sont pas disponibles sur certaines plates-formes Windows. Pour plus de détails, voir *Fonctionnalités disponibles dans Security Agent à la page 3-3*.
- **Plates-formes x64** :une version réduite de Security Agent est disponible pour les plates-formes 64 bits. Cependant, aucune assistance n'est disponible pour le moment pour les plates-formes IA-64.

- **Prise en charge d'IPv6** :Security Agent peut être installé sur des points finaux IPv6 purs ou à double pile. Cependant, certaines méthodes d'installation peuvent avoir des exigences spécifiques.

  Pour plus de détails, voir *Installation de Security Agent et prise en charge d'IPv6 à la page 3-5*.

- **Listes d'exceptions** : Assurez-vous que les listes d'exceptions pour les fonctionnalités suivantes ont été configurées correctement :

  - **Surveillance des comportements** :Ajoutez les applications client critiques dans la liste des programmes approuvés pour empêcher Security Agent de les bloquer. Pour plus d'informations, voir *Configuration de la surveillance des comportements à la page 5-12*.

  - **Réputation de sites Web** : Ajoutez les sites Web que vous considérez sans danger à la liste des URL approuvées pour empêcher Security Agent de bloquer l'accès à ces sites Web. Pour plus d'informations, voir *Configuration de la réputation des sites Web pour agents Security Agent à la page 5-24*.

- **Répertoire d'installation de l'agent** :durant l'installation de Security Server, la configuration vous invite à spécifier le répertoire d'installation de l'agent, qui est `$ProgramFiles\Trend Micro\Security Agent` par défaut. Si vous souhaitez installer les agents Security Agent dans un autre répertoire, spécifiez le nouveau répertoire dans la section **Administration** > **Paramètres généraux** > **Système** > **Installation de Security Agent**.

Fonctionnalités disponibles dans Security Agent

Les fonctionnalités de Security Agent disponibles sur un client dépendent du système d'exploitation de ce dernier. Informez-vous sur les fonctionnalités non prises en charge lors de l'installation d'un agent sur un système d'exploitation spécifique.

TABLEAU 3-1. Fonctionnalités de Security Agent

FONCTION	SYSTÈME D'EXPLOITATION WINDOWS		
	10	SBS 2011	SERVER 2012/2012 R2/2016/2019
Scan manuel (normal et agressif), scan en temps réel et scan programmé	Oui	Oui	Oui
Pare-feu.	Oui	Oui	Oui
Réputation de sites Web	Oui	Oui	Oui
Filtrage d'URL	Oui	Oui	Oui
Surveillance des comportements	Oui	Oui	Oui
Contrôle des dispositifs	Oui	Oui	Oui
Damage Cleanup Services	Oui	Oui	Oui
Scan de la messagerie (POP3)	Oui	Oui	Oui
Mises à jour manuelles et programmées	Oui	Oui	Oui
Agent de mise à jour	Oui	Oui	Oui
Agent Plug-in Manager	Oui	Oui	Oui
Smart Feedback	Oui	Oui	Oui
Barre d'outils de Trend Micro Anti-spam	Oui Clients d'e-mail pris en charge (32 et 64 bits) : • Outlook 2010 • Outlook 2013 • Outlook 2016	Non	Non

Fonction	Système d'exploitation Windows		
	10	SBS 2011	Server 2012/2012 R2/2016/2019
HouseCall	Oui	Oui	Oui
Outil Case Diagnostic Tool	Oui	Oui	Oui
Évaluation des réseaux Wi-Fi	Oui	Non	Non

Installation de Security Agent et prise en charge d'IPv6

Cette rubrique aborde les éléments à prendre en compte lors de l'installation de Security Agent sur des clients IPv6 purs ou à double pile.

Système d'exploitation

Security Agent ne peut être installé que sur les systèmes d'exploitation suivants prenant en charge l'adressage IPv6 :

- Windows SBS 2011
- Windows 10 (toutes les éditions)
- Windows Server 2012/2012 R2 (toutes les éditions)
- Windows Server 2016 (Standard, Datacenter, Essentials)
- Windows Server 2019 (Standard, Datacenter, Essentials)

Visitez le site Web suivant pour obtenir la liste complète des configurations requises :

http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx

Méthodes d'installation prises en charge

Toutes les méthodes d'installation disponibles peuvent être utilisées pour installer Security Agent sur des clients IPv6 purs ou à double pile. Pour certaines méthodes d'installation, il existe des spécifications particulières à respecter pour installer correctement Security Agent.

TABLEAU 3-2. Méthodes d'installation et prise en charge d'IPv6

MÉTHODE D'INSTALLATION	SPÉCIFICATIONS/ÉLÉMENTS À PRENDRE EN COMPTE
Page Web interne et installation sur notification par courrier électronique	Si vous effectuez l'installation sur un client IPv6 pur, le serveur Security Server doit être un serveur IPv6 pur ou à double pile, et son nom d'hôte ou son adresse IPv6 doit faire partie de l'URL. Quant aux clients à double pile, l'adresse IPv6 qui s'affiche dans l'écran d'état de l'installation dépend de l'option sélectionnée dans la section **Adresse IP préférée** sous l'onglet **Administration** > **Paramètres généraux** > **Poste de travail/serveur**.
Vulnerability Scanner et installation distante	Un serveur Security Server IPv6 pur ne peut pas installer Security Agent sur des clients IPv4 purs. De même, un serveur Security Server IPv4 pur ne peut pas installer l'agent sur des clients IPv6 purs.

Adresses IP de Security Agent

Un serveur Security Server installé dans un environnement et prenant en charge l'adressage IPv6 peut gérer les agents Security Agent suivants :

- Un serveur Security Server installé sur un client IPv6 pur peut gérer des agents Security Agent IPv6 purs.
- Un serveur Security Server installé sur un client à double pile et auquel des adresses IPv4 et IPv6 ont été affectées peut gérer des agents Security Agent IPv6 purs, IPv4 purs et à double pile.

Après avoir installé ou mis à niveau les agents Security Agent, ceux-ci s'enregistrent sur Security Server en utilisant une adresse IP.

- Les agents Security Agent IPv6 purs s'enregistrent en utilisant leur adresse IPv6.
- Les agents Security Agent IPv4 purs s'enregistrent en utilisant leur adresse IPv4.
- Les agents Security Agent à double pile s'enregistrent en utilisant leur adresse IPv4 ou IPv6. Vous pouvez sélectionner l'adresse IP que ces

agents utiliseront dans la section **Adresse IP préférée** sous l'onglet **Administration** > **Paramètres généraux** > **Poste de travail/serveur**.

Méthodes d'installation de Security Agent

Cette section récapitule les différentes méthodes permettant d'effectuer une nouvelle installation de Security Agent. Toutes les méthodes d'installation requièrent des droits d'administration locaux sur les points finaux cibles.

Si vous installez des agents Security Agent et que vous souhaitez activer la prise en charge d'IPv6, consultez les instructions de la rubrique *Installation de Security Agent et prise en charge d'IPv6 à la page 3-5*.

TABLEAU 3-3. Méthodes d'installation

MÉTHODE D'INSTALLATION/ PRISE EN CHARGE DU SYSTÈME D'EXPLOITATION	ÉLÉMENTS À PRENDRE EN COMPTE POUR LE DÉPLOIEMENT					
	DÉPLOIEMENT SUR UN WAN	GESTION CENTRALISÉE	REQUIERT L'INTERVENTION DE L'UTILISATEUR	NÉCESSITE UNE RESSOURCE INFORMATIQUE	DÉPLOIEMENT DE MASSE	BANDE PASSANTE CONSOMMÉE
Page Web interne Prise en charge sur tous les systèmes d'exploitation	Oui	Oui	Oui	Non	Non	Faible si programmée
Notification par e-mail Prise en charge sur tous les systèmes d'exploitation	Oui	Oui	Oui	Non	Non	Élevée si les installations sont lancées simultanément

Méthode d'installation/ Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
Installation à distance Prise en charge sur tous les systèmes d'exploitation	Non	Oui	Non	Oui	Oui	Faible si programmée
Configuration du script de connexion Prise en charge sur tous les systèmes d'exploitation	Non	Oui	Non	Oui	Oui	Élevée si les installations sont lancées simultanément
Client Packager Prise en charge sur tous les systèmes d'exploitation	Oui	Non	Oui	Oui	Non	Faible si programmée
Trend Micro Vulnerability Scanner (TMVS) Prise en charge sur tous les systèmes d'exploitation sauf Windows 10	Non	Oui	Non	Oui	Oui	Faible si programmée

Pour le déploiement sur un seul site et dans des entreprises dans lesquelles les stratégies informatiques sont appliquées à la lettre, les administrateurs informatiques peuvent choisir de déployer le programme à l'aide de la fonction d'**installation distante** ou de **configuration du script de connexion**.

Trend Micro recommande aux entreprises où les stratégies informatiques sont appliquées moins strictement d'installer les agents Security Agent à l'aide de la **page Web interne**. Cependant, l'utilisation de cette méthode requiert que les utilisateurs finaux qui vont installer Security Agent disposent de privilèges d'administrateur.

L'**installation à distance** est efficace pour les réseaux avec Active Directory. Si votre réseau n'utilise pas Active Directory, utilisez la page Web interne.

Installation depuis la page Web interne

Avant de commencer

Pour installer depuis la page Web interne, les éléments suivants sont obligatoires :

Éléments à vérifier	Configuration minimale requise
Security Server	Le serveur Security Server doit être installé sous : • Windows 7, 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 ou SBS 2008, 2011 • avec Internet Information Server (IIS) 7.0, 7.5, 8.0, 8.5, 10 ou Apache 2.4

ÉLÉMENTS À VÉRIFIER	CONFIGURATION MINIMALE REQUISE
Point final cible	• Le point final cible doit être installé sur Windows 10, Server 2012, 2012 R2, 2016, 2019 ou SBS 2011. • Le point final cible doit disposer d'Internet Explorer 9.0 ou version ultérieure. • Les utilisateurs doivent utiliser un compte administrateur pour se connecter au point final. **Remarque** Si le point final cible s'exécute sous un système d'exploitation de bureau, activez d'abord le compte administrateur intégré. Pour plus d'informations, consultez le site de l'assistance technique de Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account).
Paramètres de sécurité d'Internet Explorer	Les utilisateurs doivent procéder comme suit : 1. Lancez Internet Explorer et ajoutez l'URL du serveur Security Server (par exemple, `https://<nom du serveur Security Server>:4343/SMB/console/html/client`) à la liste de sites de confiance. Accédez à la liste en vous rendant dans l'onglet **Outils** > **Options Internet** > **Sécurité**, puis sélectionnez l'icône **Sites de confiance** et cliquez sur **Sites**. 2. Modifiez le paramètre de sécurité d'Internet Explorer en activant l'option **Demander confirmation pour les contrôles Active X**. Accédez à l'onglet **Outils** > **Options Internet** > **Sécurité**, puis cliquez sur **Niveau personnalisé**.
IPv6	Si vous disposez d'un environnement mixte composé de points finaux IPv4 purs, IPv6 purs et à double pile, le serveur Security Server doit posséder des adresses IPv4 et IPv6 afin que tous les points finaux puissent se connecter à la page Web interne sur le serveur Security Server.

Pour que vos utilisateurs installent l'agent Security Agent depuis la page Web interne, envoyez-leur les instructions suivantes. Pour envoyer une notification d'installation par e-mail, voir *Installation avec notification par courrier électronique à la page 3-32*.

Procédure

1. Connectez-vous au point final à l'aide d'un compte administrateur.
2. Ouvrez Internet Explorer et saisissez l'un des éléments suivants :
   - Serveur Security Server avec SSL :

     ```
     https://<nom ou adresse IP du serveur Security
     Server>:4343/SMB/console/html/client
     ```

   - Serveur Security Server sans SSL :

     ```
     http://<nom ou adresse IP du serveur Security
     Server>:8059/SMB/console/html/client
     ```

3. Cliquez sur **Installer maintenant** pour lancer l'installation de Security Agent.

   L'installation démarre. Autorisez l'installation du contrôle ActiveX quand vous y êtes invité. L'icône de l'agent Security Agent s'affiche dans la barre des tâches Windows après l'installation.

   Remarque

   Pour obtenir une liste des icônes qui s'affichent dans la barre des tâches Windows, voir *Vérification de l'état de Security Agent à la page A-2*.

Que faire ensuite

Si des utilisateurs signalent qu'ils ne parviennent pas à installer l'agent depuis la page Web interne, essayez les méthodes suivantes.

- Vérifiez que la communication point final-serveur existe en utilisant ping et telnet.
- Vérifiez si le protocole TCP/IP est activé et correctement configuré sur le point final.
- Si vous utilisez un serveur proxy pour la communication point final-serveur, assurez-vous que la configuration des paramètres proxy est correcte.

- Dans le navigateur Web, supprimez les modules complémentaires Trend Micro et l'historique de navigation.

Installation avec l'outil Configuration du script de connexion

L'outil Configuration du script de connexion automatise l'installation de Security Agent sur des clients non protégés lorsque ceux-ci se connectent au réseau. Il ajoute un programme appelé `AutoPcc.exe` dans le script de connexion au serveur.

`AutoPcc.exe` installe Security Agent sur les clients non protégés et met à jour les fichiers de programme ainsi que les composants. Les clients doivent faire partie du domaine pour pouvoir utiliser AutoPcc à l'aide du script de connexion.

Si vous disposez déjà d'un script de connexion, l'outil Configuration du script de connexion ajoute une commande permettant d'exécuter `AutoPcc.exe`. Sinon, il crée un fichier batch appelé `ofcscan.bat` qui contient la commande d'exécution du programme `AutoPcc.exe`.

L'outil Configuration du script de connexion ajoute la ligne suivante à la fin du script :

```
\\<Server_name>\ofcscan\autopcc
```

Description :

- `<Server_name>` correspond au nom ou à l'adresse IP de l'ordinateur Security Server.
- « `ofcscan` » correspond au nom de dossier partagé sur Security Server.
- « `autopcc` » correspond au lien vers le fichier exécutable autopcc qui installe Security Agent.

Emplacement du script de connexion sur toutes les versions de Windows Server (via un répertoire partagé Netlogon) :

```
\\Windows server\system drive\windir\sysvol\domain\scripts
\ofcscan.bat
```

Procédure

1. Sur l'ordinateur utilisé pour exécuter l'installation du serveur, ouvrez `<dossier d'installation de Security Server>\PCCSRV\Admin`.

2. Double-cliquez sur `SetupUsr.exe`.

   L'outil **Configuration du script de connexion** se charge. La console affiche une arborescence présentant tous les domaines du réseau.

3. Recherchez le serveur dont vous souhaitez modifier le script de connexion, sélectionnez-le puis cliquez sur **Sélectionner**. Vérifiez que ce serveur est un contrôleur de domaine principal et que vous disposez d'un accès d'administrateur à celui-ci.

   L'outil Configuration du script de connexion vous demande alors un nom d'utilisateur et un mot de passe.

4. Saisissez le nom d'utilisateur et le mot de passe. Cliquez sur **OK** pour continuer.

   La fenêtre **Sélection des utilisateurs** apparaît. la liste **Utilisateurs** affiche les profils des utilisateurs qui se connectent au serveur, tandis que la liste **Utilisateurs sélectionnés** affiche uniquement les profils des utilisateurs dont vous souhaitez modifier le script de connexion.

5. Pour modifier le script de connexion d'un profil utilisateur, faites votre sélection dans la liste Utilisateurs, puis cliquez sur **Ajouter**.

6. Pour modifier le script de connexion de tous les utilisateurs, cliquez sur **Ajouter tout**.

7. Pour retirer un profil utilisateur précédemment sélectionné, choisissez son nom dans la liste **Utilisateurs sélectionnés**, puis cliquez sur **Supprimer**.

8. Pour réinitialiser vos choix, cliquez sur **Supprimer tout**.

9. Cliquez sur **Appliquer** lorsque tous les profils d'utilisateurs cibles sont affichés dans la liste **Utilisateurs sélectionnés**.

   Un message vous informe que vous avez modifié avec succès les différents scripts de connexion.

10. Cliquez sur **OK**.

    L'outil Configuration du script de connexion retrouve alors son aspect initial.

11. Pour fermer l'outil Configuration du script de connexion, cliquez sur **Quitter**.

Installation avec Client Packager

Client Packager créé un pack d'installation que vous pouvez envoyer aux utilisateurs via des supports traditionnels tels que le CD-ROM. Les utilisateurs exécutent le pack sur le client pour installer ou mettre à niveau l'agent Security Agent et mettre à jour les composants.

Client Packager est particulièrement utile :

- Lors du déploiement de l'agent Security Agent ou de composants sur des clients dans des bureaux distants disposant d'une faible bande passante ;
- Si votre environnement dispose de restrictions en matière de connexion à Internet, comme dans le cas d'un réseau local fermé ou d'une absence de connexion à Internet.

Les agents Security Agent installés à l'aide de Client Packager communiquent avec le serveur sur lequel le pack a été créé.

Procédure

1. Sur l'ordinateur Security Server, accédez à `<dossier d'installation du serveur>\PCCSRV\Admin\Utility\ClientPackager`.
2. Double-cliquez sur `ClnPack.exe`.

   La console Client Packager s'ouvre.
3. Sélectionnez le système d'exploitation pour lequel vous voulez créer le pack. Veillez à ne déployer le pack que sur des clients qui exécutent ce type de système d'exploitation. Créez un autre pack pour effectuer un déploiement sur un autre type de système d'exploitation.

4. Sélectionnez la méthode de scan du pack.

   Pour plus d'informations concernant les méthodes de scan, voir *Méthodes de scan à la page 5-3*.

   Les composants inclus dans le pack dépendent de la méthode de scan que vous avez sélectionnée. Pour le Smart Scan, tous les composants, hormis le fichier de signatures de virus, sont inclus. Pour le scan traditionnel, tous les composants sauf signatures de l'agent Smart Scan seront inclus.

5. Sélectionnez le type de pack que vous désirez créer.

   TABLEAU 3-4. Types de pack client

TYPE DE PACK	DESCRIPTION
Installation	Sélectionnez **Installation** pour créer le pack sous forme de fichier MSI, qui correspond au format de package Microsoft Installer. Le pack installe le programme Security Agent avec les composants actuellement disponibles sur le serveur Security Server. Si une version antérieure de l'agent Security Agent est installée sur le client cible et que vous souhaitez la mettre à niveau, créez le fichier MSI à partir du serveur Security Server qui gère l'agent. Sinon, l'agent ne sera pas mis à niveau.
Mise à jour	Sélectionnez **Mise à jour** pour créer un pack contenant les composants actuellement disponibles sur le serveur Security Server. Le pack sera créé sous forme de fichier exécutable. Utilisez ce pack si vous rencontrez des problèmes lors de la mise à jour de composants sur le client sur lequel l'agent Security Agent est installé.

6. Cliquez sur **Mode silencieux** pour créer un pack capable de s'installer en arrière-plan sur le client, de façon entièrement transparente et sans aucune fenêtre d'état de l'installation. Activez cette option si vous prévoyez de déployer le pack à distance sur le client.

7. Cliquez sur **Désactiver le pré-scan (1ère installation)** si vous ne souhaitez pas scanner le client pour rechercher des menaces avant d'installer l'agent Security Agent. Procédez de la sorte si vous êtes certain que le client ne présente aucune menace.

Si le préscan est activé, le programme d'installation scanne les zones les plus vulnérables de l'ordinateur à la recherche de virus/programmes malveillants, parmi lesquelles :

- la zone et le répertoire d'amorçage (contre les virus d'amorce)
- le dossier Windows
- le dossier Program files

8. À côté de **Fichier source**, assurez-vous que l'emplacement du fichier `ofcscan.ini` est correct. Pour modifier le chemin, cliquez sur (...) pour accéder au fichier `ofcscan.ini`. Par défaut, ce fichier se trouve sous `<dossier d'installation du serveur>\PCCSRV`.

9. Dans Fichier de sortie, cliquez sur (...), indiquez l'emplacement où vous souhaitez créer le pack ainsi que le nom de fichier (par exemple, `ClientSetup.exe`).

10. Cliquez sur **Créer**.

    Lorsque Client Packager a fini de créer le pack, le message « « Création du pack réussie » » apparaît. Recherchez le pack dans le répertoire que vous avez spécifié dans l'étape précédente.

Que faire ensuite

Déployez le pack sur les clients.

Configuration requise du client :

- Espace disque
  - Scan traditionnel : 1,5 Go minimum (2 Go recommandé)
  - Smart Scan : 500 Mo

  1 Go d'espace disque libre si la méthode de scan pour le pack est traditionnelle et 500 Mo pour le smart scan
- Windows Installer 4.5 ou version ultérieure (pour pouvoir exécuter un package MSI)

Instructions de déploiement du pack :

- Envoyez le pack aux utilisateurs et demandez-leur de le lancer en double-cliquant sur le fichier (`.msi` ou `.exe`).

  Remarque

  Envoyez le pack uniquement aux utilisateurs dont l'agent Security Agent dépend du serveur sur lequel le pack a été créé.

- Demandez aux utilisateurs de cliquer avec le bouton droit de la souris sur le fichier du package et de sélectionner **Exécuter en tant qu'administrateur**.
- Si vous utilisez Active Directory, vous pouvez automatiquement déployer l'agent Security Agent sur tous les clients simultanément à l'aide du fichier `.msi`, plutôt que d'inviter chaque utilisateur à installer lui-même l'agent Security Agent. Utilisez **Configuration ordinateur** au lieu de **Configuration utilisateur** de sorte que l'agent Security Agent puisse être installé indépendamment de l'utilisateur qui se connecte au client.
- Si un agent Security Agent récemment installé ne parvient pas à se connecter au serveur Security Server, l'agent Security Agent conserve les paramètres par défaut. Lorsque l'agent Security Agent se connecte au serveur Security Server, il obtient les paramètres pour son groupe dans la console Web.
- Si vous rencontrez des problèmes lors de la mise à niveau de l'agent Security Agent avec Client Packager, Trend Micro vous recommande de désinstaller la version précédente de l'agent avant d'installer la nouvelle version. Pour des instructions de désinstallation, voir *Suppression d'agents à la page 3-39*.

Installation avec l'utilitaire d'installation à distance

Avant de commencer

Installez Security Agent à distance sur un ou plusieurs points finaux connectés au réseau.

Pour installer l'agent avec Remote Install, les éléments suivants sont requis :

ÉLÉMENTS À VÉRIFIER	CONFIGURATION MINIMALE REQUISE
Point final cible	• Utilisez un compte administrateur pour vous connecter à chaque point final cible. **Remarque** • Si le point final cible s'exécute sous un système d'exploitation de bureau, activez d'abord le compte administrateur intégré. Pour plus d'informations, consultez le site de l'assistance technique de Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account). • Lorsque vous effectuez une installation à distance sous Windows 10, vous ne pouvez pas utiliser le compte Microsoft pour vous connecter au client cible • Security Server ne doit pas être installé sur le point final cible. Lors d'une installation à distance, Security Agent ne peut pas être installé sur un point final qui s'exécute déjà sur Security Server.
Partage de fichiers et d'imprimantes	Sur le point final, activez temporairement le partage de fichiers et d'imprimantes. **Remarque** Si la stratégie de sécurité de la société est de désactiver le pare-feu Windows, passez à la section Registre distant. 1. Ouvrez le pare-feu Windows dans le Panneau de configuration. 2. Cliquez sur **Autoriser un programme via le pare-feu Windows**. Si vous êtes invité à saisir un mot de passe d'administrateur ou à le confirmer, entrez le mot de passe ou confirmez-le. La fenêtre Paramètres du pare-feu Windows apparaît. 3. Dans la liste **Programmes ou ports** sous l'onglet **Exceptions**, vérifiez que la case **Partage des fichiers et de l'imprimante** est cochée.

ÉLÉMENTS À VÉRIFIER	CONFIGURATION MINIMALE REQUISE
	4. Cliquez sur **OK**. 5. Si nécessaire, restaurez les paramètres d'origine après l'installation des agents Security Agent.
Contrôle de compte d'utilisateur	Désactivez le contrôle d'accès utilisateur. **Remarque** pour désactiver le contrôle d'accès à distance, modifiez la clé du Registre suivante : `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] "EnableLUA"=dword:00000000`. Si nécessaire, restaurez les paramètres d'origine après l'installation des agents Security Agent.
Registre distant	Démarrez temporairement le service de registre distant. 1. **Remarque** Saisissez `services.msc` dans la fenêtre Exécuter pour ouvrir Microsoft Management Console. 2. Cliquez avec le bouton droit de la souris sur **Registre distant** puis cliquez sur **Démarrer**. 3. Si nécessaire, restaurez les paramètres d'origine après l'installation des agents Security Agent.
IPv6	Un serveur Security Server à double pile peut installer Security Agent sur n'importe quel point final. Un serveur Security Server IPv6 pur peut uniquement installer Security Agent sur des points finaux IPv6 purs ou à double pile.

Procédure

1. Accédez à **Dispositifs**.
2. Cliquez sur **Ajouter des dispositifs**.

3. Sélectionnez **Poste de travail ou serveur** dans la section **Type d'ordinateur**.
4. Sélectionnez **Installation à distance**, dans la section **Méthode**.
5. Cliquez sur **Suivant**.

   Un nouvel écran s'affiche.
6. Dans la liste des clients de la zone **Groupes et ordinateurs**, sélectionnez un client, puis cliquez sur **Ajouter**. Vous êtes alors invité à fournir un nom d'utilisateur et un mot de passe pour le client.
7. Saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Connexion**. Le client s'affiche dans la zone de liste **Ordinateurs sélectionnés**.
8. Répétez ces étapes jusqu'à ce que la liste affiche tous les clients dans la zone de liste **Ordinateurs sélectionnés**.
9. Cliquez sur **Installer**.

   Une fenêtre de confirmation apparaît.
10. Cliquez sur **Oui** pour confirmer que vous souhaitez installer l'agent sur les clients.

    Un écran apparaît pour indiquer la progression de la copie des fichiers Security Agent sur chaque client.

    Lorsque Security Server termine l'installation sur un client, l'état d'installation s'affiche dans le champ **État** de la zone de liste **Ordinateurs sélectionnés**, et le nom du client est marqué d'une coche verte.

Que faire ensuite

Si l'installation avec Remote Install échoue, procédez comme suit :

- Vérifiez que la communication client-serveur existe en utilisant ping et telnet.
- Vérifiez si TCP/IP est activé et correctement configuré sur l'ordinateur client.

- Si vous utilisez un serveur proxy pour la communication client-serveur, assurez-vous que la configuration des paramètres de proxy est correcte.
- Dans le navigateur Web, supprimez les modules complémentaires Trend Micro et l'historique de navigation.

Installation avec Vulnerability Scanner

Avant de commencer

Exécutez des scans de vulnérabilité pour détecter des solutions antivirus installées, rechercher des clients non protégés sur le réseau et installer des agents Security Agent sur les clients.

Pour installer Vulnerability Scanner, les éléments suivants sont requis :

ÉLÉMENTS À VÉRIFIER	CONFIGURATION MINIMALE REQUISE
Où lancer Vulnerability Scanner	Vous pouvez lancer Vulnerability Scanner sur Security Server ou n'importe quel client du réseau. Le client ne doit pas s'exécuter sur Terminal Server.
Client cible	• Security Server ne doit pas être installé sur le client cible. Vulnerability Scanner n'installe pas Security Agent sur un client qui s'exécute déjà sur Security Server. • Les utilisateurs doivent utiliser un compte administrateur pour se connecter au client. **Remarque** Si le client cible s'exécute sous un système d'exploitation de bureau, activez d'abord le compte administrateur intégré. Pour plus d'informations, consultez le site de l'assistance technique de Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account).

Il existe plusieurs façons d'exécuter des scans de vulnérabilité.

- *Exécution d'un scan manuel de Vulnerability à la page 3-22*

- *Exécution d'un scan DHCP à la page 3-23*
- *Configuration d'un scan Vulnerability programmé à la page 3-26*

Exécution d'un scan manuel de Vulnerability

Exécutez des scans de vulnérabilité sur demande.

Procédure

1. Lancez Vulnerability Scanner.

POUR LANCER VULNERABILITY SCANNER SUR :	ÉTAPES
Security Server	a. Accédez à `<dossier d'installation du serveur>\PCCSRV\Admin\Utility\TMVS`. b. Double-cliquez sur `TMVS.exe`.
Un client sur le réseau	a. Sur Security Server, accédez à `<dossier d'installation du serveur>\PCCSRV\Admin\Utility`. b. Copiez le dossier `TMVS` sur l'autre client. c. Sur l'autre client, ouvrez le dossier `TMVS`, puis double-cliquez sur `TMVS.exe`.

2. Rendez-vous à la section **Scan manuel**.
3. Saisissez la plage d'adresses IP des clients que vous souhaitez vérifier.
   a. Saisissez une plage d'adresses IPv4.

> **Remarque**
>
> Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv4 s'il est exécuté sur un client IPv4 pur ou à double pile. Vulnerability Scanner prend uniquement en charge les plages d'adresses IP de la classe B, par exemple 168.212.1.1 à 168.212.254.254.

b. Pour une plage d'adresses IPv6, saisissez le préfixe IPv6 et la longueur du préfixe.

Remarque

Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv6 s'il est exécuté sur un client IPv6 pur ou à double pile.

4. Cliquez sur **Settings**.

   L'écran **Settings** apparaît.

5. Configurez les paramètres de scan de vulnérabilité. Pour plus de détails, voir *Paramètres de Vulnerability Scan à la page 3-28*.

6. Cliquez sur **OK**.

   L'écran Paramètres se ferme.

7. Cliquez sur **Start**.

   Les résultats du scan des failles s'affichent dans le tableau **Résultats** sous l'onglet **Scan manuel**.

Remarque

Les informations d'adresse MAC ne s'affichent pas dans la table **Résultats** si l'ordinateur exécute Windows Server 2008.

8. Pour enregistrer les résultats dans un fichier au format CSV (valeurs séparées par des virgules), cliquez sur **Exporter**, localisez le dossier dans lequel vous voulez enregistrer le fichier, tapez le nom du fichier et cliquez sur **Enregistrer**.

Exécution d'un scan DHCP

Exécutez des scans de vulnérabilité sur des clients requérant des adresses IP d'un serveur DHCP.

Vulnerability Scanner écoute sur le port 67 qui est le port d'écoute du serveur DHCP pour les requêtes DHCP. S'il détecte une requête DHCP provenant d'un client, un scan de vulnérabilité s'exécute sur l'ordinateur.

Remarque

Vulnerability Scanner ne peut pas détecter de requêtes DHCP si vous l'avez exécuté sur Windows Server 2008 ou Windows 7.

Procédure

1. Configurez les paramètres DHCP dans le fichier `TMVS.ini` qui se trouve dans le dossier suivant : `<Dossier d'installation du serveur>\PCCSRV\Admin\Utility\TMVS`.

   TABLEAU 3-5. Paramètres DHCP dans le fichier `TMVS.ini`

PARAMÈTRE	DESCRIPTION
DhcpThreadNum=x	Spécifiez le numéro de thread pour le mode DHCP. La valeur minimale est 3 et la valeur maximale 100. La valeur par défaut est 3.
DhcpDelayScan=x	C'est le délai d'attente en secondes avant que ne soit vérifié sur l'ordinateur demandeur si le logiciel antivirus est installé. La valeur minimale est 0 (aucune attente) et la valeur maximale 600. La valeur par défaut est 60.
LogReport=x	0 désactive l'écriture dans le journal et 1 l'active. Vulnerability Scanner envoie les résultats du scan au serveur Worry-Free Business Security. Les journaux s'affichent dans l'écran **Journaux des événements du système** de la console Web.
OsceServer=x	Adresse IP ou nom DNS du serveur Worry-Free Business Security.
OsceServerPort=x	Port du serveur Web sur le serveur Worry-Free Business Security.

2. Lancez Vulnerability Scanner.

POUR LANCER VULNERABILITY SCANNER SUR :	ÉTAPES
Security Server	a. Accédez à `<dossier d'installation du serveur>\PCCSRV\Admin\Utility\TMVS`. b. Double-cliquez sur `TMVS.exe`.
Un client sur le réseau	a. Sur Security Server, accédez à `<dossier d'installation du serveur>\PCCSRV\Admin\Utility`. b. Copiez le dossier `TMVS` sur l'autre client. c. Sur l'autre client, ouvrez le dossier `TMVS`, puis double-cliquez sur `TMVS.exe`.

3. En regard de la section **Scan manuel**, cliquez sur **Paramètres**.

   L'écran **Settings** apparaît.

4. Configurez les paramètres de scan de vulnérabilité. Pour plus de détails, voir *Paramètres de Vulnerability Scan à la page 3-28*.

5. Cliquez sur **OK**.

   L'écran Paramètres se ferme.

6. Dans la table **Résultats**, cliquez sur l'onglet **Scan DHCP**.

   Remarque

   L'onglet **Scan DHCP** n'est pas disponible sur les ordinateurs exécutant Windows Server 2008 et Windows 7.

7. Cliquez sur **DHCP Start**.

   Vulnerability Scanner commence à écouter les requêtes DHCP et exécute des scans de vulnérabilité sur les clients au fur et à mesure qu'ils se connectent au réseau.

8. Pour enregistrer les résultats dans un fichier au format CSV (valeurs séparées par des virgules), cliquez sur **Exporter**, localisez le dossier

dans lequel vous voulez enregistrer le fichier, tapez le nom du fichier et cliquez sur **Enregistrer**.

Configuration d'un scan Vulnerability programmé

Les scans de vulnérabilité s'exécutent automatiquement selon un planning.

Procédure

1. Lancez Vulnerability Scanner.

POUR LANCER VULNERABILITY SCANNER SUR :	ÉTAPES
Security Server	a. Accédez à `<dossier d'installation du serveur>\PCCSRV\Admin\Utility\TMVS`. b. Double-cliquez sur `TMVS.exe`.
Un client sur le réseau	a. Sur Security Server, accédez à `<dossier d'installation du serveur>\PCCSRV\Admin\Utility`. b. Copiez le dossier `TMVS` sur l'autre client. c. Sur l'autre client, ouvrez le dossier `TMVS`, puis double-cliquez sur `TMVS.exe`.

2. Rendez-vous à la section **Scan programmé**.
3. Cliquez sur **Ajouter/Modifier**.

   L'écran **Scan programmé** apparaît.
4. Saisissez un nom pour le scan de vulnérabilité programmé.
5. Saisissez la plage d'adresses IP des ordinateurs que vous souhaitez vérifier.

   a. Saisissez une plage d'adresses IPv4.

Remarque

Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv4 s'il est exécuté sur un ordinateur hôte IPv4 pur ou à double pile qui a une adresse IPv4 disponible. Vulnerability Scanner prend uniquement en charge les plages d'adresses IP de la classe B, par exemple 168.212.1.1 à 168.212.254.254.

b. Pour une plage d'adresses IPv6, saisissez le préfixe IPv6 et la longueur du préfixe.

Remarque

Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv6 s'il est exécuté sur un ordinateur hôte IPv6 pur ou à double pile qui a une adresse IPv6 disponible.

6. Spécifiez l'heure de début en utilisant le format 24 heures, puis sélectionnez la fréquence des scans. Choisissez s'il doit être quotidien, hebdomadaire ou mensuel.

7. Sélectionnez **Utiliser les paramètres en cours** si vous avez configuré les paramètres de vulnerability scan manuel et que vous souhaitez les utiliser. Pour plus de détails sur les paramètres de vulnerability scan manuel, voir *Exécution d'un scan manuel de Vulnerability à la page 3-22*.

   Si vous n'avez pas spécifié de paramètres de vulnerability scan manuel ou que vous souhaitez utiliser un autre ensemble de paramètres, sélectionnez **Modifier les paramètres**, puis cliquez sur **Paramètres**. L'écran **Settings** apparaît. Configurez les paramètres de scan, puis cliquez sur **OK**. Pour plus de détails, voir *Paramètres de Vulnerability Scan à la page 3-28*.

8. Cliquez sur **OK**.

   L'écran **Scan programmé** se ferme. Le vulnerability scan programmé que vous avez créé s'affiche sous **Scan programmé**. Si vous avez activé les notifications, Vulnerability Scanner vous envoie les résultats du vulnerability scan programmé.

9. Pour exécuter immédiatement le vulnerability scan programmé, cliquez sur **Exécuter maintenant**.

   Les résultats du vulnerability scan s'affichent dans le tableau **Résultats** sous l'onglet **Scan programmé**.

   Remarque

   Les informations d'adresse MAC ne s'affichent pas dans la table **Résultats** si l'ordinateur exécute Windows Server 2008.

10. Pour enregistrer les résultats dans un fichier au format `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter**, localisez le dossier dans lequel vous voulez enregistrer le fichier, tapez le nom du fichier et cliquez sur **Enregistrer**.

11. Pour arrêter d'exécuter les scans de vulnérabilité programmés, accédez à la section **Scans programmés**, sélectionnez le scan programmé, puis cliquez sur **Supprimer**.

Paramètres de Vulnerability Scan

Configurez les paramètres suivants lors de l'exécution de scans de vulnérabilité. Pour plus d'informations sur les différents types de scans de vulnérabilité, voir *Installation avec Vulnerability Scanner à la page 3-21*.

Paramètres	Description et instructions
Recherche Produits	Vulnerability Scanner peut vérifier la présence de logiciels de sécurité sur les clients cibles. 1. Sélectionnez le logiciel de sécurité à rechercher. 2. Vulnerability Scanner utilise les ports par défaut affichés à l'écran pour rechercher le logiciel. Si l'administrateur du logiciel a modifié les ports par défaut, apportez les modifications nécessaires, faute de quoi Vulnerability Scanner ne détectera pas le logiciel. 3. Pour Norton Antivirus Corporate Edition, vous pouvez modifier les paramètres de délai en cliquant sur **Paramètres**.
	Autres paramètres Product Query Pour définir le nombre de clients que Vulnerability Scanner vérifie simultanément à la recherche d'un logiciel de sécurité : 1. Accédez au `<dossier d'installation du serveur>\PCCSRV\Admin\Utility\TMVS` et ouvrez `TMVS.ini` à l'aide d'un éditeur de texte tel que le Bloc-notes. 2. Pour définir le nombre de clients à vérifier : • Pour les scans de vulnérabilité manuels, modifiez la valeur de `ThreadNumManual`. Indiquez une valeur comprise entre 8 et 64. Saisissez par exemple `ThreadNumManual=60` pour que Vulnerability Scanner vérifie 60 clients en même temps. • Pour les scans de vulnérabilité planifiés, modifiez la valeur de `ThreadNumSchedule`. Spécifiez une valeur comprise entre 8 et 64. Saisissez par exemple `ThreadNumSchedule=50` pour que Vulnerability Scanner vérifie 50 clients en même temps. 3. Enregistrez le fichier `TMVS.ini`.

Paramètres	Description et instructions
Description des paramètres de récupération	Lorsque Vulnerability Scanner est en mesure d'envoyer une requête « ping » aux clients, il peut récupérer des informations complémentaires sur les clients. Il existe deux méthodes de récupération des informations : • **Récupération normale** : récupère à la fois les informations relatives au domaine et à l'ordinateur • **Récupération rapide** : ne récupère que le nom de l'ordinateur
Paramètres d'alerte	Pour envoyer automatiquement les résultats de vulnerability scan à vous-même ou à d'autres administrateurs de votre entreprise : 1. Sélectionnez **Envoyer les résultats par courrier électronique à l'administrateur système**. 2. Cliquez sur **Configurer** pour spécifier les paramètres de courrier électronique. 3. Saisissez l'adresse électronique du destinataire dans **To**. 4. Saisissez l'adresse e-mail de l'expéditeur dans **De**. 5. Entrez l'adresse du serveur SMTP dans **Serveur SMTP**. Saisissez par exemple `société.smtp.com`. Les informations relatives au serveur SMTP sont obligatoires. 6. Sous **Subject**, entrez un nouvel objet pour le message ou acceptez l'objet par défaut. 7. Cliquez sur **OK**. Pour informer les utilisateurs que leurs ordinateurs n'ont aucun logiciel de sécurité installé : 1. Sélectionnez **Afficher une notification sur les ordinateurs non protégés**. 2. Cliquez sur **Personnaliser** pour configurer le message de notification. 3. Dans l'écran **Message de notification**, entrez un nouveau message ou acceptez le message par défaut. 4. Cliquez sur **OK**.

Paramètres	Description et instructions
Enregistrer en tant que fichier CSV	Enregistrez les résultats du scan de vulnérabilité dans un fichier au format CSV (valeurs séparées par des virgules). Le fichier sera enregistré sur le client sur lequel Vulnerability Scanner a été lancé. Acceptez le chemin de fichier par défaut ou modifiez-le selon vos préférences.
Paramètres de ping	Utilisez les paramètres « ping » pour confirmer l'existence d'un client et déterminer son système d'exploitation. Si ces paramètres sont désactivés, Vulnerability Scanner scanne toutes les adresses IP de la plage d'adresses IP spécifiée (même celles qui ne sont utilisées sur aucun client), ce qui rend la tentative de scan plus longue qu'elle ne devrait l'être. 1. Acceptez ou modifiez les valeurs des champs **Taille des paquets** et **Expiration**. 2. Sélectionnez **Détecter le type de SE par le système de reconnaissance de SE**. Si vous sélectionnez cette option, Vulnerability Scanner détermine si un client s'exécute sous Windows ou un autre système d'exploitation. Pour les clients s'exécutant sous Windows, Vulnerability Scanner peut identifier la version de Windows.
	Autres paramètres de requête ping Pour définir le nombre de clients auxquels Vulnerability Scanner envoie simultanément une requête ping : 1. Accédez au `<dossier d'installation du serveur>\PCCSRV\Admin\Utility\TMVS` et ouvrez `TMVS.ini` à l'aide d'un éditeur de texte tel que le Bloc-notes. 2. Modifiez la valeur d'`EchoNum`. Indiquez une valeur comprise entre 1 et 64. Saisissez par exemple `EchoNum=60` pour que Vulnerability Scanner envoie une requête ping à 60 clients en même temps. 3. Enregistrez le fichier `TMVS.ini`.

Paramètres	Description et instructions
Paramètres du serveur Security Server	1. Sélectionnez **Installation automatique de Security Agent sur les ordinateurs non protégés** pour installer l'agent Security Agent sur les clients qui seront scannés par Vulnerability Scanner. 2. Saisissez le nom d'hôte ou l'adresse IPv4/IPv6, ainsi que le numéro de port du serveur Security Server. Les agents Security Agent installés par Vulnerability Scanner dépendront de ce serveur. 3. Configurez les informations de connexion administratives à utiliser lors de la connexion aux clients en cliquant sur **Installation du compte**. Dans l'écran **Informations de compte**, saisissez un nom d'utilisateur et un mot de passe, puis cliquez sur **OK**.

Installation avec notification par courrier électronique

Utilisez cette méthode d'installation pour envoyer un e-mail contenant un lien vers le programme d'installation.

Procédure

1. Accédez à **Dispositifs**.
2. Cliquez sur **Ajouter des dispositifs**.
3. Sélectionnez **Poste de travail ou serveur** dans la section **Type d'ordinateur**.
4. Sélectionnez **Installation sur notification par courrier électronique** dans la section **Méthode**.
5. Cliquez sur **Suivant**.

   Un nouvel écran s'affiche.
6. Saisissez l'objet du message électronique et les destinataires.

7. Cliquez sur **Appliquer**. Le client de messagerie par défaut s'ouvre avec les destinataires, l'objet et le lien vers le programme d'installation.

Migration vers Security Agent

Lorsque vous installez Security Agent, le programme d'installation recherche les logiciels de sécurité de points finaux Trend Micro ou tiers installés sur le client.

Ce programme peut effectuer les actions suivantes :

- Supprimer un autre logiciel de sécurité de points finaux actuellement installé sur le client et le remplacer par l'agent Security Agent.
- Détecter un autre logiciel de sécurité de points finaux mais sans le supprimer.

Visitez le site Web suivant pour obtenir la liste complète des logiciels de sécurité de points finaux :

http://esupport.trendmicro.com/solution/en-US/1060980.aspx

Si le logiciel détecté sur le client ne peut pas être supprimé manuellement ou ne peut pas être supprimé du tout, désinstallez-le manuellement. En fonction du processus de désinstallation du logiciel, le client procédera ou non à un redémarrage après la désinstallation.

Problèmes de migration et solutions

Raisons possibles de l'échec de la désinstallation du logiciel de sécurité de points finaux tiers :

- Un problème de cohérence affecte la clé du produit ou le numéro de version du logiciel tiers.
- Le programme de désinstallation du logiciel tiers ne fonctionne pas.
- Certains fichiers du logiciel tiers manquent ou sont corrompus.
- La clé de registre du logiciel tiers ne peut pas être nettoyée.

- Le logiciel tiers ne possède pas de programme de désinstallation.

Solutions possibles :

- Supprimez manuellement le logiciel tiers.
- Arrêtez le service du logiciel tiers.
- Déchargez le service ou le processus du logiciel tiers.

Exécution de tâches de post-installation sur les agents Security Agent

Procédure

1. Vérifiez ce qui suit:
   - Les raccourcis de l'agent Security Agent apparaissent dans le menu Démarrer de Windows sur l'endpoint.
   - **Trend Micro Worry-Free Business Security Agent** figure dans la liste Ajout/Suppression de programmes du Panneau de configuration de l'endpoint.
   - L'agent Security Agent s'affiche sur l'écran des **Dispositifs** de la console Web et sous le groupe **Serveurs (par défaut)** ou **Postes de travail (par défaut)**, selon le système d'exploitation de l'endpoint.

     Remarque

     Si Security Agent ne s'y trouve pas, lancez une tâche de vérification de la connexion en allant dans **Administration** > **Paramètres généraux** > **Système (onglet)** > **Vérification de la connexion de l'agent**.

   - Les services suivants de l'agent Security Agent s'affichent dans **Microsoft Management Console** :
     - Trend Micro Security Agent Listener (`tmlisten.exe`)
     - Trend Micro Security Agent RealTime Scan (`ntrtscan.exe`)

- Pare-feu de Trend Micro Security Agent (`TmPfw.exe`) si le pare-feu a été activé pendant l'installation.
- Service de prévention des modifications non autorisées Trend Micro (`TMBMSRV.exe`) si la surveillance des comportements ou le contrôle de dispositifs a été activé pendant l'installation.
- Trend Micro Common Client Solution Framework (`TmCCSF.exe`)

2. Si l'agent Security Agent n'apparaît pas sur la console Web, c'est probablement qu'il n'est pas en mesure de communiquer son état actuel au serveur. Effectuez l'une des opérations suivantes :

- Ouvrez un navigateur Web sur le client, tapez `https://{Nom_Trend Micro Security Server}:{numéro de port}/SMB/cgi/cgionstart.exe` dans la zone de texte d'adresse et appuyez sur ENTRÉE.

  Si l'écran suivant affiche -2, cela signifie que l'agent peut communiquer avec le serveur. Cela indique également que le problème peut être lié à la base de données du serveur ; elle ne contient peut-être pas d'enregistrement de l'agent.
- Vérifiez que la communication client-serveur existe en utilisant ping et telnet.
- Si votre bande passante est limitée, assurez-vous que cette restriction n'entraîne pas un dépassement du délai de connexion entre le serveur et le client.
- Assurez-vous que le dossier `\PCCSRV` du serveur possède des privilèges de partage et que des privilèges de contrôle intégral ont été accordés à tous les utilisateurs.
- Vérifiez que les paramètres de proxy de Trend Micro Security Server sont corrects.

3. Testez l'agent Security Agent avec un script de test EICAR.

L'Institut européen pour la recherche des virus informatiques (EICAR) a mis au point un virus de test que vous pouvez utiliser pour tester votre

installation et votre configuration. Ce fichier est un texte inerte dont la structure binaire est incluse dans le fichier de signatures de virus de la plupart des distributeurs d'antivirus. Il ne s'agit pas d'un virus et il ne contient aucun code de programme.

Vous pouvez télécharger le virus de test EICAR à l'adresse suivante :

http://www.eicar.org/anti_virus_test_file.htm

Une solution alternative est de créer votre propre test de virus EICAR en saisissant le texte suivant dans un fichier texte, puis en le nommant eicar.com :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Remarque

videz la mémoire cache dans le serveur cache ainsi que le navigateur local avant de procéder au test.

Installation de Messaging Security Agent

Les agents Messaging Security Agent peuvent uniquement être installés si vous avez la version Advanced de Worry-Free Business Security.

Effectuez une nouvelle installation de Messaging Security Agent sur les serveurs Microsoft Exchange.

Remarque

Pour plus d'informations sur la mise à niveau des agents Messaging Security Agent vers cette version, voir le Guide d'installation et de mise à niveau.

Configuration requise pour l'installation de Messaging Security Agent

Visitez le site Web suivant pour obtenir la liste complète des configurations d'installation requises :

http://docs.trendmicro.com/fr-fr/smb/worry-free-business-security.aspx

Installation de Messaging Security Agent (Advanced uniquement)

Avant de commencer

Remarques et rappels d'installation :

- Vous n'avez pas besoin d'arrêter ou de démarrer les services Microsoft Exchange avant ou après l'installation.
- Si l'endpoint contient des informations d'une installation de Messaging Security Agent, vous ne pourrez pas installer correctement la nouvelle version. Utilisez le Panneau de configuration Windows pour supprimer les fichiers restants de l'installation précédente.

  Voir *Désinstallation de l'agent Messaging Security Agent du serveur Microsoft Exchange (Advanced uniquement) à la page 3-43* pour obtenir des informations complémentaires.
- Si vous installez Messaging Security Agent sur un serveur qui exécute des outils de blocage, supprimez l'outil de blocage pour qu'il ne désactive pas le service IIS et fasse échouer l'installation.
- Messaging Security Agent peut également être installé lors de l'installation de Security Server. Pour plus de détails, reportez-vous au Guide d'installation et de mise à niveau.
- Messaging Security Agent ne prend pas en charge certaines fonctionnalités de Microsoft Exchange Server Enterprise, telles que le Groupe de disponibilité de données (DAG).

Procédure

1. Accédez à **Dispositifs**.
2. Cliquez sur **Ajouter des dispositifs**.
3. Sélectionnez **Serveur Exchange**.
4. Sous **Informations sur le serveur Exchange**, entrez les informations suivantes :
   - **Nom du serveur** : nom du serveur Microsoft Exchange sur lequel vous souhaitez installer l'agent.
   - **Compte** : nom d'utilisateur d'administrateur de domaine intégré.
   - **Mot de passe** : mot de passe d'administrateur de domaine intégré.
5. Cliquez sur **Suivant**.

   L'assistant d'installation affiche un écran qui varie selon le type d'installation voulue.
   - **Nouvelle installation** : l'agent n'existe pas sur le serveur Microsoft Exchange et sera installé.
   - **Mise à niveau** : une version précédente de l'agent existe sur le serveur Microsoft Exchange et sera mise à niveau vers la version actuelle.
   - **Aucune installation requise** : la version actuelle de l'agent existe sur le serveur Microsoft Exchange. Si l'agent n'apparaît pas actuellement dans l'arborescence des groupes de sécurité, il sera automatiquement ajouté.
   - **Non valide** : un problème est survenu lors de l'installation de l'agent.

Remarque

Pour le **Type de gestion du spam**, **End User Quarantine** sera utilisé.

6. Sous **Répertoires**, modifiez ou acceptez les répertoires cibles et partagés par défaut pour l'installation de Messaging Security Agent. Par défaut, le répertoire cible est `C:\Program Files\Trend Micro\Messaging Security Agent` et le répertoire partagé est `C$`.
7. Cliquez sur **Suivant**.

   Un nouvel écran s'affiche.
8. Vérifiez que les paramètres du serveur Microsoft Exchange spécifiés sur l'écran précédent sont corrects, puis cliquez sur **Suivant** pour démarrer l'installation.
9. Pour afficher l'état de l'installation, cliquez sur l'onglet **État actuel**.

Suppression d'agents

La commande **Désinstaller l'agent** permet de supprimer les agents Security Agent et Messaging Security Agent (Advanced uniquement) comme suit :

- *Suppression d'agents de la console Web à la page 3-40*

  Utilisez cette option pour les agents inactifs. Un agent inactif apparaît toujours hors ligne sur la console Web, car le client sur lequel il est installé est peut-être éteint depuis longtemps ou a été reformaté avant la désinstallation de l'agent.

  Lorsque vous supprimez des agents de la console Web :

  - L'agent, s'il existe toujours sur le client, n'est pas désinstallé.
  - Le serveur arrête de gérer l'agent.
  - Lorsque l'agent recommence à communiquer avec le serveur (par exemple, si le client est rallumé), il figure à nouveau sur la console Web. Un agent Security Agent applique les paramètres de son groupe d'origine. Si le groupe n'existe plus, l'agent est enregistré dans **Serveurs (par défaut)** ou **Postes de travail (par défaut)**, selon le système d'exploitation du client, et applique les paramètres de ce groupe.

Conseil

WFBS propose une autre fonction qui permet de rechercher et de supprimer les agents inactifs de la console Web. Cette fonction permet d'automatiser la tâche de suppression des agents. Pour l'utiliser, accédez à **Administration** > **Paramètres généraux** > **Système**, puis allez dans la section Suppression des agents Security Agent inactifs.

- *Désinstallation d'agents à partir de la console Web à la page 3-41*

  Vous pouvez désinstaller l'agent (et donc, le supprimer de la console Web) si vous rencontrez des problèmes avec le programme. Trend Micro recommande de réinstaller immédiatement l'agent afin que le client reste protégé des menaces.

Suppression d'agents de la console Web

Procédure

1. Accédez à **Dispositifs**.
2. Pour supprimer des agents Security Agent, cliquez sur un groupe puis sélectionnez les agents à déplacer. Pour supprimer un agent Messaging Security Agent, sélectionnez-le.

   Conseil

   Pour sélectionner plusieurs agents Security Agent adjacents, cliquez sur le premier agent de la plage, maintenez la touche MAJ enfoncée, puis cliquez sur le dernier agent de la plage. Pour sélectionner plusieurs agents non adjacents, cliquez sur le premier agent de la plage, maintenez la touche CTRL enfoncée, puis cliquez sur les agents que vous souhaitez sélectionner.

3. Cliquez sur **Autres** > **Désinstaller l'agent**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Supprimer le ou les agents sélectionnés**.

5. Cliquez sur **Appliquer**.

Désinstallation d'agents à partir de la console Web

Lorsque vous désinstallez l'agent Messaging Security Agent, le service IIS Admin/serveur Apache et tous les services connexes sont automatiquement arrêtés puis redémarrés.

Procédure

1. Accédez à **Dispositifs**.
2. Pour désinstaller des agents Security Agent, cliquez sur un groupe puis sélectionnez les agents à déplacer. Pour désinstaller un agent Messaging Security Agent, sélectionnez-le.

   Conseil

   Pour sélectionner plusieurs agents Security Agent adjacents, cliquez sur le premier agent de la plage, maintenez la touche MAJ enfoncée, puis cliquez sur le dernier agent de la plage. Pour sélectionner plusieurs agents non adjacents, cliquez sur le premier agent de la plage, maintenez la touche CTRL enfoncée, puis cliquez sur les agents que vous souhaitez sélectionner.

3. Cliquez sur **Autres** > **Désinstaller l'agent**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Désinstaller le ou les agents sélectionnés**.
5. Cliquez sur **Appliquer**.

   Une fenêtre contextuelle apparaît et affiche le nombre de notifications de désinstallation envoyées par le serveur, ainsi que le nombre d'agents ayant reçu la notification.

Remarque

Pour un agent Messaging Security Agent, saisissez le nom de compte et le mot de passe du serveur Microsoft Exchange correspondant lorsque vous y êtes invité.

6. Cliquez sur **OK**.
7. Pour vérifier que l'agent a été désinstallé, actualisez l'écran Paramètres de sécurité. L'agent ne doit plus apparaître dans l'arborescence des groupes de sécurité.

Désinstallation de l'agent Security Agent à partir de l'endpoint

Selon votre configuration, la désinstallation peut nécessiter un mot de passe. Si c'est le cas, veillez à partager le mot de passe uniquement avec les utilisateurs qui exécuteront le programme de désinstallation et à le modifier immédiatement s'il a été divulgué à d'autres utilisateurs.

Pour définir ou désactiver le mot de passe, allez dans **Administration** > **Paramètres généraux** > **Onglet Poste de travail/serveur** > **Mot de passe de désinstallation de Security Agent**.

Procédure

1. Cliquez sur **Panneau de configuration** > **Ajout/Suppression de programmes**.
2. Recherchez **Trend Micro Worry-Free Business Security Agent** et cliquez sur **Changer** ou **Désinstaller**, selon l'option disponible.
3. Suivez les instructions indiquées à l'écran.
4. Si vous y êtes invité, entrez le mot de passe de désinstallation.

   Le serveur Security Server informe l'utilisateur sur la progression de la désinstallation et l'avertit lorsque celle-ci est terminée. L'utilisateur ne doit pas redémarrer le client pour terminer la désinstallation.

Désinstallation de l'agent Messaging Security Agent du serveur Microsoft Exchange (Advanced uniquement)

Lorsque vous désinstallez l'agent Messaging Security Agent, le service IIS Admin/serveur Apache et tous les services connexes sont automatiquement arrêtés puis redémarrés.

Procédure

1. Connectez-vous au serveur Microsoft Exchange à l'aide des droits d'administration.
2. Cliquez sur **Panneau de configuration** > **Désinstaller un programme**.
3. Sélectionnez **Trend Micro Messaging Security Agent** et cliquez sur **Modifier**.
4. Suivez les instructions indiquées à l'écran.

Chapitre 4

Gestion des dispositifs

Worry-Free Business Security divise l'écran **Dispositifs** en deux sections principales.

- Arborescence de dispositifs

  L'arborescence de dispositifs est une liste de groupes logiques que vous pouvez développer. Vous pouvez gérer les groupes en fonction du type d'endpoint ou configurer manuellement des groupes et organiser les agents Security Agent selon vos besoins.

  Voir *Utilisation de l'arborescence de dispositifs à la page 4-2* pour obtenir des informations complémentaires.

- Tableau d'informations de groupe

  Lorsque vous sélectionnez un groupe dans l'arborescence de dispositifs, la liste des agents Security Agent du groupe s'affiche sur la droite.

  Voir *Utilisation des commandes des dispositifs à la page 4-5* pour obtenir des informations complémentaires.

Utilisation de l'arborescence de dispositifs

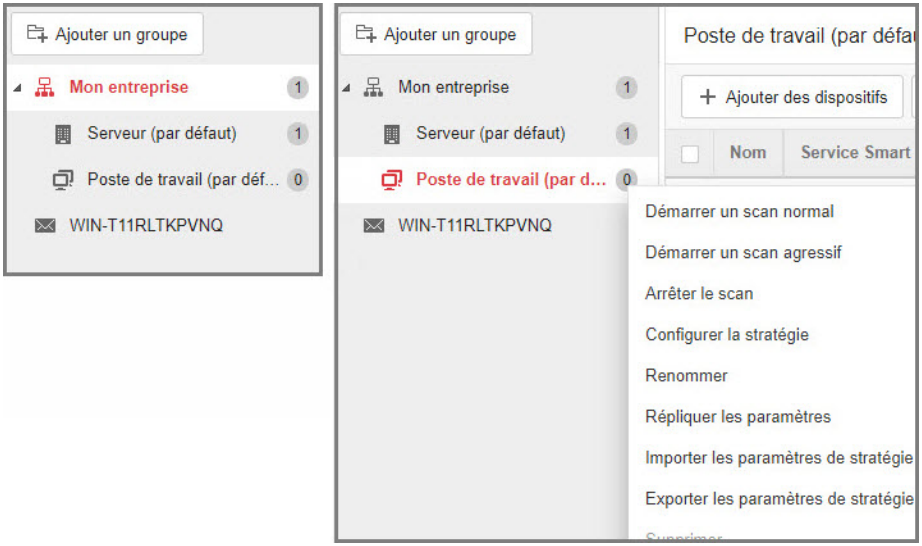


FIGURE 4-1. Utilisation du menu de commandes de l'arborescence de dispositifs

Pour ouvrir le menu de l'arborescence de dispositifs, procédez comme suit :

- Sélectionnez un groupe dans l'arborescence de dispositifs et cliquez sur l'icône représentant un engrenage en regard du nom du groupe
- Sélectionnez un agent Messaging Security Agent et cliquez sur l'icône représentant un engrenage à côté du nom de l'agent

Les commandes disponibles dépendent du type de groupe sélectionné et selon le cas, certaines commandes peuvent être désactivées.

TABLEAU 4-1. Commandes de l'arborescence de dispositifs

COMMANDE	DESCRIPTION
Ajouter un groupe	Ajoute un nouveau groupe à l'arborescence de dispositifs. Voir *Ajout de groupes à la page 4-9* pour obtenir des informations complémentaires.
Démarrer un scan normal	• Démarre le scan de tous les endpoints du groupe sélectionné. • Démarre le scan du serveur Exchange.
Démarrer un scan agressif	Lance un scan avancé sur tous les endpoints du groupe sélectionné pour analyser et éliminer les menaces qu'un scan normal ne peut supprimer. **Remarque** L'exécution du scan agressif peut avoir un impact sur les performances de l'endpoint et peut générer un nombre accru de faux positifs.
Arrêter le scan	• Arrête le scan de tous les endpoints du groupe sélectionné. • Arrête le scan du serveur Exchange.
Configurer les paramètres généraux	Configure les paramètres généraux de Security Agent pour les scans de sécurité, la liste des éléments approuvés/bloqués, le contrôle de Security Agent et la gestion des périphériques Voir *Paramètres généraux à la page 11-2* pour obtenir des informations complémentaires.

COMMANDE	DESCRIPTION
Configurer la stratégie	• Configure les paramètres de sécurité de tous les agents Security Agent du groupe sélectionné. Voir *Synthèse des paramètres de sécurité de base des agents Security Agent à la page 5-2* pour obtenir des informations complémentaires. • Configure les paramètres de sécurité de l'agent Messaging Security Agent sélectionné. Voir *Gestion des param. sécurité de base des MSA (Advanced uniq.) à la page 6-1* pour obtenir des informations complémentaires.
Renommer	Modifie le nom du groupe sélectionné.
Répliquer les paramètres	Copie les paramètres d'un groupe vers un autre. Les agents Security Agent du groupe cible adoptent alors les mêmes paramètres que le groupe source. Voir *Réplication des paramètres à la page 4-17* pour obtenir des informations complémentaires.
Importer les paramètres de stratégie	Importe les paramètres d'un autre groupe. Voir *Importation et exportation des paramètres des groupes Security Agent à la page 4-19* pour obtenir des informations complémentaires.
Exporter les paramètres de stratégie	Exporte les paramètres du groupe sélectionné. Voir *Importation et exportation des paramètres des groupes Security Agent à la page 4-19* pour obtenir des informations complémentaires.
Supprimer	Supprime un groupe de l'arborescence de dispositifs.

Utilisation des commandes des dispositifs

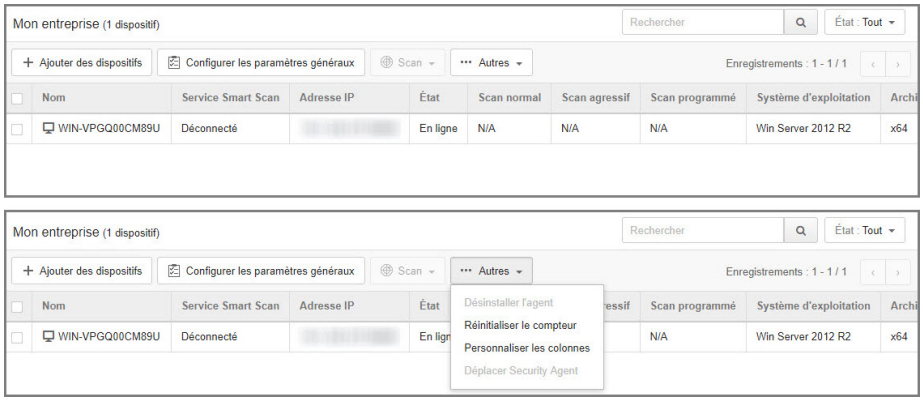


FIGURE 4-2. Utilisation du menu de commande des dispositifs

Lorsque vous sélectionnez un groupe dans l'arborescence de dispositifs, la liste des agents Security Agent de ce groupe s'affiche sur la droite dans un tableau. La barre de menus en haut du tableau contient les commandes que vous pouvez utiliser pour gérer les agents Security Agent. Les commandes disponibles dépendent du type de groupe sélectionné et selon le cas, certaines commandes peuvent être désactivées.

Utilisez la barre de recherche dans l'écran des **Dispositifs** pour rechercher des endpoints par nom, étiquette ou adresse IP.

Conseil

Pour rechercher des endpoints dans un réseau, vous pouvez saisir partiellement une adresse IP. Par exemple, « 192 » renvoie toutes les adresses IP contenant « 192 » tandis que « 192. » renvoie uniquement les adresses IP commençant par « 192 ». Vous ne pouvez cependant pas utiliser de caractères génériques et de symboles spéciaux (*, +, (,), -, &) pour rechercher des noms d'endpoint.

TABLEAU 4-2. Commandes des dispositifs

COMMANDE	DESCRIPTION
Ajouter des dispositifs	Installer l'un des logiciels suivants : • **Security Agent** sur un endpoint (poste de travail ou serveur) • **Messaging Security Agent** sur un serveur Microsoft Exchange (Advanced uniquement) Voir *Ajout d'agents aux groupes à la page 4-7* pour obtenir des informations complémentaires.
Configurer la stratégie	Configure les paramètres de sécurité de tous les agents Security Agent du groupe sélectionné. Voir *Synthèse des paramètres de sécurité de base des agents Security Agent à la page 5-2* pour obtenir des informations complémentaires.
Démarrer un scan normal	Démarre le scan des endpoints sélectionnés.
Démarrer un scan agressif	Lance un scan avancé sur tous les endpoints du groupe sélectionné pour analyser et éliminer les menaces qu'un scan normal ne peut supprimer. **Remarque** L'exécution du scan agressif peut avoir un impact sur les performances de l'endpoint et peut générer un nombre accru de faux positifs.
Arrêter le scan	Arrête le scan des endpoints sélectionnés.
Désinstaller l'agent	Supprime Security Agent des endpoints sélectionnés Voir *Suppression d'agents à la page 3-39* pour obtenir des informations complémentaires.
Réinitialiser le compteur	Permet de réinitialiser les compteurs de détection de risques de sécurité pour tous les agents Security Agent de votre réseau. Les informations pertinentes des journaux restent disponibles via la requête de journal.

COMMANDE	DESCRIPTION
Personnaliser les colonnes	Choisit les colonnes à afficher dans le tableau. Voir *Personnalisation des colonnes de la liste de dispositifs à la page 4-9* pour obtenir des informations complémentaires.
Déplacer Security Agent	Déplacer les agents Security Agent sélectionnés vers un autre groupe ou un autre serveur Security Server. Voir *Déplacement d'agents à la page 4-12* pour obtenir des informations complémentaires.

Ajout d'agents aux groupes

Après l'installation d'un agent qui dépend du serveur Security Server, le serveur l'ajoute à un groupe.

- Les agents Security Agent installés sur des plates-formes de serveur sont ajoutés au groupe **Serveurs (par défaut)**.
- Les agents Security Agent installés sur des plates-formes de poste de travail sont ajoutés au groupe **Postes de travail (par défaut)**.

Remarque

Vous pouvez affecter des agents Security Agent à d'autres groupes en les déplaçant. Pour plus de détails, voir *Déplacement d'agents à la page 4-12*.

- Chaque agent Messaging Security Agent (Advanced uniquement) constitue son propre groupe. Il est impossible d'organiser plusieurs agents Messaging Security Agent en un seul groupe.

Si le nombre d'agents indiqué dans l'arborescence des groupes de sécurité est incorrect, il est possible qu'ils aient été supprimés sans en avertir le serveur (par exemple, si une communication client-serveur a été perdue lors de la suppression de l'agent). Le serveur conserve alors les informations de l'agent dans sa base de données et affiche l'agent comme hors ligne dans la console Web. Lorsque vous réinstallez l'agent, le serveur crée un nouvel enregistrement dans la base de données et traite l'agent comme nouveau, ce

qui entraîne l'apparition de doublons dans l'arborescence des groupes de sécurité. Pour rechercher les enregistrements d'agent en double, utilisez la fonction Vérification de la connexion de l'agent dans **Administration** > **Paramètres généraux** > **Système**.

Installation des agents Security Agent

Consultez les rubriques suivantes :

- *Configuration minimale requise pour l'installation de Security Agent à la page 3-2*
- *Considérations d'installation de Security Agent à la page 3-2*
- *Méthodes d'installation de Security Agent à la page 3-7*
  - *Installation depuis la page Web interne à la page 3-9*
  - *Installation avec l'outil Configuration du script de connexion à la page 3-12*
  - *Installation avec Client Packager à la page 3-14*
  - *Installation avec l'utilitaire d'installation à distance à la page 3-17*
  - *Installation avec Vulnerability Scanner à la page 3-21*
  - *Installation avec notification par courrier électronique à la page 3-32*
- *Exécution de tâches de post-installation sur les agents Security Agent à la page 3-34*

Installation des agents Messaging Security Agent (Advanced uniquement)

Consultez les rubriques suivantes :

- *Configuration requise pour l'installation de Messaging Security Agent à la page 3-37*
- *Installation de Messaging Security Agent (Advanced uniquement) à la page 3-37*

Ajout de groupes

Ajoutez un groupe de serveurs ou de postes de travail, qui peut contenir un ou plusieurs agents Security Agent.

Il est impossible d'ajouter un groupe contenant des agents Messaging Security Agent. Une fois qu'un agent Messaging Security Agent est installé et dépend du serveur Security Server, il forme automatiquement son propre groupe dans l'**arborescence des groupes de sécurité**.

Procédure

1. Accédez à **Dispositifs**.
2. Cliquez sur **Ajouter un groupe**.

   Un nouvel écran s'affiche.
3. Sélectionnez un type de groupe.
   - **Postes de travail**
   - **Serveurs**
4. Saisissez un nom de groupe.
5. Pour appliquer les paramètres d'un groupe existant au groupe que vous ajoutez, cliquez sur **Importer les paramètres à partir du groupe**, puis sélectionnez le groupe. Seuls les groupes ayant le même type que le groupe sélectionné s'afficheront.
6. Cliquez sur **Enregistrer**.

Personnalisation des colonnes de la liste de dispositifs

Vous pouvez choisir les colonnes à afficher en cliquant sur **Autres** > **Personnaliser les colonnes** en haut de la liste des dispositifs.

COLONNE	INFORMATIONS AFFICHÉES
Pour les agents Security Agent	
Client	
Adresse IP	Adresse IP du client sur lequel l'agent est installé
État	• **En ligne** : l'agent est connecté au serveur Security Server. • **Hors ligne** : l'agent est déconnecté du serveur Security Server.
Version de l\'agent	Version de l'agent
Système d'exploitation	Système d'exploitation du client sur lequel l'agent est installé
Architecture	• **x64** : système d'exploitation 64 bits • **x86** : système d'exploitation 32 bits
Exchange Version	Version du serveur Microsoft Exchange
Scan	
Service Smart Scan **Remarque** Cette colonne s'affiche uniquement si la méthode de scan est Smart Scan.	• **Connecté** : l'agent est connecté au service Smart Scan. • **Déconnecté** : l'agent est déconnecté du service Smart Scan. **Remarque** Le service Smart Scan est hébergé sur le serveur Security Server. Si un agent est déconnecté, cela signifie qu'il ne peut pas se connecter au serveur Security Server ou que le service Smart Scan n'est pas fonctionnel (par exemple, si le service a été arrêté). • **Désactivé** : l'agent utilise le scan traditionnel.
Signatures de l'agent Smart Scan / Signatures de virus	Version des signatures de l'agent Smart Scan ou des signatures de virus
Scan programmé	Date et heure du dernier scan programmé

COLONNE	INFORMATIONS AFFICHÉES
Scan agressif	Date et heure du dernier scan agressif
Scan POP3	• **Activé** • **Désactivé**
Méthode de scan	• **Smart** : scans locaux et dans le cloud • **Traditionnel** : scans locaux uniquement Pour plus de détails, voir *Méthodes de scan à la page 5-3*.
Scan normal	Date et heure du dernier scan normal
Menace	
Nombre de virus détectés	Nombre de virus/programmes malveillants détectés
Nombre de spyware détectés	Nombre de spywares/graywares détectés
Messages de spam détectés	Nombre de messages électroniques de spam
Cas de violation d'URL	Nombre d'URL interdites auxquelles vous avez accédé
Moteur antivirus	Version du moteur de scan antivirus
Pour les agents Messaging Security Agent (Advanced uniquement)	
Nom	Nom d'hôte du client sur lequel l'agent est installé
Adresse IP	Adresse IP du client sur lequel l'agent est installé
En ligne/Hors ligne	• **En ligne** : l'agent est connecté au serveur Security Server. • **Hors ligne** : l'agent est déconnecté du serveur Security Server.
Plate-forme	Système d'exploitation du client sur lequel l'agent est installé
Architecture	• **x64** : système d'exploitation 64 bits • **x86** : système d'exploitation 32 bits
Exchange Version	Version du serveur Microsoft Exchange

Colonne	Informations affichées
Fichier de signatures de virus	Version du fichier de signatures de virus
Moteur antivirus	Version du moteur de scan antivirus
Version de l\'agent	Version de l'agent

Déplacement d'agents

Il existe plusieurs façons de déplacer des agents.

Agent à déplacer	Détails	Déplacer des agents
Security Agent	Déplacez des agents Security Agent d'un groupe à un autre. Une fois l'opération terminée, les agents héritent des paramètres du nouveau groupe.	Utilisez la console Web pour déplacer un ou plusieurs agents. Voir *Déplacements d'agents Security Agent entre plusieurs groupes à la page 4-13*.
	Si vous avez au moins deux serveurs Security Server, vous pouvez déplacer les agents Security Agent entre les serveurs. Une fois l'opération terminée, l'un des agents sera regroupé sous **Postes de travail (par défaut)** ou **Serveurs (par défaut)** dans l'autre Security Server, selon le système d'exploitation du client. L'agent hérite des paramètres du nouveau groupe.	• Utilisez la console Web pour déplacer un ou plusieurs agents. Voir *Déplacement d'agents entre plusieurs serveurs Security Server à l'aide de la console Web à la page 4-14*. • Lancez l'outil Client Mover sur un client pour déplacer l'agent qui s'y trouve. Voir *Déplacement d'un agent Security Agent entre plusieurs serveurs Security Server à l'aide de Client Mover à la page 4-15*.

Agent à déplacer	Détails	Déplacer des agents
Messaging Security Agent (Advanced uniquement)	Si vous avez au moins deux serveurs Security Server, vous pouvez déplacer les agents Messaging Security Agent entre les serveurs. Une fois l'opération terminée, l'un des agents constituera son propre groupe dans l'autre serveur Security Server et héritera de ses paramètres.	Utilisez la console Web pour déplacer un agent à la fois. Voir *Déplacement d'agents entre plusieurs serveurs Security Server à l'aide de la console Web à la page 4-14*.

Déplacements d'agents Security Agent entre plusieurs groupes

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Sélectionnez les agents à déplacer.

   Conseil

   Pour sélectionner plusieurs agents Security Agent adjacents, cliquez sur le premier agent de la plage, maintenez la touche MAJ enfoncée, puis cliquez sur le dernier agent de la plage. Pour sélectionner plusieurs agents non adjacents, cliquez sur le premier agent de la plage, maintenez la touche CTRL enfoncée, puis cliquez sur les agents que vous souhaitez sélectionner.

4. Faites glisser les agents dans leur nouveau groupe.

Déplacement d'agents entre plusieurs serveurs Security Server à l'aide de la console Web

Avant de commencer

Lorsque vous déplacez un agent d'un serveur Security Server vers un autre :

- Si un agent exécute une version antérieure vers un serveur Security Server exécutant la version actuelle, l'agent sera mis à niveau automatiquement.
- Ne déplacez pas un agent exécutant la version actuelle vers un serveur Security Server exécutant une version antérieure, car l'agent ne sera plus géré (Il ne sera plus enregistré sur l'ancien serveur et ne parviendra pas à s'enregistrer sur le nouveau ; il n'apparaîtra donc plus sur les consoles Web respectives). L'agent gardera sa version actuelle et ne sera pas mis à niveau.
- Les serveurs Security Server doivent posséder une version dans la même langue.
- Notez le nom d'hôte et le port d'écoute du serveur Security Server vers lequel l'agent est déplacé. Le nom d'hôte et le port d'écoute se trouvent sur l'écran Paramètres de sécurité du serveur Security Server, au-dessus du panneau Tâches.

Procédure

1. Sur la console Web du serveur Security Server qui gère actuellement les agents, accédez à **Dispositifs**.
2. Pour déplacer des agents Security Agent, cliquez sur un groupe puis sélectionnez les agents à déplacer. Pour déplacer un agent Messaging Security Agent, sélectionnez-le.
3. Cliquez sur **Autres** > **Déplacer Security Agent**.

   Un nouvel écran s'affiche.
4. Notez le nom d'hôte et le port d'écoute du serveur Security Server vers lequel les agents sont déplacés.

5. Cliquez sur **Déplacer**.

6. Pour vérifier que les agents dépendent maintenant de l'autre serveur Security Server, ouvrez la console Web du serveur concerné et recherchez les agents dans l'arborescence des groupes de sécurité.

Remarque

Si l'agent Security Agent n'apparaît pas dans l'arborescence des groupes de sécurité, redémarrez le service Trend Micro Security Server Master Service.

Déplacement d'un agent Security Agent entre plusieurs serveurs Security Server à l'aide de Client Mover

Avant de commencer

Lorsque vous déplacez un agent d'un serveur Security Server vers un autre :

- Si un agent exécute une version antérieure vers un serveur Security Server exécutant la version actuelle, l'agent sera mis à niveau automatiquement.
- Ne déplacez pas un agent exécutant la version actuelle vers un serveur Security Server exécutant une version antérieure, car l'agent ne sera plus géré (Il ne sera plus enregistré sur l'ancien serveur et ne parviendra pas à s'enregistrer sur le nouveau ; il n'apparaîtra donc plus sur les consoles Web respectives). L'agent gardera sa version actuelle et ne sera pas mis à niveau.
- Les serveurs Security Server doivent posséder une version dans la même langue.
- Notez le nom d'hôte et le port d'écoute du serveur Security Server vers lequel l'agent est déplacé. Le nom d'hôte et le port d'écoute se trouvent sur l'écran Paramètres de sécurité du serveur Security Server, au-dessus du panneau Tâches.

- Connectez-vous au client à l'aide d'un compte administrateur.

Procédure

1. Sur le client, ouvrez une invite de commande.

   Remarque

   Vous devez ouvrir l'invite de commande en tant qu'administrateur.

2. Saisissez `cd` ainsi que le chemin d'accès au dossier d'installation de Security Agent. Par exemple : `cd C:\Program Files\Trend Micro\Security Agent`

3. Exécutez Client Mover à l'aide de la syntaxe suivante :

   ```
   <nom du fichier exécutable> -s <nom du serveur> -p <port d'écoute du serveur> -c <port d'écoute du client> -pwd <Mot de passe du privilège de déchargement et de déverrouillage de l'agent>
   ```

TABLEAU 4-3. Paramètres de Client Mover

PARAMÈTRE	EXPLICATION
`<nom du fichier exécutable>`	`IpXfer.exe` (32 bits) `IpXfer_x64.exe` (64 bits)
`<nom du serveur>`	Nom du serveur Worry-Free Business Security de destination (serveur vers lequel l'agent doit être transféré)
`<port d'écoute du serveur>`	Port d'écoute (ou Port sécurisé) du serveur Security Server de destination
`<port d'écoute du client>`	Numéro de port utilisé par l'agent Security Agent pour communiquer avec le serveur
`<Mot de passe du privilège de déchargement et de déverrouillage de l'agent>`	Mot de passe utilisé pour décharger et déverrouiller Security Agent

Exemple :

```
Mot de passe ipXfer.exe -s Server01 -p 8080 -c 21112 -pwd
```

4. Pour vérifier que l'agent Security Agent dépend maintenant de l'autre serveur Security Server, ouvrez la console Web du serveur concerné et recherchez l'agent dans l'arborescence des groupes de sécurité.

Remarque

Si l'agent Security Agent n'apparaît pas dans l'arborescence des groupes de sécurité, redémarrez le service Trend Micro Security Server Master Service.

Réplication des paramètres

Répliquez des paramètres entre les groupes d'agents Security Agent ou entre les agents Messaging Security Agent (Advanced uniquement).

Réplication de paramètres de groupes d'agents Security Agent

Cette fonction permet d'appliquer les paramètres d'un groupe de postes de travail ou de serveurs à un autre groupe du même type. Vous ne pouvez pas répliquer les paramètres d'un groupe de serveurs sur un groupe de postes de travail, et inversement.

Si l'un des types de groupe ne compte qu'un seul groupe, la fonction sera désactivée.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur l'icône représentant un engrenage en regard du nom du groupe.

4. Cliquez sur **Répliquer les paramètres**.

   Un nouvel écran s'affiche.

5. Sélectionnez les groupes cibles qui hériteront des paramètres.

6. Cliquez sur **Appliquer**.

Réplication des paramètres de Messaging Security Agent (Advanced uniquement)

Vous ne pouvez répliquer les paramètres qu'entre des agents Messaging Security Agent partageant le même domaine.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur l'icône représentant un engrenage en regard de l'agent Messaging Security Agent.
4. Cliquez sur **Répliquer les paramètres**.

   Un nouvel écran s'affiche.

5. Sélectionnez l'agent Messaging Security Agent qui héritera des paramètres.
6. Cliquez sur **Appliquer**.
7. Si la réplication a réussi :
   a. Ouvrez l'Éditeur du Registre (regedit).
   b. Accédez à `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`.
   c. Cliquez avec le bouton droit de la souris sur **winreg** > **Autorisations**.

d. Ajoutez le **groupe admin Smex** du domaine cible et activez **Autoriser la lecture**.

Importation et exportation des paramètres des groupes Security Agent

Exportez les paramètres d'un groupe de postes de travail ou de serveurs vers un fichier `.dat` pour sauvegarder les paramètres. Vous pouvez également utiliser le fichier `.dat` pour importer les paramètres vers un autre groupe.

Remarque

Vous pouvez importer/exporter les paramètres entre des groupes de postes de travail et de serveurs. Les paramètres ne dépendent pas du type de groupe. Vous pouvez également utiliser la fonction **Répliquer les paramètres**, bien qu'elle dépende du type de groupe. Pour plus d'informations sur la fonction **Répliquer les paramètres**, voir *Réplication des paramètres à la page 4-17*.

TABLEAU 4-4. Paramètres pouvant être importés et exportés

SÉLECTION	ÉCRAN CONTENANT LES PARAMÈTRES	PARAMÈTRES POUVANT ÊTRE EXPORTÉS/IMPORTÉS
Groupe de postes de travail ( ) ou groupe de serveurs ( )	Dispositifs (**Dispositifs** > **Configurer la stratégie**)	• Antivirus/anti-programme espion (scan en temps réel) • Apprentissage automatique prédictif • Surveillance des comportements • Programme sécurisé • Mettre en quarantaine • Réputation de sites Web • Filtrage d'URL • Pare-feu • Contrôle des dispositifs • Outils utilisateur (disponible uniquement sur les groupes de postes de travail) • Privilèges d'agent
	Scan manuel (**Scans** > **Scan manuel**)	Tous les paramètres
	Scan programmé (**Scans** > **Scan programmé**)	Tous les paramètres

Exportation des paramètres

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.

3. Cliquez sur l'icône représentant un engrenage en regard du nom du groupe.
4. Cliquez sur **Exporter les paramètres de stratégie**.

   Un nouvel écran s'affiche.
5. Cliquez sur **Exporter**.

   Une boîte de dialogue s'affiche.
6. Cliquez sur **Enregistrer**, recherchez l'emplacement de votre choix, puis cliquez sur **Enregistrer**.

Importation des paramètres

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Importer les paramètres de stratégie**.

   Un nouvel écran s'affiche.
4. Cliquez sur **Parcourir**, trouvez le fichier, puis cliquez sur **Importer**.

Chapitre 5

Gestion des paramètres de sécurité de base des agents Security Agent

Ce chapitre explique comment configurer les paramètres de sécurité de base des agents Security Agent.

Synthèse des paramètres de sécurité de base des agents Security Agent

TABLEAU 5-1. Synthèse des paramètres de sécurité de base des agents Security Agent

OPTION	DESCRIPTION	PAR DÉFAUT
Méthode de scan	Configure Smart Scan pour l'activer ou le désactiver.	L'activation ou la désactivation est choisie durant l'installation.
Antivirus/anti-programme espion	Configure les options de scan en temps réel, d'antivirus et d'anti-spyware	Activé (scan en temps réel)
Apprentissage automatique prédictif	Configure les options d'apprentissage automatique prédictif	Désactivé
Surveillance des comportements	Configure les options de surveillance des comportements	Activé pour les groupes de postes de travail Désactivé pour les groupes de serveurs
Programme sécurisé	Spécifiez les programmes qu'il n'est pas nécessaire de surveiller en vue de détecter un éventuel comportement suspect	N/A
Mise en quarantaine	Spécifie le répertoire de mise en quarantaine	http://<Nom du serveur Security Server ou adresse IP>
Réputation de sites Web	Configure les options réputation de sites Web Au bureau et Hors du bureau	Au bureau : activé, faible Hors du bureau : activé, moyen
Filtrage d'URL	le filtrage d'URL bloque les sites Web enfreignant les stratégies configurées.	activé, faible

Option	Description	Par défaut
URL approuvées/bloquées	Configurez les listes approuvées/bloquées générales	Désactivé
Pare-feu.	Configure les options de pare-feu	Désactivé
Contrôle des dispositifs	Configure l'exécution automatique, ainsi que l'accès USB et réseau	Désactivé
Outils utilisateur	Configuration de l'évaluation des réseaux Wi-Fi et de la barre d'outils de Trend Micro Anti-Spam	Désactivé : Évaluation des réseaux Wi-Fi Désactivé : barre d'outils anti-spam dans les clients de messagerie pris en charge
Privilèges agent	Configure l'accès aux paramètres depuis la console de l'agent Désactiver la mise à niveau de Security Agent et le déploiement des correctifs de type hotfix	N/A

Méthodes de scan

Les Agents Security Agent peuvent utiliser l'une des deux méthodes de scan suivantes pour rechercher les menaces de sécurité.

- **Smart scan** : Dans ce document, les Agents Security Agent qui utilisent smart scan sont appelés les **agents Smart Scan**. Les agents Smart Scan bénéficient de scans locaux et de requêtes en ligne fournis par les services de File Reputation.
- **Scan traditionnel** : Les Agents Security Agent qui n'utilisent pas smart scan sont dénommés **agents de scan traditionnel**. Un agent de scan

traditionnel stocke tous les composants sur le client et scanne tous les fichiers localement.

Le tableau suivant compare les deux méthodes de scan.

TABLEAU 5-2. Comparaison entre le scan traditionnel et smart scan

BASE DE COMPARAISON	SCAN TRADITIONNEL	SMART SCAN
Comportement de scan	Le Security Agent de scan traditionnel effectue le scan sur le client.	• L'agent smart scan effectue le scan sur le client. • Si le Security Agent ne parvient pas à déterminer le risque auquel le fichier est exposé durant le scan, le Security Agent vérifie le risque en envoyant une requête à Scan Server (pour les Agents Security Agent connectés à Smart Scan Server) ou à Trend Micro Smart Protection Network (pour les Agents Security Agent déconnectés de Smart Scan Server). **Remarque** Le serveur de scan est un service s'exécutant sur Smart Scan Server. • Le Security Agent met en mémoire cache le résultat de la requête de scan pour améliorer les performances du scan.
Composants utilisés et mis à jour	Tous les composants Security Agent disponibles sur la source de mise à jour, hormis signatures de l'agent Smart Scan	Tous les composants disponibles sur la source de mise à jour, hormis le fichier de signatures de virus

BASE DE COMPARAISON	SCAN TRADITIONNEL	SMART SCAN
Source de mise à jour habituelle	Serveur ActiveUpdate	Serveur ActiveUpdate

Configuration des méthodes de scan

Avant de commencer

À l'installation du serveur Security Server, vous avez la possibilité d'activer smart scan. Si vous avez activé cette option, smart scan est la méthode de scan par défaut et sera donc utilisée par tous les agents Security Agent. Sinon, la méthode par défaut sera le scan traditionnel. Vous pouvez changer ces méthodes de scan des agents en fonction de vos exigences actuelles. Par exemple :

- si les agents utilisent actuellement le scan traditionnel et que l'exécution de la procédure prend beaucoup de temps, vous pouvez basculer sur smart scan, plus rapide et plus efficace. Vous pouvez également utiliser la fonction smart scan lorsque l'espace disque libre sur l'agent diminue. Les agents smart scan téléchargent des fichiers de signature moins volumineux, qui nécessitent donc moins d'espace disponible.

  Avant de basculer vers Smart Scan, accédez à **Administration** > **Paramètres généraux**, cliquez sur l'onglet **Poste de travail/serveur**, puis accédez à la section **Paramètres de scan généraux**. Assurez-vous que l'option **Désactiver le service Smart Scan** est désactivée.

- Basculez les agents sur le scan traditionnel si vous remarquez une baisse des performances dans le serveur Security Server, ce qui indique son incapacité à traiter toutes les requêtes de scan des agents en temps et en heure.

Le tableau suivant répertorie d'autres éléments à prendre en compte lorsque vous changez de méthode de scan :

TABLEAU 5-3. Éléments à prendre en compte lors du changement de méthode de scan

ÉLÉMENTS À PRENDRE EN COMPTE	DÉTAILS
Connexion au serveur Security Server	Vérifiez que les agents Security Agent peuvent se connecter au serveur Security Server. Seuls les agents en ligne seront invités à passer à une méthode de scan différente. Les agents hors ligne sont notifiés lorsqu'ils sont en ligne. Vérifiez également que le serveur Security Server dispose des derniers composants, car les agents doivent télécharger de nouveaux composants à partir du serveur Security Server, c'est-à-dire, signatures de l'agent Smart Scan pour les agents qui passent à Smart Scan et Virus Pattern pour les agents qui passent au scan traditionnel.
Nombre d'agents Security Agent devant basculer	Le basculement simultané d'un nombre d'agents Security Agent relativement réduit permet d'utiliser efficacement les ressources du serveur Security Server. Le serveur Security Server peut effectuer d'autres tâches critiques lorsque les agents changent de méthode de scan.
Synchronisation	Lors du basculement des agents Security Agent pour la première fois, les agents doivent télécharger la **version complète** de signatures de l'agent Smart Scan (pour les agents basculant vers smart scan) ou Virus Pattern (pour les agents basculant vers le scan traditionnel). Prévoyez d'effectuer le basculement pendant les heures creuses pour vous assurer que le processus de téléchargement se termine rapidement. De plus, désactivez temporairement l'option « Mettre à jour » sur les agents pour éviter les mises à jour déclenchées par les utilisateurs et réactivez-la lorsque les agents ont changé de méthode de scan. **Remarque** Par la suite, les agents téléchargeront des versions **incrémentielles plus petites** de signatures de l'agent Smart Scan ou Virus Pattern, à condition d'être fréquemment mis à jour.

Éléments à prendre en compte	Détails
Prise en charge d'IPv6	Un agent Smart Scan IPv6 pur se trouvant hors ligne ne peut pas envoyer directement de requêtes à Trend Micro Smart Protection Network. Un serveur proxy double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents smart scan d'envoyer des requêtes.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Accédez à **Méthode de scan**.
5. Sélectionnez votre méthode de scan favorite.
6. Cliquez sur **Enregistrer**.

Scan en temps réel pour les agents Security Agent

Le scan en temps réel s'effectue en continu. Chaque fois qu'un fichier est ouvert, téléchargé, copié ou modifié, le scan en temps réel dans l'agent **Security Agent** s'exécute pour détecter les menaces éventuelles.

Configuration du scan en temps réel pour les agents Security Agent

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Cliquez sur **Antivirus/anti-programme espion**.

   Un nouvel écran s'affiche.
5. Sélectionnez **Activer le scan antivirus/anti-programme espion en temps réel**.
6. Configurez les paramètres de scan. Pour plus d'informations, voir *Cibles de scan et actions des agents Security Agent à la page 7-10* :

   Remarque

   Si vous autorisez les utilisateurs à configurer leurs propres paramètres de scan, ces derniers seront utilisés lors du scan.
7. Cliquez sur **Enregistrer**.

Apprentissage automatique prédictif

L'apprentissage automatique prédictif de Trend Micro utilise des technologies d'apprentissage automatique avancées pour mettre en corrélation des informations liées aux menaces et exécuter des analyses approfondies afin de détecter l'apparition de risques inconnus liés à la sécurité, grâce à l'empreinte digitale numérique, à la correspondance des API et à d'autres fonctions liées aux fichiers. L'apprentissage automatique

prédictif effectue également une analyse comportementale sur des processus inconnus ou de faible prévalence afin de détecter les tentatives d'infection de votre réseau par une menace émergente ou inconnue.

L'apprentissage automatique prédictif est un outil puissant qui contribue à protéger votre environnement contre les menaces non identifiées et les attaques émergentes.

Type de détection	Description
Fichier	Après la détection d'un fichier inconnu ou à faible prévalence, l'Security Agent analyse le fichier à l'aide du Moteur de scan de menaces avancées (ATSE) pour extraire des caractéristiques de fichiers et envoie le rapport au moteur d'apprentissage automatique prédictif, hébergé sur le réseau Trend Micro Smart Protection Network. Grâce à l'utilisation de la modélisation de programmes malveillants, l'apprentissage automatique prédictif compare l'exemple au modèle de programme malveillants, affecte un score de probabilité et détermine le type de programme malveillant potentiel contenant le fichier. Selon la configuration d'apprentissage automatique prédictif, l'Security Agent peut tenter de « mettre en quarantaine » le fichier affecté pour éviter que la menace ne continue à se propager sur votre réseau.
Processus	Après la détection d'un processus inconnu ou à faible prévalence, l'Security Agent surveille le processus en utilisant le moteur d'intelligence contextuelle et envoie le rapport comportemental au moteur d'apprentissage automatique prédictif. Grâce à l'utilisation de la modélisation de programmes malveillants, l'apprentissage automatique prédictif compare le comportement du processus au modèle de programme, affecte un score de probabilité et détermine le type de programme malveillant potentiel contenant le fichier. Selon la configuration de l'apprentissage automatique prédictif, l'Security Agent peut « Interrompre » le processus concerné et tenter de nettoyer le fichier ayant exécuté le processus ou le script.

Configuration de l'apprentissage automatique prédictif

Remarque

L'apprentissage automatique prédictif requiert les éléments suivants :

- L'activation de la surveillance des comportements dans **Configurer la stratégie** > **Surveillance des comportements**
- Une connexion Internet fonctionnelle pour se connecter à Smart Protection Network

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Cliquez sur **Apprentissage automatique prédictif**.
5. Sélectionnez **Activer l'apprentissage automatique prédictif**.
6. Sélectionnez le type de détection et l'action associée que doit effectuer l'apprentissage automatique prédictif.

TYPE DE DÉTECTION	ACTIONS
Fichier	• **Mettre en quarantaine** : Sélectionnez cette option pour mettre automatiquement en quarantaine les fichiers qui présentent des fonctionnalités associées aux programmes malveillants sur la base de l'analyse d'apprentissage automatique prédictif • **Consigner uniquement** : Sélectionnez cette option pour scanner les fichiers inconnus et consigner l'analyse de l'apprentissage automatique prédictif pour un examen interne plus poussé de la menace

Type de détection	Actions
Processus	• **Interrompre** : Sélectionnez cette option pour arrêter automatiquement les processus ou les scripts qui présentent des comportements de programmes malveillants sur la base de l'analyse de l'apprentissage automatique prédictif **Important** L'apprentissage automatique prédictif tente de nettoyer les fichiers exécutés par les processus ou les scripts malveillants. Si l'action de nettoyage a échoué, l'apprentissage automatique prédictif met les fichiers concernés en quarantaine. • **Consigner uniquement** : Sélectionnez cette option pour scanner les processus ou les scripts inconnus et consigner l'analyse de l'apprentissage automatique prédictif pour un examen interne plus poussé de la menace

7. Cliquez sur **Enregistrer**.

Surveillance des comportements

Les agents Security Agent surveillent constamment les clients pour détecter d'éventuelles modifications inhabituelles apportées au système d'exploitation ou aux logiciels installés. Les administrateurs (ou utilisateurs) peuvent créer des listes d'exceptions permettant à certains programmes de démarrer alors qu'ils enfreignent une modification surveillée ou permettant de bloquer totalement certains programmes. De plus, les programmes dotés d'une signature numérique valide sont toujours autorisés à démarrer.

Une autre fonction de la surveillance des comportements vise à protéger les fichiers EXE et DLL des suppressions ou modifications. Lorsque la surveillance des comportements est activée, les utilisateurs créent des exceptions pour approuver ou bloquer des programmes spécifiques. De plus,

les utilisateurs peuvent choisir de protéger collectivement tous les programmes Intuit QuickBooks.

Configuration de la surveillance des comportements

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Cliquez sur **Surveillance des comportements**.
5. Mettez à jour les éléments suivants, si nécessaire :
   - **Activer la surveillance des comportements**

     Remarque

     Pour permettre aux utilisateurs de personnaliser leurs paramètres de surveillance des comportements, accédez à **Dispositifs** > **{groupe}** > **Configurer la stratégie** > **Privilèges agent** > **Surveillance des comportements** et sélectionnez **Autoriser aux utilisateurs de modifier les paramètres de surveillance des comportements**.
   - **Activer le blocage des comportements de programmes malveillants pour les menaces connues et potentielles** : vous pouvez bloquer le comportement des programmes malveillants en utilisant un ensemble de règles internes définies dans des **fichiers de signature**. Ces règles identifient les comportements connus suspects qui sont communs aux programmes malveillants. L'exécution soudaine et inexplicable de nouveaux services, les modifications du pare-feu ou encore, les modifications du système de fichiers, sont des exemples de comportements suspects.

     La surveillance des comportements de programmes malveillants fournit les options de scan de niveau de menace suivantes :

- **Menaces connues** : bloque le comportement associé aux menaces connues.
- **Menaces connues et potentielles** : bloque le comportement associé aux menaces connues et prend des mesures en cas de détection d'un comportement potentiellement malveillant.

- **Inviter les utilisateurs avant d'exécuter les derniers programmes détectés et téléchargés par HTTP (à l'exclusion des plates-formes serveur)** : la surveillance des comportements fonctionne en association avec la réputation de sites Web pour vérifier la prévalence de fichiers téléchargés par des canaux HTTP ou des applications de messagerie. Les administrateurs peuvent choisir de présenter une invite aux utilisateurs avant d'exécuter un fichier nouvellement détecté. Trend Micro classe un programme comme étant nouvellement détecté en fonction du nombre de détections de fichiers ou de l'âge du fichier tels qu'ils sont déterminés par Smart Protection Network.

  Remarque

  Pour les canaux HTTP, les fichiers exécutables (.exe) sont scannés. Pour les applications de messagerie (uniquement Outlook et Windows Live Mail), les fichiers exécutables (.exe) présents dans les fichiers archivés (zip/rar) non protégés par mot de passe font l'objet d'un scan.

- **Activer la protection Intuit QuickBooks** : cette fonctionnalité protège tous les fichiers et dossiers QuickBooks pour empêcher les modifications non autorisées par d'autres programmes. L'activation de cette fonction n'affecte pas les modifications apportées depuis les programmes Intuit QuickBooks, mais seulement les modifications apportées aux fichiers par d'autres applications non autorisées.

  Les produits suivants sont pris en charge :

  - QuickBooks Simple Start
  - QuickBooks Pro

- QuickBooks Premier
- QuickBooks Online

Remarque

Tous les fichiers exécutables Intuit ont une signature numérique et les mises à jour de ces fichiers ne seront pas bloquées. Si d'autres programmes tentent de modifier les fichiers binaires Intuit, l'agent affiche un message avec le nom du programme qui tente de les mettre à jour. D'autres programmes peuvent être autorisés à mettre à jour des fichiers Intuit. Pour ce faire, ajoutez le programme requis à la liste d'exception de la surveillance des comportements sur l'agent. Veillez bien à supprimer le programme de la liste d'exceptions après la mise à jour.

- **Protection contre les logiciels de rançon** : empêche que des fichiers soient modifiés ou chiffrés sans autorisation sur des ordinateurs par des menaces de « logiciels de rançon ». Un logiciel de rançon est un type de programme malveillant qui restreint l'accès à des fichiers et exige un paiement pour restaurer les fichiers affectés.
  - **Activer la protection des documents contre toute opération de chiffrement ou de modification non autorisée** : protège les documents contre toute modification non autorisée.
    - **Sauvegarder automatiquement les fichiers modifiés par des programmes suspects** : sauvegarde automatiquement les fichiers modifiés par des programmes suspects si la protection des documents est activée.
  - **Activer le blocage des processus couramment associés aux rançongiciels** : protège les endpoints des attaques par rançongiciels en bloquant les processus généralement associés à des tentatives de piratage.
  - (groupes de postes de travail uniquement) **Activer le programme d'inspection pour détecter et bloquer les fichiers exécutables compromis** : améliore la détection par les

processus de surveillance de comportements de type logiciels de rançon.

- **Arrêter les programmes qui présentent un comportement anormal associé à des attaques par exploitation** : la protection contre les exploitations s'associe à l'inspection des programmes pour surveiller le comportement des programmes et détecter tout comportement anormal pouvant indiquer qu'un pirate a exploité une faille de sécurité d'un programme. Après la détection d'un comportement anormal, la fonction de surveillance des comportements met fin aux processus du programme.

  Remarque

  La protection contre les exploitations impose la sélection de l'option **Activer l'inspection des programmes afin de détecter et de bloquer les fichiers exécutables compromis**.

Remarque

Pour limiter le risque de détection d'un processus sans danger comme malveillant, Worry-Free Business Security vérifie que l'ordinateur a accès à Internet pour effectuer un processus de vérification supplémentaire à l'aide de serveurs Trend Micro.

- **Exceptions**: les exceptions incluent une liste de programmes approuvés et une liste de programmes bloqués. Vous pouvez exécuter un programme de la liste des programmes approuvés même si cela enfreint une modification surveillée ; en revanche, il est impossible d'exécuter un programme de la liste des programmes bloqués.

  - **Saisissez le chemin d'accès complet au programme**: tapez le chemin d'accès Windows ou UNC complet au programme. Séparez les entrées multiples par des points-virgules. Cliquez sur **Ajouter à la liste approuvée** ou **Ajouter à la liste bloquée**. Utilisez les variables d'environnement pour indiquer des chemins, si nécessaire.

- **Liste des programmes approuvés** : les programmes de cette liste peuvent être démarrés. Pour supprimer une entrée, cliquez sur l'icône correspondante.

  La liste des programmes approuvés prend en charge les caractères génériques et les variables d'environnement.

  Pour obtenir la liste des variables d'environnement prises en charge, voir *Variables d'environnement prises en charge à la page 5-16*.

- **Liste des programmes bloqués** : les programmes de cette liste ne peuvent jamais être démarrés. Pour supprimer une entrée, cliquez sur l'icône correspondante.

  La liste des programmes bloqués prend uniquement en charge les caractères génériques.

6. Cliquez sur **Enregistrer**.

Variables d'environnement prises en charge

Le tableau suivant répertorie les variables d'environnement que vous pouvez utiliser lorsque vous ajoutez un chemin de fichier ou de dossier à la liste.

Variable d'environnement	Exemple	Chemin équivalent
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe
$programdir$	$programdir$\test\sample.exe	C:\Program Files\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Program Files (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe

Variable d'environnement	Exemple	Chemin équivalent
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{current_user_account}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

Programme sécurisé

Les programmes figurant dans la liste des programmes de confiance ne font pas l'objet d'une surveillance destinée à détecter les activités suspectes d'accès aux fichiers.

Configuration du programme sécurisé

Remarque

La liste des programmes sécurisés ne prend pas en charge les caractères génériques et les variables d'environnement.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.

4. Cliquez sur **Programme sécurisé**.

   Un nouvel écran s'affiche.

5. Pour exclure un programme de la surveillance destinée à détecter les activités suspectes d'accès aux fichiers, saisissez le chemin complet du fichier, à l'aide d'un chemin de fichier spécifique, puis cliquez sur **Ajouter à la liste des programmes de confiance**.

   `<drive_name>:/<path>/<file_name>`

   Exemple 1 : `C:\Windows\system32\regedit.exe`

   Exemple 2 : `D:\backup\tool.exe`

   Cela empêche les pirates d'utiliser les noms de programme dans la liste des exclusions, car ils sont glissés dans un chemin d'accès de fichier différent à exécuter.

6. Cliquez sur **Enregistrer**.

Répertoire de quarantaine

Si l'action à entreprendre pour le fichier infecté est « Mettre en quarantaine », l'agent Security Agent encode le fichier et le déplace **temporairement** dans un fichier de quarantaine situé dans :

- `<dossier d'installation de Security Agent>\quarantine` pour les agents mis à niveau à partir de la version 6.x ou d'une version antérieure.
- `<dossier d'installation de Security Agent>\SUSPECT\Backup` pour les nouveaux agents et ceux mis à niveau à partir de la version 7.x ou d'une version supérieure.

L'agent Security Agent envoie le fichier infecté vers un répertoire de quarantaine centralisé que vous pouvez configurer à partir de la console Web, dans **Dispositifs** > **{Groupe}** > **Configurer la stratégie** > **Mettre en quarantaine**.

Répertoire de quarantaine centralisé par défaut

Le répertoire de quarantaine centralisé par défaut est situé sur le serveur Security Server. Le répertoire est au format URL et contient le nom d'hôte ainsi que l'adresse IP du serveur Security Server (ex. : `http://server`). Le chemin absolu correspondant est `<dossier d'installation de Security Server>\PCCSRV\Virus`.

- Si le serveur gère simultanément des agents IPv4 et des agents IPv6, utilisez le nom d'hôte de façon à ce que tous les agents puissent envoyer des fichiers mis en quarantaine vers le serveur.
- Si le serveur dispose uniquement d'une adresse IPv4 ou qu'il est identifié par celle-ci, seuls les agents IPv4 purs et les agents double pile peuvent envoyer des fichiers mis en quarantaine vers le serveur.
- Si le serveur dispose uniquement d'une adresse IPv6 ou qu'il est identifié par celle-ci, seuls les agents IPv6 purs et les agents double pile peuvent envoyer des fichiers mis en quarantaine vers le serveur.

Répertoire de quarantaine centralisé alternatif

Vous pouvez définir un autre répertoire de quarantaine centralisé en saisissant l'emplacement au format URL, dans le chemin UNC ou dans le chemin de fichier absolu. Les agents Security Agent doivent pouvoir se connecter à ce répertoire. Par exemple, le répertoire alternatif doit avoir une adresse IPv6 s'il est susceptible de recevoir des fichiers mis en quarantaine d'agents double pile et d'agents IPv6 purs. Trend Micro vous recommande de concevoir un répertoire double pile, qui sera identifié par son nom d'hôte et pour lequel vous utiliserez le chemin UNC lorsque vous le saisirez.

Instructions sur la manière de définir le répertoire de quarantaine centralisé

Reportez-vous au tableau suivant pour obtenir de l'aide sur l'utilisation d'une URL, d'un chemin UNC ou d'un chemin de fichier absolu :

TABLEAU 5-4. Répertoire de quarantaine

RÉPERTOIRE DE QUARANTAINE	FORMAT ACCEPTÉ	EXEMPLE	REMARQUES
Répertoire par défaut sur le serveur Security Server	URL	`http:// <nom d'hôte ou adresse IP du serveur>`	Si vous souhaitez conserver le répertoire par défaut, configurez les paramètres de maintenance correspondants, tels que la taille du dossier de quarantaine, dans la section **Administration** > **Paramètres généraux** > **Onglet Système** > **Maintenance de la mise en quarantaine**.
	Chemin UNC	`\\<nom d'hôte ou adresse IP du serveur>\ ofcscan\Virus`	
Autre répertoire sur le serveur Security Server	Chemin UNC	`\\<nom d'hôte ou adresse IP du serveur>\ D$ \Quarantined Files`	Si vous ne souhaitez pas utiliser le répertoire par défaut (par exemple, parce que l'espace disque est insuffisant), tapez le nom du chemin UNC menant à un autre répertoire. Dans ce cas, tapez le chemin absolu correspondant dans la section **Administration** > **Paramètres généraux** > **Onglet Système** > **Maintenance de la mise en quarantaine** pour que les paramètres de maintenance prennent effet.

Répertoire de quarantaine	Format accepté	Exemple	Remarques
Un répertoire sur un autre ordinateur Security Server (si vous possédez d'autres serveurs Security Server sur votre réseau)	URL	`http:// <nom d'hôte ou adresse IP du serveur2>`	Vérifiez que les agents peuvent se connecter à ce répertoire. Si vous spécifiez un répertoire non valide, l'agent conserve les fichiers en quarantaine jusqu'à ce que vous spécifiiez un répertoire de quarantaine valide. Dans les journaux de virus/programmes malveillants du serveur, le résultat de scan est « Impossible d'envoyer le fichier en quarantaine vers le dossier de quarantaine spécifié ». Si vous utilisez un chemin UNC, vérifiez que le répertoire de quarantaine est partagé avec le groupe « Tous » et que vous avez attribué des privilèges de lecture et d'écriture à ce groupe.
	Chemin UNC	`\\<nom d'hôte ou adresse IP du serveur2>\ofcscan\Virus`	
Autre ordinateur du réseau	Chemin UNC	`\\<computer_name>\temp`	
Autre répertoire installé sur le client	Chemin de fichier absolu	`C:\temp`	Spécifiez un répertoire absolu si : • Vous souhaitez que les fichiers mis en quarantaine restent enregistrés uniquement sur le client. • Vous ne souhaitez pas que les agents enregistrent les fichiers dans le répertoire par défaut du client. Si le chemin n'existe pas, l'agent Security Agent le crée automatiquement.

Configuration du répertoire de quarantaine

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Cliquez sur **Mettre en quarantaine**.

   Un nouvel écran s'affiche.
5. Configurez le répertoire de quarantaine. Pour plus de détails, voir *Répertoire de quarantaine à la page 5-18*.
6. Cliquez sur **Enregistrer**.

Réputation de sites Web

La réputation de sites Web contribue à empêcher l'accès aux URL sur le Web ou incorporés dans des messages électroniques qui représentent des risques potentiels. La réputation de sites Web vérifie la réputation de l'URL sur les serveurs de réputation de sites Web de Trend Micro, puis la corrèle avec la stratégie de réputation Web spécifique appliquée sur le client. Selon la stratégie utilisée :

- Security Agent doit bloquer ou autoriser l'accès à un site Web.
- Messaging Security Agent (Advanced uniquement) mettra en quarantaine, supprimera ou marquera le message contenant des URL malveillantes ou autorisera l'envoi du message si les URL sont sûres.

La réputation de sites Web envoie à la fois une notification par e-mail à l'administrateur et une notification en ligne à l'utilisateur pour les détections.

Selon l'emplacement (Au bureau/Hors du bureau) du client, configurez un niveau de sécurité différent pour les agents Security Agent.

Si la réputation de sites Web bloque une URL que vous pensez sûre, ajoutez-le à la liste des URL approuvées.

Conseil

Pour économiser la bande passante, Trend Micro recommande d'ajouter les sites Web internes de l'entreprise à la liste des URL approuvées établie par la fonction de réputation de sites Web.

Score de réputation

Le « score de réputation » d'une URL détermine s'il s'agit d'une menace Internet ou non. Trend Micro calcule le score à l'aide de mesures propriétaires.

Trend Micro considère une URL comme étant une menace Internet si le score atteint se situe dans la plage définie et comme sûre si le score dépasse le seuil.

Un agent Security Agent dispose de trois niveaux de sécurité en fonction desquels il autorise ou bloque l'accès à une URL.

- **Élevé** : Bloque les pages qui sont :
  - **Dangereux :** caractère frauduleux avéré ou sources de menaces connues
  - **Hautement suspect** : caractère frauduleux suspecté ou sources de menaces possibles
  - **Suspect** : associées à du spam ou potentiellement compromises
  - **Non testée** : Bien que Trend Micro teste activement la sécurité des pages Web, les utilisateurs peuvent rencontrer des pages non testées lorsqu'ils visitent des sites Web nouveaux ou peu consultés. Le blocage de l'accès aux pages non testées peut améliorer la sécurité, mais il peut également empêcher l'accès à des pages sûres.

- **Moyen** : Bloque les pages qui sont :
  - **Dangereux :** caractère frauduleux avéré ou sources de menaces connues
  - **Hautement suspect** : caractère frauduleux suspecté ou sources de menaces possibles
- **Faible** : Bloque les pages qui sont :
  - **Dangereux :** caractère frauduleux avéré ou sources de menaces connues

Configuration de la réputation des sites Web pour agents Security Agent

L'outil d'évaluation de la réputation des sites Web évalue le risque de sécurité potentiel de toutes les URL demandées, en interrogeant la base de données de sécurité de Trend Micro lors de chaque requête HTTP/HTTPS.

Remarque

(Standard uniquement) Configurez les paramètres de la réputation de sites Web pour Au bureau et Hors du bureau. Si la détection d'emplacement est désactivée, les paramètres Au bureau seront utilisés pour les connexions Hors du bureau. Pour plus d'informations sur la détection d'emplacement, voir *Configuration des paramètres des postes de travail/serveurs à la page 11-5*.

Si la réputation des sites Web et la prévention d'exploitation de faille de navigateur sont toutes deux activées, les URL qui ne sont pas bloquées par la réputation des sites Web sont ensuite scannées par la prévention d'exploitation de faille de navigateur. Cette dernière scanne les objets incorporés (par exemple :fichiers jar, class, pdf, swf, html, js) dans les pages Web de l'URL.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.

3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.

4. Cliquez sur **Réputation de sites Web** > **Au bureau** ou **Réputation des sites Web** > **Hors du bureau**.

   Un nouvel écran s'affiche.

5. Mettez à jour les éléments suivants, si nécessaire :

   - **Activer la réputation des sites Web**
   - Niveau de sécurité : **Élevé**, **Moyen** ou **Faible**
   - Prévention d'exploitation de faille de navigateur : **Bloquer les pages contenant un script malveillant**

6. Cliquez sur **Enregistrer**.

Filtrage d'URL

Le filtrage d'URL vous aide a contrôler l'accès aux sites Web pour réduire les périodes d'improductivité du personnel, diminuer l'utilisation de la bande passante et créer un environnement Internet plus sûr. Vous pouvez définir un niveau de protection par filtrage URL ou personnaliser les types de sites Web que vous souhaitez surveiller.

Remarque

Pour protéger les clients, Trend Micro bloque automatiquement toutes les URL avec du contenu considéré comme illégal dans la plupart des pays.

Configuration du filtrage d'URL

Vous pouvez sélectionner des types spécifiques de sites Web à bloquer à différents moments de la journée en sélectionnant **Personnalisé**.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Cliquez sur **Filtrage d'URL**.

   Un nouvel écran s'affiche.
5. Mettez à jour les éléments suivants, si nécessaire :
   - **Activer le filtrage d'URL**
   - **Niveau de filtrage**
     - **Élevé** : Bloque les menaces de sécurité connues ou potentielles, le contenu inapproprié ou potentiellement injurieux, le contenu nuisible à la productivité ou à la bande passante et les pages non classifiées
     - **Moyen** : Bloque les menaces de sécurité connues et le contenu inapproprié
     - **Faible** : Bloque les menaces de sécurité connues
     - **Personnalisée** : Sélectionnez vos propres catégories, que vous souhaitiez les bloquer pendant les heures de bureau ou les heures de temps libre.
   - **Règles de filtre** : sélectionnez des catégories entières ou des sous-catégories à bloquer.
   - **Heures de bureau** : Les jours ou les heures qui ne sont pas définis comme des heures de bureau sont considérés comme des heures de temps libre.
6. Cliquez sur **Enregistrer**.

URL approuvées/bloquées

L'approbation et le blocage automatiques d'URL vous permettent de contrôler l'accès aux sites Web et de créer un environnement Internet plus sûr. L'identification des URL approuvées ou bloquées s'effectue dans les paramètres généraux.

Vous pouvez également créer des listes personnalisées d'approbation et de blocage d'URL pour des groupes spécifiques. Lorsque l'option **Personnaliser les URL approuvées/bloquées pour ce groupe** est sélectionnée, Security Agent utilise la liste personnalisée d'URL approuvées ou bloquées du groupe pour contrôler l'accès aux sites Web.

Configuration des URL approuvées/bloquées

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Cliquez sur **URL approuvées/bloquées**.

   Un nouvel écran s'affiche.
5. Mettez à jour les éléments suivants, si nécessaire.
   - **Personnaliser les URL approuvées/bloquées de ce groupe** : Les URL reprises dans cette liste remplacent tous les autres paramètres.
   - Dans la zone de texte **URL à approuver**, saisissez les URL de sites Web à exclure des vérifications de réputation de sites Web et de filtrage d'URL. Séparez les URL multiples par un point virgule (;). Cliquez sur **Ajouter**.

Conseil

Cliquez sur **Importer à partir des paramètres généraux** pour insérer toutes les entrées. Vous pouvez ensuite personnaliser les URL de ce groupe.

- Dans la zone de texte **URL à bloquer**, saisissez les URL de sites Web à bloquer pendant le filtrage d'URL. Séparez les URL multiples par un point virgule (;). Cliquez sur **Ajouter**.

Conseil

Cliquez sur **Importer à partir des paramètres généraux** pour insérer toutes les entrées. Vous pouvez ensuite personnaliser les URL de ce groupe.

6. Cliquez sur **Enregistrer**.

Pare-feu.

Le pare-feu peut bloquer ou autoriser certains types de trafic réseau en créant une barrière entre le client et le réseau. En outre, le pare-feu identifie les signatures dans les paquets réseau qui sont susceptibles d'indiquer une attaque visant les clients.

Worry-Free Business Security vous permet de choisir entre deux options lorsque vous configurez le pare-feu : le mode simple et le mode avancé. Le mode simple active le pare-feu avec les paramètres par défaut recommandés par Trend Micro. Le mode avancé permet de personnaliser les paramètres du pare-feu.

Conseil

Trend Micro recommande de désinstaller les autres pare-feux logiciels avant de déployer et d'activer le pare-feu de Trend Micro.

Paramètres par défaut du mode simple du pare-feu

Le pare-feu fournit des paramètres par défaut que vous pouvez utiliser comme référence pour la mise en place de votre stratégie de protection des clients par pare-feu. Les paramètres par défaut sont conçus pour inclure des conditions habituelles propres aux clients, comme le besoin d'accéder à Internet et de télécharger des fichiers depuis et vers un FTP.

Remarque

Par défaut, Worry-Free Business Security désactive le pare-feu pour tous les nouveaux groupes et agents Security Agent.

TABLEAU 5-5. paramètres par défaut du pare-feu

PARAMÈTRES	ÉTAT
Niveau de sécurité	Faible Trafic entrant et sortant autorisé, seuls les virus de réseau sont bloqués.
Système de détection d'intrusion	Désactivé
Message d'alerte (envoyé)	Désactivé

TABLEAU 5-6. Exceptions par défaut du pare-feu

NOM DE L'EXCEPTION	ACTION	DIRECTION	PROTOCOLE	PORT
DNS	Autoriser	Entrant et sortant	TCP/UDP	53
NetBIOS	Autoriser	Entrant et sortant	TCP/UDP	137, 138, 139, 445
HTTPS	Autoriser	Entrant et sortant	TCP	443
HTTP	Autoriser	Entrant et sortant	TCP	80

Nom de l'exception	Action	Direction	Protocole	Port
Telnet	Autoriser	Entrant et sortant	TCP	23
SMTP	Autoriser	Entrant et sortant	TCP	25
FTP	Autoriser	Entrant et sortant	TCP	21
POP3	Autoriser	Entrant et sortant	TCP	110
MSA	Autoriser	Entrant et sortant	TCP	16372, 16373
LDAP	Autoriser	Entrant et sortant	TCP/UDP	389

Tableau 5-7. Paramètres par défaut du pare-feu en fonction de l'emplacement

Emplacement	Paramètres du pare-feu
Au bureau	Désactivé
Hors du bureau	Désactivé

Filtrage du trafic

Le pare-feu personnel filtre l'ensemble du trafic entrant et sortant, permettant ainsi de bloquer certains types de trafic sur la base des critères suivants :

- Direction (entrant/sortant)
- Protocole (TCP/UDP/ICMP/ICMPv6)
- Ports de destination
- Ordinateur de destination

Recherche de virus de réseau

Le pare-feu vérifie également la présence de virus de réseau dans chaque paquet.

Stateful Inspection (Inspection avec état)

Le pare-feu est un pare-feu de type stateful inspection ; il contrôle toutes les connexions au client et mémorise tous les états de connexion. Il peut identifier les conditions spécifiques de toute connexion, prédire les actions qui doivent être effectuées et détecter toute anomalie de connexion. L'utilisation efficace du pare-feu repose donc non seulement sur la création de profils et de stratégies, mais aussi sur l'analyse des connexions et le filtrage des paquets qui transitent par le pare-feu.

Pilote du pare-feu commun

Combiné aux paramètres de pare-feu définis par l'utilisateur, le pilote de pare-feu commun bloque les ports en cas d'épidémie. Le pilote de pare-feu commun utilise également le fichier de signatures des virus de réseau pour détecter les virus de réseau.

Configuration du pare-feu

Configurez le pare-feu pour Au bureau et Hors du bureau. Si la détection d'emplacement est désactivée, les paramètres Au bureau seront utilisés pour les connexions Hors du bureau.

Pour plus d'informations sur la détection d'emplacement, voir *Configuration des paramètres des postes de travail/serveurs à la page 11-5*.

Trend Micro désactive le pare-feu par défaut.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.

4. Cliquez sur **Pare-feu** > **Au bureau** ou **Hors du bureau**.
5. Sélectionnez **Activer le pare-feu**.
6. Sélectionnez l'un des systèmes suivants :
   - **Mode simple** : activez le pare-feu avec les paramètres par défaut.

     Pour plus de détails, voir *Pare-feu. à la page 5-28*.
   - **Mode avancé** : active le pare-feu avec des paramètres personnalisés.
7. Si vous avez sélectionné **Mode avancé**, mettez à jour les options suivantes au besoin :
   - **Niveau de sécurité** : le niveau de sécurité contrôle les règles de trafic à appliquer pour les ports qui ne figurent pas dans la liste d'exceptions.
     - **Élevé** : bloque l'ensemble du trafic entrant et sortant, sauf le trafic autorisé dans la liste d'exceptions.
     - **Moyen** : bloque l'ensemble du trafic entrant et autorise l'intégralité du trafic sortant, sauf le trafic autorisé et bloqué dans la liste d'exceptions.
     - **Faible** : autorise l'ensemble du trafic entrant et sortant, sauf le trafic bloqué dans la liste d'exceptions. Il s'agit du paramètre par défaut pour le Mode simple.
   - **Paramètres**
     - **Activer le système de détection d'intrusion** : le système de détection d'intrusion identifie les signatures des paquets réseau susceptibles d'indiquer une attaque.

       Pour plus de détails, voir *Système de détection d'intrusion à la page D-4*.
     - **Activer les messages d'alerte** : lorsque Worry-Free Business Security détecte une violation, le client est averti.

- **Exceptions**: les ports de la liste d'exceptions ne seront pas bloqués.

  Pour obtenir des informations détaillées, consultez *Gestion des exceptions du pare-feu à la page 5-33*.

8. Cliquez sur **Enregistrer**.

Gestion des exceptions du pare-feu

La liste des exceptions du pare-feu contient des entrées que vous pouvez configurer de manière à autoriser ou à bloquer divers types de trafic réseau en fonction des numéros de port du client et des adresses IP. Lors d'une épidémie, Security Server applique les exceptions aux stratégies Trend Micro, qui sont automatiquement déployées pour protéger votre réseau.

Par exemple, pendant une épidémie, vous pouvez choisir de bloquer tout le trafic des clients, y compris le port HTTP (port 80). Cependant, si vous souhaitez accorder l'accès Internet aux clients bloqués, vous pouvez ajouter le serveur proxy Web à la liste des exceptions.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Cliquez sur **Pare-feu** > **Au bureau** ou **Pare-feu** > **Hors du bureau**.

   Un nouvel écran s'affiche.
5. Sélectionnez **Activer le pare-feu**.
6. Sélectionnez **Mode avancé** :
7. Pour ajouter une exception :

a. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

b. Entrez un nom pour l'exception.

c. En regard de **Action**, cliquez sur l'une des options suivantes :

   - **Autoriser tout le trafic réseau**
   - **Refuser tout le trafic réseau**

d. En regard de **Direction**, cliquez sur **Entrant** ou **Sortant** pour sélectionner le type de trafic auquel appliquer les paramètres de cette exception.

e. Dans la liste des protocoles, sélectionnez le type de protocole réseau :

   - **Tout**
   - **TCP/UDP** (par défaut)
   - **TCP**
   - **UDP**
   - **ICMP**
   - **ICMPv6**

f. Cliquez sur l'une des options suivantes pour spécifier les ports clients :

   - **Tous les ports** (par défaut)
   - **Plage** : saisissez une plage de ports
   - **Ports spécifiés** : spécifiez des ports individuels. Utilisez une virgule « , » pour séparer les numéros de port.

g. Sous **Ordinateurs**, sélectionnez les adresses IP clientes à inclure dans l'exception. Par exemple, si vous sélectionnez **Refuser tout le trafic réseau (Entrant et Sortant)** et que vous saisissez l'adresse IP d'un client sur le réseau, les clients dont la stratégie contient cette

exception ne pourront pas envoyer de données vers cette adresse IP ou en recevoir à partir de celle-ci. Choisissez l'une des options suivantes :

- **Toutes les adresses IP** (par défaut)
- **IP unique** : saisissez une adresse IPv4 ou IPv6 ou un nom d'hôte. Pour résoudre le nom de l'hôte du client vers une adresse IP, cliquez sur **Résoudre**.
- **Plage IP (pour IPv4 ou IPv6)** : saisissez deux adresses IPv4 ou IPv6 dans les champs **De** et **À**. Il est impossible de saisir une adresse IPv6 dans un champ et une adresse IPv4 dans l'autre.
- **Plage IP (pour IPv6)** : saisissez un préfixe et une longueur d'adresse IPv6.

h. Cliquez sur **Enregistrer**.

8. Pour modifier une exception, cliquez sur **Modifier**, puis modifiez les paramètres dans l'écran qui s'affiche.
9. Pour déplacer une exception vers le haut ou le bas de la liste, sélectionnez-la, puis cliquez sur **Monter** ou **Descendre** jusqu'à atteindre la position de votre choix.
10. Pour supprimer une exception, sélectionnez-la, puis cliquez sur **Supprimer**.

Désactivation du pare-feu sur un groupe d'agents

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.

4. Cliquez sur **Pare-feu** > **Au bureau** ou **Pare-feu** > **Hors du bureau**.

   Un nouvel écran s'affiche.

5. Sélectionnez **Désactiver le pare-feu**.

6. Cliquez sur **Enregistrer**.

Désactivation du pare-feu sur tous les agents

Procédure

1. Accédez à **Administration** > **Paramètres généraux**.

2. Cliquez sur **Poste de travail/serveur**.

3. Sous **Paramètres du pare-feu**, sélectionnez **Désactiver le pare-feu et désinstaller les pilotes**.

4. Cliquez sur **Enregistrer**.

Contrôle des dispositifs

Le contrôle des dispositifs régule l'accès aux périphériques de stockage externes reliés aux terminaisons. Plus spécifiquement, le contrôle des dispositifs restreint l'accès à tous les types de périphériques de stockage qui se connectent via une interface USB, à l'exception des périphériques mobiles et des caméras numériques.

Configuration du contrôle des dispositifs

Procédure

1. Accédez à **Dispositifs**.

2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Cliquez sur **Contrôle des dispositifs**.
5. Mettez à jour les éléments suivants, si nécessaire :
   - **Activer le contrôle des dispositifs**
   - **Activer la prévention d'exécution automatique sur USB**
   - **Autorisations** :définissez des autorisations pour les dispositifs USB et les ressources réseau.

     TABLEAU 5-8. Autorisations du contrôle des dispositifs

PERMISSIONS	FICHIERS PRÉSENTS SUR LE PÉRIPHÉRIQUE	FICHIERS ENTRANTS
Accès complet	Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer, Exécuter	Opérations autorisées : Enregistrer, Déplacer, Copier En d'autres termes, un fichier peut être enregistré, déplacé et copié sur le périphérique.
Aucun accès	Opérations interdites : Toutes les opérations Le dispositif et les fichiers qu'il contient sont visibles par l'utilisateur (par exemple, dans l'Explorateur Windows).	Opérations interdites : Enregistrer, Déplacer, Copier
Lecture	Opérations autorisées : Copier, Ouvrir Opérations interdites : Enregistrer, Déplacer, Supprimer, Exécuter	Opérations interdites : Enregistrer, Déplacer, Copier

Permissions	Fichiers présents sur le périphérique	Fichiers entrants
Modifier	Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer Opérations interdites : Exécuter	Opérations autorisées : Enregistrer, Déplacer, Copier
Lire et exécuter	Opérations autorisées : Copier, Ouvrir, Exécuter Opérations interdites : Enregistrer, Déplacer, Supprimer	Opérations interdites : Enregistrer, Déplacer, Copier

- **Exceptions**:Si un utilisateur ne dispose pas de l'autorisation en lecture pour un dispositif particulier, il est néanmoins autorisé à exécuter ou à ouvrir n'importe quel fichier ou programme de la liste approuvée.

  Toutefois, si la prévention d'exécution automatique est activée, même si un fichier figure dans la liste approuvée, l'exécution restera interdite.

  Pour ajouter une exception à la liste approuvée, saisissez le nom de fichier avec le chemin ou la signature numérique, puis cliquez sur **Ajouter à la liste approuvée**.

6. Cliquez sur **Enregistrer**.

Outils utilisateur

- **Barre d'outils Anti-Spam**: filtre les spams dans Microsoft Outlook, fournit des statistiques et permet de modifier certains paramètres.
- **HouseCall** : Détermine la sécurité d'une connexion sans fil en vérifiant l'authenticité des points d'accès en fonction de la validité de leurs SSID, de leurs méthodes d'authentification et de leurs règles de chiffrement.

Un message contextuel d'alerte s'affiche si une connexion présente un risque.

- **Outil Case Diagnostic Tool** : l'outil Trend Micro Case Diagnostic Tool (CDT) collecte les informations de débogage nécessaires issues du produit d'un client à chaque fois qu'un problème apparaît. Il active ou désactive automatiquement le débogage du produit et collecte les fichiers nécessaires en fonction des catégories de problèmes. Trend Micro utilise ces informations pour résoudre les problèmes liés au produit.

  Cet outil est disponible uniquement sur la console Security Agent.

- **Client Mover** : cet outil permet de transférer des clients d'un serveur vers un autre. La version linguistique et le type des serveurs doivent être identiques.

- **Outil de communication client-serveur** : Utilisez cet outil pour résoudre les problèmes liés à la communication client-serveur.

Configuration des outils utilisateur

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.

4. Cliquez sur **Outils utilisateur**.

   Un nouvel écran s'affiche.

5. Mettez à jour les éléments suivants, si nécessaire :

   - **Évaluation des réseaux Wi-Fi** : vérifie la sécurité des réseaux sans fil en fonction de la validité de leurs SSID, de leurs méthodes d'authentification et de leurs règles de chiffrement.

- **Barre d'outils Anti-spam** : filtre les spams dans Microsoft Outlook.

6. Cliquez sur **Enregistrer**.

Privilèges agent

Accordez des privilèges d'agent pour autoriser les utilisateurs à modifier les paramètres de Security Agent sur le client.

Conseil

Toutefois, pour réguler la stratégie de sécurité dans votre entreprise, Trend Micro vous recommande d'accorder aux utilisateurs des privilèges limités. Ainsi, vous éviterez que les utilisateurs ne modifient les paramètres de scan ou ne déchargent Security Agent.

Configuration des privilèges des agents

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un groupe de postes de travail ou de serveurs.
3. Cliquez sur **Configurer la stratégie**.

   L'écran **Configurer la stratégie : <nom du groupe>** s'affiche.
4. Cliquez sur **Privilèges agent**.
5. Mettez à jour les éléments suivants, si nécessaire :

Section	Privilèges
Antivirus/anti-programme espion	• Paramètres de scan en temps réel • Paramètres de scan manuel • Paramètres de scan programmé • Ignorer le scan programmé
Pare-feu	Paramètres du pare-feu
Réputation de sites Web - Poursuivre la navigation	Affiche un lien qui permet aux utilisateurs de poursuivre la navigation sur une URL malveillante jusqu'au redémarrage de l'ordinateur. Des avertissements continuent de s'afficher pour les autres URL malveillantes.
Filtrage d'URL - Poursuivre la navigation	Affiche un lien qui permet aux utilisateurs de poursuivre la navigation sur une URL restreinte jusqu'au redémarrage de l'ordinateur. Des avertissements continuent de s'afficher pour les autres URL restreintes.
Surveillance des comportements	Permet aux utilisateurs de modifier les paramètres de surveillance des comportements.
Programme sécurisé	Permet aux utilisateurs de modifier la liste des programmes de confiance.
Paramètres de proxy	Permet aux utilisateurs de configurer les paramètres de proxy. **Remarque** Si cette fonction est désactivée, les paramètres de proxy par défaut sont réinitialisés.

Section	Privilèges
Privilèges de mise à jour	• Permet aux utilisateurs d'effectuer des mises à jour • Utiliser ActiveUpdate de Trend Micro en tant que source de mise à jour secondaire • Désactiver le déploiement des correctifs de type hot fix **Remarque** Le déploiement simultané de correctifs de type hot fix, de patchs, de patchs de sécurité ou critiques, ainsi que de Service Packs sur un grand nombre d'agents peut augmenter de manière significative le trafic réseau. Songez à activer cette option sur plusieurs groupes afin d'échelonner le déploiement. L'activation de cette option désactive également les **mises à niveau de compilation** automatiques sur les agents (par exemple, de la compilation bêta vers la compilation commerciale de la version actuelle du produit) mais PAS les **mises à niveau de version** automatiques (par exemple, de la version 7.x à la version actuelle). Pour désactiver les mises à niveau de version automatiques, exécutez le pack d'installation de Security Server et sélectionnez l'option permettant de repousser les mises à niveau.
Client Security	Empêche les utilisateurs ou d'autres processus de modifier les fichiers de programme, les entrées de Registre et les processus Trend Micro.

6. Cliquez sur **Enregistrer**.

Chapitre 6

Gestion des param. sécurité de base des MSA (Advanced uniq.)

Ce chapitre décrit Messaging Security Agent et explique comment définir les options de scan en temps réel, configurer la fonction anti-spam, le filtrage de contenu, le blocage des pièces jointes et les options de maintenance de la mise en quarantaine pour l'agent.

Agents Messaging Security Agent

Les agents Messaging Security Agent protègent les serveurs Microsoft Exchange. L'agent évite la propagation des menaces de messagerie en scannant les e-mails qui transitent par la banque de boîtes aux lettres Microsoft Exchange, ainsi que ceux échangés entre le serveur Microsoft Exchange et les destinations externes. De plus, Messaging Security Agent peut :

- Limiter la quantité de spam
- Bloquer les messages électroniques en fonction de leur contenu
- Bloquer ou restreindre les messages électroniques avec pièces jointes
- Détecter les URL malveillantes dans les e-mails
- Prévenir la fuite de données confidentielles

Informations importantes sur les agents Messaging Security Agent

- Les agents Messaging Security Agent ne peuvent être installés que sur des serveurs Microsoft Exchange.
- Messaging Security Agent ne prend pas en charge certaines fonctionnalités de Microsoft Exchange Server Enterprise, telles que le Groupe de disponibilité de données (DAG).
- L'arborescence des groupes de sécurité de la console Web affiche tous les agents Messaging Security Agent. Il est impossible de combiner plusieurs agents Messaging Security Agent dans un groupe ; chaque agent Messaging Security Agent doit être administré et géré individuellement.
- Worry-Free Business Security utilise Messaging Security Agent pour recueillir des informations de sécurité auprès des serveurs Microsoft Exchange. Par exemple, Messaging Security Agent rapporte les détections de spam et l'exécution des mises à jour des composants au serveur Security Server. Ces informations s'affichent dans la console Web. Security Server utilise également ces informations pour

générer des journaux et des rapports relatifs à l'état de sécurité des serveurs Microsoft Exchange.

Chaque menace détectée génère une entrée de journal/notification. Cela signifie que si Messaging Security Agent détecte plusieurs menaces dans un seul message électronique, il génère plusieurs entrées de journal et notifications. Il peut aussi exister des cas dans lesquels la même menace est détectée plusieurs fois, surtout si vous utilisez le mode cache dans Outlook 2003. Lorsque le mode cache est activé, il se peut que la même menace soit détectée à la fois dans le dossier d'éléments en file d'attente et le dossier d'éléments envoyés ou dans le dossier d'envoi.

- Messaging Security Agent utilise une base de données SQL Server pour les ordinateurs exécutant Microsoft Exchange Server 2007. Pour éviter tout problème, les services Messaging Security Agent sont conçus de façon à dépendre de l'instance `MSSQL$SCANMAIL` du service SQL Server. Dès que cette instance est interrompue ou redémarrée, les services Messaging Security Agent suivants sont également arrêtés :

  - `ScanMail_Master`
  - `ScanMail_RemoteConfig`

  Redémarrez manuellement ces services si `MSSQL$SCANMAIL` est arrêté ou redémarré. Différents événements, y compris lors de la mise à jour de SQL Server, peuvent amener `MSSQL$SCANMAIL` à redémarrer ou à s'arrêter.

Scan des messages électroniques par Messaging Security Agent

Messaging Security Agent utilise la séquence suivante pour scanner les e-mails :

1. Recherche de spam (anti-spam)

   a. Compare l'e-mail à la liste des expéditeurs approuvés/bloqués de l'administrateur

b. Recherche les événements de phishing

c. Compare le message électronique à la liste d'exceptions fournie par Trend Micro

d. Compare le message électronique à la base de données de signatures de spam

e. Applique les règles de scan heuristique

2. Recherche les violations de règles de filtrage de contenu
3. Scanne les pièces jointes qui dépassent les paramètres de scan définis par l'utilisateur
4. Recherche de virus/programmes malveillants (antivirus)
5. Recherche les URL malveillantes

Paramètres par défaut de Messaging Security Agent

Consultez les options répertoriées dans le tableau, qui vous aideront à optimiser les configurations de Messaging Security Agent.

TABLEAU 6-1. Actions par défaut de Trend Micro pour Messaging Security Agent

OPTIONS DE SCAN	SCAN EN TEMPS RÉEL	SCANS MANUEL ET PROGRAMMÉ
Anti-spam		
Spam	Mise en quarantaine du message dans le dossier de spam de l'utilisateur (par défaut, si le courrier indésirable d'Outlook ou End User Quarantine est installé)	Non applicable
Phishing	Supprimer la totalité du message	Non applicable
Filtrage de contenu		

Options de scan	Scan en temps réel	Scans manuel et programmé
Filtrer les messages correspondant à une condition définie	Mettre la totalité du message en quarantaine	Remplacer
Filtrer les messages correspondant à toutes les conditions définies	Mettre la totalité du message en quarantaine	Non applicable
Surveiller le contenu des messages provenant de comptes de messagerie particuliers	Mettre la totalité du message en quarantaine	Remplacer
Créer une exception pour des comptes de messagerie particuliers	Ignorer	Ignorer
Blocage des pièces jointes		
Action	Remplacer la pièce jointe par un texte/fichier	Remplacer la pièce jointe par un texte/fichier
Autre		
Fichiers chiffrés et protégés par un mot de passe	Ignorer (Lorsque vous sélectionnez « Ignorer » pour définir l'action, les fichiers chiffrés et protégés par mot de passe sont transmis et l'événement n'est pas enregistré.)	Ignorer (Lorsque vous sélectionnez « Ignorer » pour définir l'action, les fichiers chiffrés et protégés par mot de passe sont transmis et l'événement n'est pas enregistré.)
Fichiers exclus (fichiers dépassant les restrictions de scan spécifiées)	Ignorer (Lorsque vous sélectionnez « Ignorer » pour définir l'action, les fichiers ou les corps de message dépassant les restrictions de scan spécifiées sont ignorés et l'événement n'est pas enregistré.)	Ignorer (Lorsque vous sélectionnez « Ignorer » pour définir l'action, les fichiers ou les corps de message dépassant les restrictions de scan spécifiées sont ignorés et l'événement n'est pas enregistré.)

Scan en temps réel pour les agents Messaging Security Agent

Le scan en temps réel s'effectue en continu. Le scan en temps réel de **Messaging Security Agent** (Advanced uniquement) surveille tous les points d'entrée de virus connus en scannant tous les messages entrants, les messages SMTP, les documents publiés dans des dossiers publics et des fichiers répliqués à partir d'autres serveurs Microsoft Exchange.

Configuration du scan en temps réel pour des agents Messaging Security Agent

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.
4. Cliquez sur **Antivirus**.

   Un nouvel écran s'affiche.
5. Sélectionnez **Activer le scan antivirus en temps réel**.
6. Configurez les paramètres de scan. Pour plus de détails, voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*.
7. Cliquez sur **Enregistrer**.

   Configurez les destinataires des notifications lorsqu'un événement se produit. Voir *Configuration d'événements pour les notifications à la page 10-4*.

Anti-Spam

Worry-Free Business Security propose deux façons de lutter contre le spam : la **réputation de messagerie** et le **scan de contenu**.

Messaging Security Agent utilise les composants suivants pour détecter la présence de spams ou d'incidents de phishing dans les courriers électroniques :

- Moteur Trend Micro Anti-Spam
- Fichiers de signatures de spam de Trend Micro

Trend Micro met fréquemment à jour le moteur et les fichiers de signatures et les rend accessibles au téléchargement. Security Server peut télécharger ces composants grâce à une mise à jour manuelle ou programmée.

Le moteur anti-spam utilise les signatures de messages de spam et les règles heuristiques pour filtrer les messages électroniques. Il scanne les messages électroniques et affecte un score de spam à chacun d'entre eux en fonction de leur correspondance aux règles et signatures des fichiers de signatures. Messaging Security Agent compare le score de spam au niveau de détection de messages de spam défini par l'utilisateur. Lorsque le score de spam dépasse le niveau de détection, l'agent entreprend une action contre le message de spam.

Par exemple : les spammers utilisent de nombreux points d'exclamation ou des séries de points d'exclamation (!!!!) dans leurs messages électroniques. Lorsque Messaging Security Agent détecte un message utilisant les points d'exclamation de la sorte, le score de spam augmente pour ce message électronique.

Conseil

Outre la fonction d'anti-spam, vous pouvez configurer l'option Filtrage de contenu de façon à ce qu'elle filtre l'en-tête, l'objet et le corps des messages, ainsi que les informations relatives aux pièces jointes afin de bloquer les spams et tout autre contenu indésirable.

Les utilisateurs ne peuvent pas modifier la méthode utilisée par le moteur anti-spam pour affecter des scores de spam. Ils peuvent par contre régler les

niveaux de détection utilisés par Messaging Security Agent pour juger de la nature d'un message et déterminer s'il s'agit d'un message de spam ou non.

Remarque

Il se peut que Microsoft Outlook filtre et envoie automatiquement les messages identifiés par Messaging Security Agent comme spam vers son dossier de courrier indésirable.

Évaluation de la réputation de messagerie

La technologie d'évaluation de la réputation de messagerie détermine le spam en fonction de la réputation du MTA d'origine. Cela permet de décharger Security Server de la tâche. Lorsque l'évaluation de la réputation de messagerie est activée, l'ensemble du trafic SMTP entrant est vérifié par les bases de données IP pour vérifier si l'adresse IP d'origine est saine ou si elle a été désignée comme vecteur de spam connu.

L'évaluation de la réputation de messagerie propose les deux niveaux de service. suivants :

- **Standard** : le service standard utilise une base de données pour évaluer la réputation d'environ deux millions d'adresses IP. Les adresses IP ayant été correctement associées à la remise de messages de spam sont ajoutées à la base de données et rarement supprimées.
- **Avancé** : le service avancé est un service DNS reposant sur des demandes, comme le service standard. La clé de voûte de ce service est la base de données de réputation standard, associée à la base de données de réputation dynamique, en temps réel, qui bloque les messages des sources de spam connues et suspectes.

Lorsqu'un message électronique provenant d'une adresse IP bloquée ou suspecte est détecté, la réputation de messagerie le bloque avant qu'il n'atteigne votre passerelle.

Configuration de l'évaluation de la réputation de messagerie

Configurez l'évaluation de la réputation de messagerie pour bloquer les messages provenant de sources de spam connues ou suspectes. De même,

créez des exclusions pour autoriser ou bloquer les messages provenant d'autres expéditeurs.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.
4. Cliquez sur **Anti-spam** > **Réputation de messagerie**.

   Un nouvel écran s'affiche.
5. Sous l'onglet **Cible**, mettez à jour les éléments suivants si nécessaire :
   - **Activer l'anti-spam en temps réel (réputation de messagerie)**
   - **Niveau de service** :
     - **Standard**
     - **Avancé**
   - **Adresses IP approuvées** : les messages électroniques provenant de ces adresses IP ne seront jamais bloqués. Tapez l'adresse IP à approuver et cliquez sur **Ajouter**. Si nécessaire, vous pouvez importer une liste d'adresses à partir d'un fichier texte. Pour supprimer une adresse IP, sélectionnez l'adresse et cliquez sur **Supprimer**.
   - **Adresses IP bloquées** : les messages électroniques provenant de ces adresses IP seront toujours bloqués. Tapez l'adresse IP à bloquer et cliquez sur **Ajouter**. Si nécessaire, vous pouvez importer une liste d'adresses à partir d'un fichier texte. Pour supprimer une adresse IP, sélectionnez l'adresse et cliquez sur **Supprimer**.
6. Cliquez sur **Enregistrer**.

7. Accédez à : http://ers.trendmicro.com/ pour consulter les rapports.

Remarque

la réputation de messagerie est un service Web. Les administrateurs peuvent uniquement configurer le niveau de service à partir de la console Web.

Scan de contenu

Le scan de contenu identifie le spam en fonction du contenu du message plutôt que de son adresse IP d'origine. Messaging Security Agent utilise le les fichiers de signatures de anti-spam et le moteur Trend Micro Anti-Spam pour détecter la présence de spam dans chaque message électronique avant de le transmettre à la banque d'informations. Le serveur Microsoft Exchange ne traite pas les spams rejetés et ces messages ne parviennent donc pas jusqu'aux boîtes aux lettres des utilisateurs.

Remarque

Ne confondez pas le scan de contenu (anti-spam fondé sur l'utilisation de fichiers de signatures et des techniques heuristiques) et le filtrage de contenu (scan et blocage des courriers électroniques basés sur des mots-clés classés). Voir *Filtrage de contenu à la page 6-16*.

Configuration du scan de contenu

Messaging Security Agent détecte les messages de spam en **temps réel** et prend des mesures pour protéger les serveurs Microsoft Exchange.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

Un nouvel écran s'affiche.

4. Cliquez sur **Anti-spam** > **Scan de contenu**.

   Un nouvel écran s'affiche.

5. Sélectionnez **Activer l'anti-spam en temps réel**.

6. Sélectionnez l'onglet **Cible** pour sélectionner la méthode et le taux de détection du spam devant être utilisés par Messaging Security Agent pour filtrer le spam :

   a. Sélectionnez le niveau de détection, **faible**, **moyen** ou **élevé**, dans la liste des taux de détection de spams. Messaging Security Agent utilise ce taux pour filtrer tous les messages.

      - **Élevé**: niveau de détection de spams le plus rigoureux. Messaging Security Agent contrôle tous les messages électroniques pour savoir s'ils contiennent des fichiers ou des textes suspects. Les risques de détection de faux-positifs ne sont pas exclus. Les faux-positifs sont les messages électroniques que Messaging Security Agent identifie en tant que messages de spam alors qu'ils sont en réalité des messages électroniques légitimes.

      - **Moyen** : paramètre par défaut (recommandé). Messaging Security Agent applique à un niveau élevé de détection des spams. Les risques de filtrage de faux-positifs sont modérés.

      - **Faible** : niveau de détection de spams le moins sensible. Messaging Security Agent ne filtre que les spams les plus évidents et les plus communs, mais il est peu probable qu'il filtre les faux positifs. Filtrage par score de spam.

   b. Cliquez sur **Détecter les incidents de phishing** pour demander à Messaging Security Agent de rechercher des incidents de phishing. Pour plus de détails, voir *Incidents de type phishing à la page 1-13*.

   c. Ajoutez les adresses à votre liste d'expéditeurs approuvés et d'expéditeurs bloqués. Pour plus de détails, voir *Listes des expéditeurs approuvés et des expéditeurs bloqués à la page 6-13*.

- **Expéditeurs approuvés** : les messages électroniques provenant de ces adresses ou noms de domaines ne seront jamais bloqués. Tapez les adresses ou noms de domaines à approuver et cliquez sur **Ajouter**. Si nécessaire, vous pouvez importer une liste d'adresses ou de noms de domaines à partir d'un fichier texte. Pour supprimer des adresses ou noms de domaines, sélectionnez-les et cliquez sur **Supprimer**.
- **Expéditeurs bloqués** : les messages électroniques provenant de ces adresses ou noms de domaines seront toujours bloqués. Tapez les adresses ou noms de domaines à bloquer et cliquez sur **Ajouter**. Si nécessaire, vous pouvez importer une liste d'adresses ou de noms de domaines à partir d'un fichier texte. Pour supprimer des adresses ou noms de domaines, sélectionnez-les et cliquez sur **Supprimer**.

Remarque

l'administrateur Microsoft Exchange dispose d'une liste séparée d'expéditeurs approuvés et bloqués pour le serveur Microsoft Exchange. Si un utilisateur final crée un expéditeur approuvé, mais que cet expéditeur se trouve sur la liste des expéditeurs bloqués de l'administrateur, Messaging Security Agent identifie les messages venant de cet expéditeur bloqué en tant que spam et prend les mesures appropriées à l'encontre de ces messages.

7. Cliquez sur l'onglet **Action** pour définir les mesures prises par Messaging Security Agent lorsqu'il détecte un message de spam ou un incident de phishing.

Remarque

Pour plus d'informations sur les actions, voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*.

Messaging Security Agent prend l'une des mesures suivantes en fonction de votre configuration :

- **Mise en quarantaine du message dans le dossier spam côté serveur**

- **Mise en quarantaine du message dans le dossier spam de l'utilisateur**

  Remarque

  Si vous sélectionnez cette action, configurez End User Quarantine. Pour plus de détails, voir *Configuration de la maintenance des spams à la page 6-76*.

- **Supprimer la totalité du message**
- **Marquer et envoyer**

8. Cliquez sur **Enregistrer**.

Listes des expéditeurs approuvés et des expéditeurs bloqués

La liste d'expéditeurs approuvés est une liste d'adresses considérées sans danger. Messaging Security Agent ne recherche pas la présence éventuelle de spams dans les messages qui proviennent de ces adresses, sauf lorsque l'option **Détecter les incidents de phishing** est activée. Lorsque la fonction **Détecter les incidents de phishing** est activée et que l'agent détecte un incident de phishing dans un e-mail, celui-ci n'est pas transmis, même s'il figure dans une liste d'expéditeurs approuvés. Une liste d'expéditeurs bloqués est une liste d'adresses considérées suspectes. L'agent considère systématiquement les e-mails provenant d'expéditeurs bloqués comme des spams et prend les mesures appropriées.

Il existe deux listes d'expéditeurs approuvés : l'une pour l'administrateur Microsoft Exchange et l'autre pour les utilisateurs finaux.

- Les listes d'expéditeurs approuvés et bloqués de l'administrateur Microsoft Exchange (de l'écran **Anti-spam**) contrôlent la façon dont Messaging Security Agent traite les messages électroniques acheminés vers le serveur Microsoft Exchange.
- L'utilisateur final gère le dossier de spam créé pour ces messages au cours de l'installation. Les listes des utilisateurs finaux n'affectent que les messages à destination de la boîte aux lettres côté serveur de chaque utilisateur individuel.

Directives générales

- Les listes d'expéditeurs approuvés et bloqués d'un serveur Microsoft Exchange remplacent les listes d'expéditeurs approuvés et bloqués d'un client. Par exemple, l'expéditeur « utilisateur@exemple.com » figure dans la liste d'expéditeurs bloqués de l'administrateur, mais l'utilisateur final a ajouté cette adresse à sa liste d'expéditeurs approuvés. Les messages provenant de cet expéditeur accèdent à la banque d'informations Microsoft Exchange et Messaging Security Agent les identifie en tant que spam et exécute l'action nécessaire. Si l'agent exécute l'action de mise en quarantaine dans le dossier de spam de l'utilisateur, il tente de transférer le message vers le dossier de spam de l'utilisateur final, mais le message est finalement redirigé vers la boîte de réception de l'utilisateur final, car celui-ci a approuvé cet expéditeur.
- si vous utilisez Outlook, il existe une limite de taille concernant la quantité et la taille des adresses de la liste. Afin d'éviter une erreur système, Messaging Security Agent limite le nombre d'adresses que l'utilisateur peut répertorier dans sa liste d'expéditeurs approuvés (cette limite est calculée selon la longueur des adresses électroniques et leur quantité).

Recherche par caractère de substitution

Messaging Security Agent prend en charge la recherche par caractère de substitution pour les listes d'expéditeurs approuvés et bloqués. Le programme utilise l'astérisque (*) comme caractère de substitution.

Messaging Security Agent ne prend pas en charge la recherche par caractère de substitution au niveau de la partie de l'adresse correspondant au nom d'utilisateur. Cependant, si vous saisissez un modèle tel que « *@trend.com », l'agent le considère de la même façon que « @trend.com ».

Vous ne pouvez utiliser un caractère de substitution que lorsqu'il se trouve :

- En regard d'un seul point et qu'il s'agit du premier ou dernier caractère d'une chaîne
- À gauche d'un signe @ et qu'il s'agit du premier caractère de la chaîne
- Toute section manquante au début ou à la fin de la chaîne donne le même résultat qu'un caractère de substitution

TABLEAU 6-2. Correspondances d'adresses électroniques pour les caractères de substitution

MODÈLE	EXEMPLES CORRESPONDANTS	EXEMPLES NON CORRESPONDANTS
jean@exemple.com	jean@exemple.com	Toute adresse ne correspondant pas à ce modèle.
@exemple.com *@exemple.com	jean@exemple.com marie@exemple.com	jean@ms1.exemple.com jean@exemple.com.us marie@exemple.com.us
exemple.com	jean@exemple.com jean@ms1.exemple.com marie@ms1.rd.exemple.com marie@exemple.com	jean@exemple.com.us marie@monexemple.com.us joseph@exemple.comon
*.exemple.com	jean@ms1.exemple.com marie@ms1.rd.exemple.com joseph@ms1.exemple.com	jean@exemple.com jean@monexemple.com.us marie@ms1.exemple.comon
exemple.com.*	jean@exemple.com.us jean@ms1.exemple.com.us jean@ms1.rd.exemple.com.us marie@exemple.com.us	jean@exemple.com marie@ms1.exemple.com jean@monexemple.com.us
.exemple.com.	jean@ms1.exemple.com.us jean@ms1.rd.exemple.com.us marie@ms1.exemple.com.us	jean@exemple.com jean@ms1.exemple.com jean@trend.exemple.us
..*.exemple.com *****.exemple.com	Même chose que pour « *.exemple.com »	

Modèle	Exemples correspondants	Exemples non correspondants
exemple.com exemple.com exemple.*.com @*.exemple.com	Modèles non valides	

Filtrage de contenu

La fonction de filtrage de contenu évalue les messages électroniques entrants et sortants en fonction de règles définies par l'utilisateur. Chaque règle contient une liste de mots-clés et d'expressions. Le filtrage de contenu évalue l'en-tête et/ou le contenu des messages en les comparant à la liste de mots-clés. Lorsque le filtrage de contenu détecte un mot qui correspond à un mot clé, il peut empêcher la transmission du contenu indésirable aux clients Microsoft Exchange. Messaging Security Agent peut envoyer des notifications lorsqu'il entreprend une action contre du contenu indésirable.

Remarque

Ne confondez pas le scan de contenu (anti-spam fondé sur l'utilisation de fichiers de signatures et des techniques heuristiques) et le filtrage de contenu (scan et blocage des courriers électroniques basés sur des mots-clés classés). Voir *Scan de contenu à la page 6-10*.

Le filtre de contenu constitue pour l'administrateur un moyen d'analyser et de contrôler le trafic des messages électroniques en fonction du texte du message. Il peut servir à surveiller les messages entrants et sortants pour s'assurer qu'ils ne contiennent aucun propos à caractère sexuel (harcèlement), injurieux ou choquant. Le filtre de contenu propose par ailleurs une fonction de vérification des synonymes qui permet d'étendre la portée de vos règles de filtrage. À titre d'exemple, vous pouvez créer des règles de filtrage pour contrôler :

- Les propos relevant du harcèlement sexuel
- Les propos racistes
- Les spams intégrés dans le corps d'un message électronique

Remarque

Par défaut, le filtrage de contenu n'est pas activé.

Gestion des règles de filtrage de contenu

Messaging Security Agent affiche toutes les règles de filtrage de contenu sur l'écran **Filtrage de contenu**. Pour afficher cet écran, accédez à :

- Pour le scan en temps réel :

  Dispositifs > **{Agent Messaging Security Agent}** > **Configurer la stratégie** > **Filtrage de contenu**

- Pour le scan manuel :

  Scans > **Manuel** > **{Développer l'agent Messaging Security Agent}** > **Filtrage de contenu**

- Pour le scan programmé :

  Scans > **Programmé** > **{Développer l'agent Messaging Security Agent}** > **Filtrage de contenu**

Procédure

1. Cet écran affiche un résumé des informations relatives aux règles, comprenant :
   - **Règle** : Worry-Free Business Security propose des règles par défaut qui permettent de filtrer du contenu selon les catégories suivantes : **insultes**, **discrimination raciale**, **discrimination sexuelle**, **canulars** et **chaîne de messages**. Ces règles sont désactivées par défaut. Vous pouvez les adapter à vos besoins ou les supprimer. Si aucune de ces règles ne vous est utile, ajoutez vos propres règles.

- **Action** : l'agent Messaging Security Agent exécute cette action lorsqu'il détecte un contenu indésirable.
- **Priorité** : l'agent Messaging Security Agent applique successivement chaque filtre selon l'ordre indiqué sur cette page.
- **Activé** : l'icône verte désigne une règle activée et l'icône rouge une règle désactivée.

2. Effectuez les actions suivantes :

TÂCHE	ÉTAPES
Activer/Désactiver le filtrage de contenu	Cochez ou décochez la case **Activer le filtrage de contenu en temps réel** située en haut de la page.
Ajouter une règle	Cliquez sur **Ajouter**. Dans la nouvelle fenêtre qui s'ouvre, vous pouvez choisir le type de règle à ajouter. Pour plus d'informations, voir *Types de règles de filtrage de contenu à la page 6-21*.

TÂCHE	ÉTAPES
Modifier une règle	a. Cliquez sur le nom de la règle à modifier. Un nouvel écran s'affiche. b. Les options disponibles dépendent du type de règle choisi. Pour choisir un type de règle, identifiez le deuxième élément du chemin de navigation situé en haut de l'écran. Par exemple : Filtrage de contenu > **Faire correspondre la règle d'une condition** > Modifier la règle Pour en savoir plus sur les paramètres de règle que vous pouvez modifier, reportez-vous aux rubriques suivantes : • *Ajout d'une règle de filtrage de contenu pour n'importe quelle condition de correspondance à la page 6-25* • *Ajout d'une règle de filtrage de contenu pour toutes les conditions de correspondance à la page 6-22* **Remarque** Ce type de règle n'est pas disponible pour les scans de filtrage de contenu manuels et programmés. • *Ajout d'une règle de surveillance du filtrage de contenu à la page 6-28* • *Création d'exceptions aux règles de filtrage de contenu à la page 6-32*

TÂCHE	ÉTAPES
Réorganiser les règles	Messaging Security Agent applique les règles de filtrage de contenu aux courriers électroniques dans l'ordre dans lequel elles apparaissent sur l'écran **Filtrage de contenu**. Configurez l'ordre selon lequel les règles s'appliquent. L'agent filtre tous les messages électroniques en fonction de chaque règle jusqu'à ce qu'une violation de contenu déclenche une action qui empêche de continuer le scan (par exemple, Supprimer ou Quarantaine). Modifiez l'ordre de ces règles afin d'optimiser le filtrage de contenu. a. Cochez la case correspondant à la règle dont vous souhaitez modifier le numéro d'ordre. b. Cliquez sur **Réorganiser**. Un encadré s'affiche autour du numéro d'ordre de la règle. c. Dans la case de la colonne **Priorité**, supprimez le numéro d'ordre existant et entrez-en un nouveau. **Remarque** Veillez à ne pas entrer un numéro supérieur au nombre total de règles de la liste. Si vous entrez un numéro supérieur au nombre total de règles, Worry-Free Business Security l'ignore et ne modifie pas le numéro d'ordre de la règle. d. Cliquez sur **Enregistrer la réorganisation**. La règle est déplacée vers le niveau de priorité entré et tous les autres numéros d'ordre des règles sont modifiés en conséquence. Par exemple, si vous sélectionnez le numéro d'ordre 5 et que vous le remplacez par 3, les numéros d'ordre 1 et 2 ne changent pas, tandis que le numéro 3 et les numéros supérieurs augmentent d'une unité.
Activer/Désactiver des règles	Cliquez sur l'icône dans la colonne Activé.

TÂCHE	ÉTAPES
Supprimer des règles	Lorsque vous supprimez une règle, Messaging Security Agent met à jour l'ordre des autres règles afin d'indiquer les modifications. **Remarque** la suppression d'une règle est irréversible. Il est préférable de désactiver une règle plutôt que de la supprimer. a. Sélectionnez une règle. b. Cliquez sur **Supprimer**.

3. Cliquez sur **Enregistrer**.

Types de règles de filtrage de contenu

Vous pouvez créer des règles pour filtrer les messages électroniques en fonction de conditions que vous spécifiez ou selon l'adresse électronique de l'expéditeur ou du destinataire. Les conditions que vous pouvez spécifier pour la règle comprennent : quels champs d'en-tête doivent être scannés, si le corps d'un message électronique doit être scanné ou non et quels mots-clés rechercher.

Vous pouvez créer des règles capables de :

- **Filtrer les messages correspondant à une condition définie** : ce type de règle est capable de filtrer le contenu de tout message au cours d'un scan. Pour plus de détails, voir *Ajout d'une règle de filtrage de contenu pour n'importe quelle condition de correspondance à la page 6-25*.
- **Filtrer les messages correspondant à toutes les conditions définies** : ce type de règle est capable de filtrer le contenu de tout message au cours d'un scan. Pour plus de détails, voir *Ajout d'une règle de filtrage de contenu pour toutes les conditions de correspondance à la page 6-22*.

Remarque

Ce type de règle n'est pas disponible pour les scans de filtrage de contenu manuels et programmés.

- **Surveiller le contenu des messages provenant de comptes de messagerie particuliers** : ce type de règle surveille le contenu des messages provenant de comptes de messagerie particuliers. Les règles de surveillance sont similaires à des règles générales de filtrage de contenu, sauf qu'elles ne filtrent que le contenu provenant de comptes de messagerie spécifiés. Pour plus de détails, voir *Ajout d'une règle de surveillance du filtrage de contenu à la page 6-28*.
- **Créer des exceptions pour des comptes de messagerie particuliers** : ce type de règles crée une exception pour des comptes de messagerie particuliers. Lorsque vous excluez un compte de messagerie particulier, ce compte n'est pas filtré pour y détecter des violations de règles de contenu. Pour plus de détails, voir *Création d'exceptions aux règles de filtrage de contenu à la page 6-32*.

Une fois votre règle créée, Messaging Security Agent commence à filtrer tous les messages entrants et sortants en fonction de votre règle. En cas de violation de contenu, Messaging Security Agent entreprend une action adéquate. L'action entreprise par Security Server dépend également des actions spécifiées pour la règle.

Ajout d'une règle de filtrage de contenu pour toutes les conditions de correspondance

Ce type de règle n'est pas disponible pour les scans de filtrage de contenu manuels et programmés.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.

3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Filtrage de contenu**.

   Un nouvel écran s'affiche.

5. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

6. Sélectionnez **Filtrer les messages correspondant à toutes les conditions définies**.

7. Cliquez sur **Suivant**.

8. Saisissez le nom de votre règle dans le champ **Nom de la règle**.

9. Sélectionnez la partie du message à filtrer pour détecter un éventuel contenu indésirable. Messaging Security Agent peut filtrer les e-mails par :

   - En-tête (From, To et Cc)
   - Objet
   - Taille du corps du message ou de la pièce jointe
   - Nom du fichier joint

   Remarque

   Messaging Security Agent prend uniquement en charge le filtrage de contenu des en-têtes et objets au cours d'un scan en temps réel.

10. Cliquez sur **Suivant**.

11. Sélectionnez une action que Messaging Security Agent doit effectuer lorsqu'il détecte un contenu indésirable. Messaging Security Agent peut exécuter les actions suivantes (pour des descriptions, voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*) :

- Remplacer par un texte/fichier

  Remarque

  Vous ne pouvez pas remplacer le texte des champs De, À, Cc ou Objet.

- Mettre la totalité du message en quarantaine
- Mettre en quarantaine une partie du message
- Supprimer la totalité du message
- Archivage
- Ignorer la totalité du message

12. Sélectionnez **Notifier les destinaires** pour que Messaging Security Agent avertisse les destinataires prévus des messages électroniques dont le contenu a été filtré.

    Sélectionnez **Ne pas notifier les destinataires externes** pour envoyer les notifications aux destinataires internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

13. Sélectionnez **Notifier les expéditeurs** pour que Messaging Security Agent avertisse les expéditeurs des messages électroniques dont le contenu a été filtré.

    Sélectionnez **Ne pas notifier les expéditeurs externes** pour envoyer les notifications aux expéditeurs internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

14. Dans la section **Options avancées**, cliquez sur l'icône plus (+) pour développer la sous-section **Configuration d'archive**.

    a. Dans le champ **Répertoire de quarantaine**, saisissez le chemin d'accès au dossier dans lequel la fonction de filtrage de contenu doit placer les e-mails mis en quarantaine ou acceptez la valeur par défaut : `<Dossier d'installation de Messaging Security Agent>\storage\quarantine`

b. Dans le champ **Répertoire d'archivage**, saisissez le chemin d'accès au dossier dans lequel la fonction de filtrage de contenu doit placer les e-mails archivés ou acceptez la valeur par défaut : `<Dossier d'installation de Messaging Security Agent>\storage \sauvegarde du filtrage de contenu`

15. Cliquez sur l'icône plus (+) pour développer la sous-section **Paramètres de remplacement**.

    a. Dans le champ **Nom du fichier de remplacement**, saisissez le nom du fichier que la fonction de filtrage de contenu doit utiliser pour remplacer un e-mail lorsqu'une règle utilisant l'action « Remplacer par un texte/fichier » est déclenchée ou acceptez la valeur par défaut :

    b. Dans le champ **Texte de remplacement**, saisissez ou collez le contenu du texte de remplacement que la fonction de filtrage du contenu doit utiliser lorsqu'un e-mail déclenche une règle dont l'action est « Remplacer par un texte/fichier » ou acceptez le texte par défaut :

16. Cliquez sur **Terminer**.

    L'assistant se ferme et l'écran Filtrage de contenu s'affiche.

Ajout d'une règle de filtrage de contenu pour n'importe quelle condition de correspondance

- Pour le scan en temps réel :

  Dispositifs > **{Agent Messaging Security Agent}** > **Configurer la stratégie** > **Filtrage de contenu**

- Pour le scan manuel :

  Scans > **Manuel** > **{Développer l'agent Messaging Security Agent}** > **Filtrage de contenu**

- Pour le scan programmé :

Scans > **Programmé** > **{Développer l'agent Messaging Security Agent}** > **Filtrage de contenu**

Procédure

1. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

2. Sélectionnez **Filtrer les messages correspondant à une condition définie**.

3. Cliquez sur **Suivant**.

4. Saisissez le nom de votre règle dans le champ **Nom de la règle**.

5. Sélectionnez la partie du message à filtrer pour détecter un éventuel contenu indésirable. Messaging Security Agent peut filtrer les e-mails par :

   - En-tête (From, To et Cc)
   - Objet
   - Corps
   - Pièce jointe

   Remarque

   Messaging Security Agent prend uniquement en charge le filtrage de contenu des en-têtes et objets au cours d'un scan en temps réel.

6. Cliquez sur **Suivant**.

7. Ajoutez des mots-clés pour la portion cible dont vous souhaitez filtrer le contenu indésirable. Pour plus de détails sur l'utilisation de mots-clés, voir *Mots-clés à la page D-5*.

   a. Le cas échéant, indiquez si le filtre de contenu doit prendre en compte les majuscules et les minuscules.

b. Importez de nouveaux fichiers de mots-clés à partir d'un fichier `.txt` si nécessaire.

c. Définissez une liste de synonymes.

8. Cliquez sur **Suivant**.

9. Sélectionnez une action que Messaging Security Agent doit effectuer lorsqu'il détecte un contenu indésirable. Messaging Security Agent peut exécuter les actions suivantes (pour des descriptions, voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*) :

   - Remplacer par un texte/fichier

     Remarque

     Vous ne pouvez pas remplacer le texte des champs De, À, Cc ou Objet.

   - Mettre la totalité du message en quarantaine
   - Mettre en quarantaine une partie du message
   - Supprimer la totalité du message
   - Archivage

10. Sélectionnez **Notifier les destinaires** pour que Messaging Security Agent avertisse les destinataires prévus des messages électroniques dont le contenu a été filtré.

    Sélectionnez **Ne pas notifier les destinataires externes** pour envoyer les notifications aux destinataires internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

11. Sélectionnez **Notifier les expéditeurs** pour que Messaging Security Agent avertisse les expéditeurs des messages électroniques dont le contenu a été filtré.

    Sélectionnez **Ne pas notifier les expéditeurs externes** pour envoyer les notifications aux expéditeurs internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

12. Dans la section **Options avancées**, cliquez sur l'icône plus (+) pour développer la sous-section **Configuration d'archive**.

    a. Dans le champ **Répertoire de quarantaine**, saisissez le chemin d'accès au dossier dans lequel la fonction de filtrage de contenu doit placer les e-mails mis en quarantaine ou acceptez la valeur par défaut : `<Dossier d'installation de Messaging Security Agent>\storage\quarantine`

    b. Dans le champ **Répertoire d'archivage**, saisissez le chemin d'accès au dossier dans lequel la fonction de filtrage de contenu doit placer les e-mails archivés ou acceptez la valeur par défaut : `<Dossier d'installation de Messaging Security Agent>\storage\sauvegarde du filtrage de contenu`

13. Cliquez sur l'icône plus (+) pour développer la sous-section **Paramètres de remplacement**.

    a. Dans le champ **Nom du fichier de remplacement**, saisissez le nom du fichier que la fonction de filtrage de contenu doit utiliser pour remplacer un e-mail lorsqu'une règle utilisant l'action « Remplacer par un texte/fichier » est déclenchée ou acceptez la valeur par défaut :

    b. Dans le champ **Texte de remplacement**, saisissez ou collez le contenu du texte de remplacement que la fonction de filtrage du contenu doit utiliser lorsqu'un e-mail déclenche une règle dont l'action est « Remplacer par un texte/fichier » ou acceptez le texte par défaut :

14. Cliquez sur **Terminer**.

    L'assistant se ferme et l'écran Filtrage de contenu s'affiche.

Ajout d'une règle de surveillance du filtrage de contenu

- Pour le scan en temps réel :

  Dispositifs > **{Agent Messaging Security Agent}** > **Configurer la stratégie** > **Filtrage de contenu**

- Pour le scan manuel :

  Scans > **Manuel** > **{Développer l'agent Messaging Security Agent}** > **Filtrage de contenu**

- Pour le scan programmé :

  Scans > **Programmé** > **{Développer l'agent Messaging Security Agent}** > **Filtrage de contenu**

Procédure

1. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

2. Sélectionnez **Surveiller le contenu des messages provenant de comptes de messagerie particuliers**.

3. Cliquez sur **Suivant**.

4. Saisissez le nom de votre règle dans le champ **Nom de la règle**.

5. Définissez les comptes de messagerie à surveiller.

6. Cliquez sur **Suivant**.

7. Sélectionnez la partie du message à filtrer pour détecter un éventuel contenu indésirable. Messaging Security Agent peut filtrer les e-mails par :

   - Objet
   - Corps
   - Pièce jointe

   Remarque

   Messaging Security Agent prend uniquement en charge le filtrage de ces éléments d'un message au cours d'un scan en temps réel. Il ne prend pas en charge le filtrage de contenu des en-têtes et objets au cours de scans manuels et programmés.

8. Ajoutez des mots-clés pour la portion cible dont vous souhaitez filtrer le contenu indésirable. Pour plus de détails sur l'utilisation de mots-clés, voir *Mots-clés à la page D-5*.

   a. Le cas échéant, indiquez si le filtre de contenu doit prendre en compte les majuscules et les minuscules.

   b. Importez de nouveaux fichiers de mots-clés à partir d'un fichier `.txt` si nécessaire.

   c. Définissez une liste de synonymes.

9. Cliquez sur **Suivant**.

10. Sélectionnez une action que Messaging Security Agent doit effectuer lorsqu'il détecte un contenu indésirable. Messaging Security Agent peut exécuter les actions suivantes (pour des descriptions, voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*) :

    - Remplacer par un texte/fichier

      Remarque

      Vous ne pouvez pas remplacer le texte des champs De, À, Cc ou Objet.

    - Mettre la totalité du message en quarantaine
    - Mettre en quarantaine une partie du message
    - Supprimer la totalité du message
    - Archivage

11. Sélectionnez **Notifier les destinaires** pour que Messaging Security Agent avertisse les destinataires prévus des messages électroniques dont le contenu a été filtré.

    Sélectionnez **Ne pas notifier les destinataires externes** pour envoyer les notifications aux destinataires internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

12. Sélectionnez **Notifier les expéditeurs** pour que Messaging Security Agent avertisse les expéditeurs des messages électroniques dont le contenu a été filtré.

    Sélectionnez **Ne pas notifier les expéditeurs externes** pour envoyer les notifications aux expéditeurs internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

13. Dans la section **Options avancées**, cliquez sur l'icône plus (+) pour développer la sous-section **Configuration d'archive**.

    a. Dans le champ **Répertoire de quarantaine**, saisissez le chemin d'accès au dossier dans lequel la fonction de filtrage de contenu doit placer les e-mails mis en quarantaine ou acceptez la valeur par défaut : `<Dossier d'installation de Messaging Security Agent>\storage\quarantine`

    b. Dans le champ **Répertoire d'archivage**, saisissez le chemin d'accès au dossier dans lequel la fonction de filtrage de contenu doit placer les e-mails archivés ou acceptez la valeur par défaut : `<Dossier d'installation de Messaging Security Agent>\storage \sauvegarde du filtrage de contenu`

14. Cliquez sur l'icône plus (+) pour développer la sous-section **Paramètres de remplacement**.

    a. Dans le champ **Nom du fichier de remplacement**, saisissez le nom du fichier que la fonction de filtrage de contenu doit utiliser pour remplacer un e-mail lorsqu'une règle utilisant l'action « Remplacer par un texte/fichier » est déclenchée ou acceptez la valeur par défaut :

    b. Dans le champ **Texte de remplacement**, saisissez ou collez le contenu du texte de remplacement que la fonction de filtrage du contenu doit utiliser lorsqu'un e-mail déclenche une règle dont l'action est « Remplacer par un texte/fichier » ou acceptez le texte par défaut :

15. Cliquez sur **Terminer**.

L'assistant se ferme et l'écran Filtrage de contenu s'affiche.

Création d'exceptions aux règles de filtrage de contenu

- Pour le scan en temps réel :

  Dispositifs > **{Agent Messaging Security Agent}** > **Configurer la stratégie** > **Filtrage de contenu**

- Pour le scan manuel :

  Scans > **Manuel** > **{Développer l'agent Messaging Security Agent}** > **Filtrage de contenu**

- Pour le scan programmé :

  Scans > **Programmé** > **{Développer l'agent Messaging Security Agent}** > **Filtrage de contenu**

Procédure

1. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

2. Sélectionnez **Créer des exceptions pour des comptes de messagerie particuliers**.

3. Cliquez sur **Suivant**.

4. Entrez un nom de règle.

5. Saisissez les comptes de messagerie électronique que vous souhaitez exclure du filtrage de contenu dans le champ prévu à cet effet et cliquez sur **Ajouter**.

   Ces comptes de messagerie électronique sont ajoutés à votre liste de comptes de messagerie exclus. Messaging Security Agent n'applique pas les règles de contenu avec une priorité inférieure à cette règle aux comptes de messagerie de cette liste

6. Lorsque vous avez fini de compléter votre liste de comptes de messagerie exclus, cliquez sur **Terminer**.

   L'assistant se ferme et l'écran **Filtrage de contenu** s'affiche.

Prévention de la perte des données

Vous pouvez utiliser la prévention de la perte de données pour assurer une protection contre la perte de données via les e-mails sortants. Cette fonction peut protéger des données telles que des numéros de sécurité sociale, des numéros de téléphone, des numéros de compte bancaire et autres informations professionnelles confidentielles correspondant à un modèle défini.

Les versions de Microsoft Exchange suivantes sont prises en charge dans cette version :

TABLEAU 6-3. VERSIONS DE MICROSOFT EXCHANGE PRISES EN CHARGE

PRIS EN CHARGE	NON PRIS EN CHARGE
2007 x64	2003 x86/x64
2010 x64	2007 x86
	2010 x86

Travail préliminaire

Avant de surveiller les données sensibles pour éviter les pertes potentielles, déterminez ce qui suit :

- Quelles données nécessitent une protection contre les utilisateurs non autorisés ?
- Où les données résident-elles ?
- Où et quand les données sont-elles transmises ?

- Quels utilisateurs sont autorisés à accéder à ces informations ou à les transmettre ?

Cet audit important requiert généralement la participation de plusieurs départements et d'un personnel connaissant les informations sensibles de votre entreprise. Les procédures ci-dessous partent du principe que vous avez identifié les informations sensibles et avez mis en place des stratégies de sécurité concernant leur gestion.

La fonction de prévention de la perte de données est constituée des trois composants suivants :

- **Règles** (modèles à rechercher)
- **Domaines à exclure** du filtrage
- **Expéditeurs approuvés** (comptes de messagerie à exclure du filtrage)

Pour plus de détails, voir *Gestion des règles de prévention contre la perte de données à la page 6-34*.

Gestion des règles de prévention contre la perte de données

L'agent Messaging Security Agent affiche toutes les règles de prévention contre la perte de données sur l'écran **Prévention contre la perte de données** (**Dispositifs** > **{Messaging Security Agent}** > **Configurer la stratégie** > **Prévention contre la perte de données**).

Procédure

1. Cet écran affiche un résumé des informations relatives aux règles, comprenant :
    - **Règle** : Worry-Free Business Security propose des règles par défaut (voir *Règles de prévention de la perte de données par défaut à la page 6-42*). Ces règles sont désactivées par défaut. Vous pouvez les adapter à vos besoins ou les supprimer. Si aucune de ces règles ne vous est utile, ajoutez vos propres règles.

Conseil

Faites passer le pointeur de la souris sur le nom de la règle pour afficher son contenu. Les règles utilisant une expression rationnelle comportent une icône de loupe (

).

- **Action** : l'agent Messaging Security Agent exécute cette action lorsqu'une règle est déclenchée.
- **Priorité** : l'agent Messaging Security Agent applique successivement chaque règle selon l'ordre indiqué sur cette page.
- **Activé** : l'icône verte désigne une règle activée et l'icône rouge une règle désactivée.

2. Effectuez les actions suivantes :

TÂCHE	ÉTAPES
Activer/Désactiver la prévention contre la perte de données	Cochez ou décochez la case **Activer la prévention de la perte des données en temps réel** située en haut de la page.
Ajouter une règle	Cliquez sur **Ajouter**. Dans la nouvelle fenêtre qui s'ouvre, vous pouvez choisir le type de règle à ajouter. Pour plus d'informations, voir *Ajout de règles de prévention de la perte de données à la page 6-43*.
Modifier une règle	Cliquez sur le nom de la règle à modifier. Un nouvel écran s'affiche. Pour en savoir plus sur les paramètres de règle que vous pouvez modifier, reportez-vous à la rubrique *Ajout de règles de prévention de la perte de données à la page 6-43*.

TÂCHE	ÉTAPES

Importer et exporter des règles	Pour importer une ou plusieurs règles d'un fichier en texte brut (ou les exporter vers un fichier en texte brut), suivez les instructions ci-dessous. Si vous le souhaitez, vous pouvez modifier directement les règles au moyen de ce fichier.
	
	`[SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599]`
	
	`RuleName=Bubbly`
	
	`UserExample=`
	
	`Value=Bubbly`
	
	`[SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6]`
	
	`RuleName=Master Card No.`
	
	`UserExample=Value=.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b`

	Pour exporter des règles vers un fichier en texte brut, sélectionnez une ou plusieurs règles dans la liste et cliquez sur **Exporter**. **Conseil** Vous pouvez sélectionner des règles qui apparaissent sur un écran uniquement. Pour sélectionner des règles apparaissant sur différents écrans, augmentez la valeur de l'option « Lignes par page » en haut du tableau de la liste des règles afin d'afficher suffisamment de lignes pour englober toutes les règles à exporter.

TÂCHE	ÉTAPES
	Pour importer des règles : a. Créez un fichier en texte brut au format affiché ci-dessus. Vous pouvez également cliquer sur le bouton **Télécharger plus de règles par défaut** situé sous le tableau, puis enregistrer les règles. b. Cliquez sur **Importer**. Une nouvelle fenêtre s'affiche. c. Cliquez sur **Parcourir** pour localiser le fichier à importer, puis cliquez sur **Importer**. La prévention contre la perte de données importe les règles du fichier et les ajoute à la fin de la liste des règles actuelle. **Conseil** Si vous avez déjà plus de 10 règles, les règles importées ne sont pas visibles sur la première page. Utilisez les icônes de navigation dans les pages en haut ou en bas de la liste des règles pour afficher la dernière page de la liste. Les règles que vous venez d'importer doivent s'y trouver.

TÂCHE	ÉTAPES
Réorganiser les règles	Messaging Security Agent applique les règles de prévention contre la perte de données aux courriers électroniques dans l'ordre dans lequel elles apparaissent sur l'écran **Prévention contre la perte de données**. Configurez l'ordre selon lequel les règles s'appliquent. L'agent filtre tous les messages électroniques en fonction de chaque règle jusqu'à ce qu'une violation de contenu déclenche une action qui empêche de continuer le scan (par exemple, Supprimer ou Quarantaine). Modifiez l'ordre de ces règles pour optimiser la prévention de la perte de données. a. Cochez la case correspondant à la règle dont vous souhaitez modifier le numéro d'ordre. b. Cliquez sur **Réorganiser**. Un encadré s'affiche autour du numéro d'ordre de la règle. c. Dans la case de la colonne **Priorité**, supprimez le numéro d'ordre existant et entrez-en un nouveau. **Remarque** Veillez à ne pas entrer un numéro supérieur au nombre total de règles de la liste. Si vous entrez un numéro supérieur au nombre total de règles, Worry-Free Business Security l'ignore et ne modifie pas le numéro d'ordre de la règle. d. Cliquez sur **Enregistrer la réorganisation**. La règle est déplacée vers le niveau de priorité entré et tous les autres numéros d'ordre des règles sont modifiés en conséquence. Par exemple, si vous sélectionnez le numéro d'ordre 5 et que vous le remplacez par 3, les numéros d'ordre 1 et 2 ne changent pas, tandis que le numéro 3 et les numéros supérieurs augmentent d'une unité.
Activer/Désactiver des règles	Cliquez sur l'icône dans la colonne Activé.

TÂCHE	ÉTAPES
Supprimer des règles	Lorsque vous supprimez une règle, Messaging Security Agent met à jour l'ordre des autres règles afin d'indiquer les modifications. **Remarque** la suppression d'une règle est irréversible. Il est préférable de désactiver une règle plutôt que de la supprimer. a. Sélectionnez une règle. b. Cliquez sur **Supprimer**.

TÂCHE	ÉTAPES
Exclure des comptes de domaine spécifiques	Au sein d'une entreprise, l'échange d'informations commerciales confidentielles est une nécessité quotidienne. Par ailleurs, la charge de traitement des serveurs Security Server serait excessive si la fonction de prévention contre la perte de données devait filtrer tous les messages internes. Pour ces raisons, vous devez configurer un ou plusieurs domaines par défaut représentant votre trafic de messagerie interne afin que la prévention de la perte de données ne filtre pas des messages envoyés d'un compte à un autre au sein du domaine de votre domaine. Cette liste permet à tous les messages électroniques internes (qui circulent au sein du domaine de l'entreprise) de contourner les règles de prévention de la perte de données. Au moins un domaine est requis. Complétez la liste si vous utilisez plusieurs domaines. Par exemple : `*@exemple.com` a. Cliquez sur l'icône plus (+) pour développer la section **Compte(s) de domaine(s) particulier(s) exclu(s) de la prévention de la perte des données**. b. Placez le curseur dans le champ **Ajouter** et tapez le domaine, selon le modèle suivant : `*@exemple.com` c. Cliquez sur **Ajouter**. Le domaine apparaît dans la liste sous le champ **Ajouter**. d. Cliquez sur **Enregistrer** pour terminer le processus. **AVERTISSEMENT!** Le domaine n'est ajouté que lorsque vous cliquez sur **Enregistrer**. Si vous cliquez sur **Ajouter**, mais pas sur **Enregistrer**, le domaine n'est pas ajouté.

TÂCHE	ÉTAPES
Ajouter des comptes de messagerie dans la liste des expéditeurs approuvés	Le courrier des expéditeurs approuvés est transmis à l'extérieur de votre réseau sans filtrage effectué par la prévention de la perte de données. La prévention de la perte de données ignore le contenu des messages envoyés depuis des comptes de messagerie figurant dans la liste approuvée. a. Cliquez sur l'icône plus (+) pour développer la section **Expéditeurs approuvés**. b. Placez le curseur dans le champ **Ajouter** et tapez l'adresse électronique complète, selon le modèle suivant : `exemple@exemple.com` c. Cliquez sur **Ajouter**. L'adresse apparaît dans la liste sous le champ **Ajouter**. d. Cliquez sur **Enregistrer** pour terminer le processus. **Remarque** L'adresse n'est ajoutée que lorsque vous cliquez sur **Enregistrer**. Si vous cliquez sur **Ajouter**, mais pas sur **Enregistrer**, l'adresse n'est pas ajoutée.

Tâche	Étapes

Importer des comptes de messagerie dans la liste des expéditeurs approuvés	Vous pouvez importer une liste d'adresses électroniques d'un fichier en texte brut mis en forme avec un compte de messagerie par ligne, tel que :
	`admin@example.com`
	`ceo@example.com`
	`president@example.com`
	a. Cliquez sur l'icône plus (+) pour développer la section **Expéditeurs approuvés**.
	b. Cliquez sur **Importer**.
	Une nouvelle fenêtre s'affiche.
	c. Cliquez sur **Parcourir** pour localiser le fichier en texte brut à importer, puis cliquez sur **Importer**.
	La prévention contre la perte de données importe les règles dans le fichier et les ajoute à la fin de la liste actuelle.

3. Cliquez sur **Enregistrer**.

Règles de prévention de la perte de données par défaut

La prévention de la perte de données propose quelques règles par défaut, comme indiqué dans le tableau suivant.

Tableau 6-4. Règles de prévention de la perte de données par défaut

Nom de la règle	Exemple	Expression rationnelle
Numéro de compte de carte Visa	4111-1111-1111-1111	.REG. \b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
Numéro de compte de carte MasterCard	5111-1111-1111-1111	.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b

Nom de la règle	Exemple	Expression rationnelle
Numéro de compte de carte American Express	3111-111111-11111	.REG. \b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b
Numéro de compte de carte Diners Club/Carte Blanche	3111-111111-1111	.REG. [^\d-]((36\d{2}|38\d{2}|30[0-5]\d)-?\d{6}-?\d{4})[^\d-]
IBAN	BE68 5390 0754 7034, FR14 2004 1010 0505 0001 3M02 606, DK50 0040 0440 1162 43	.REG. [^\w](([A-Z]{2}\d{2}[-|\s]?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}[-|\s]){3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}[-|\s]){2}[A-Za-z0-9]{3,4}))[^\w]
Swift/BIC	BANK US 99	.REG. [^\w-]([A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?)[^\w-]
Date ISO	2004/01/23, 04/01/23, 2004-01-23, 04-01-23	.REG. [^\d\/-]([1-2]\d{3}[-\/][0-1]?\d[-\/][0-3]?\d|\d{2}[-\/][0-1]?\d[-\/][0-3]?\d)[^\d\/-]

Remarque

Un fichier .zip contenant plusieurs règles de prévention de la perte de données peut être téléchargé à partir de la console Web. Accédez à **Paramètres de sécurité** > **{Messaging Security Agent}** > **Configurer les paramètres** > **Prévention de la perte de données**, puis cliquez sur **Télécharger plus de règles par défaut**.

Ajout de règles de prévention de la perte de données

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Prévention de la perte de données**.

   Un nouvel écran s'affiche.

5. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

6. Sélectionnez la partie du message que vous souhaitez évaluer. Messaging Security Agent peut filtrer les e-mails par :

   - En-tête (From, To et Cc)
   - Objet
   - Corps
   - Pièce jointe

7. Ajoutez une règle.

   Pour ajouter une règle basée sur un mot-clé :

   a. Sélectionnez **Mot-clé**.

   b. Saisissez le mot-clé dans le champ affiché. Celui-ci doit contenir entre 1 et 64 caractères alphanumériques.

   c. Cliquez sur **Suivant**.

   Pour ajouter une règle basée sur des expressions générées automatiquement :

   a. Pour obtenir des directives sur la définition d'expressions rationnelles, voir *Expressions rationnelles à la page D-10*.

   b. Sélectionnez **Expression rationnelle (générée automatiquement)**.

   c. Tapez un **nom de la règle** dans le champ prévu à cet effet. Ce champ est obligatoire.

   d. Dans le champ **Exemple**, saisissez ou collez un exemple de type de chaîne (jusqu'à 40 caractères) auquel l'expression rationnelle doit correspondre. Les caractères alphanumériques apparaissent en

majuscules dans la zone ombrée avec des rangées de cases sous le champ **Exemple**.

e. Si l'expression contient des constantes, sélectionnez-les en cliquant sur les cases dans lesquelles sont affichés les caractères.

   Lorsque vous cliquez sur une case, son contour devient rouge pour indiquer qu'il s'agit d'une constante et l'outil de génération automatique modifie l'expression rationnelle figurant sous la zone ombrée.

> **Remarque**
>
> Les caractères non alphanumériques (par exemple, les espaces, les points-virgules et d'autres signes de ponctuation) sont automatiquement considérés comme des constantes et ne peuvent pas être convertis en variables.

f. Pour vérifier que l'expression rationnelle générée correspond au modèle prévu, sélectionnez **Fournissez un autre exemple pour vérifier la règle (facultatif)**.

   Un champ de test s'affiche sous cette option.

g. Tapez un autre exemple du modèle que vous venez d'entrer.

   Par exemple, si cette expression doit correspondre à une série de numéros de compte suivant le modèle « 01-EX????? 20?? », saisissez un autre exemple correspondant, tel que « 01-Extreme 2010 », puis cliquez sur **Test**.

   L'outil valide le nouvel exemple par rapport à l'expression rationnelle existante et place une coche verte en regard du champ si cet exemple correspond. Si l'expression rationnelle ne correspond pas au nouvel exemple, un X rouge s'affiche en regard du champ.

AVERTISSEMENT!

Les expressions rationnelles créées avec cet outil ne respectent pas la casse. Ces expressions ne peuvent correspondre qu'à des modèles ayant le nombre exact de caractères de votre échantillon ; elles ne peuvent pas évaluer un modèle « un ou plusieurs » d'un caractère donné.

h. Cliquez sur **Suivant**.

Pour ajouter une règle basée sur des expressions définies par l'utilisateur :

AVERTISSEMENT!

Les expressions rationnelles constituent un outil puissant de correspondance de chaînes. Veillez à bien connaître la syntaxe des expressions rationnelles avant d'utiliser celles-ci. Les expressions rationnelles n'utilisant pas une syntaxe correcte peuvent diminuer considérablement les performances. Trend Micro vous recommande de commencer par des expressions rationnelles simples. Lorsque vous créez une règle, utilisez l'action d'« archivage » et étudiez la façon dont la prévention de la perte de données gère les messages à l'aide de cette règle. Si vous êtes sûr que la règle ne peut pas avoir de conséquences inattendues, vous pouvez modifier l'action.

a. Pour obtenir des directives sur la définition d'expressions rationnelles, voir *Expressions rationnelles à la page D-10*.

b. Sélectionnez **Expression rationnelle (définie par l'utilisateur)**.

Les champs **Nom de la règle** et **Expression rationnelle** s'affichent.

c. Tapez un **nom de la règle** dans le champ prévu à cet effet. Ce champ est obligatoire.

d. Dans le champ **Expressions rationnelles**, saisissez une expression rationnelle commençant par le préfixe « `.REG.` », sans dépasser 255 caractères, préfixe compris.

AVERTISSEMENT!

Procédez avec précaution lorsque vous collez des éléments dans ce champ. Si des caractères non pertinents, par exemple un saut de ligne propre à un système d'exploitation ou une balise HTML, sont inclus dans le contenu du Presse-papiers, l'expression collée est inexacte. Pour cette raison, Trend Micro vous recommande d'entrer l'expression manuellement.

e. Pour vérifier que l'expression rationnelle correspond au modèle prévu, sélectionnez **Fournissez un autre exemple pour vérifier la règle (facultatif)**.

Un champ de test s'affiche sous cette option.

f. Tapez un autre exemple du modèle que vous venez d'entrer (40 caractères au maximum).

Par exemple, si cette expression doit correspondre à une série de numéros de compte suivant le modèle « ACC-????? 20?? », saisissez un autre exemple correspondant, tel que « Acc-65432 2012 », puis cliquez sur **Test**.

L'outil valide le nouvel exemple par rapport à l'expression rationnelle existante et place une coche verte en regard du champ si cet exemple correspond. Si l'expression rationnelle ne correspond pas au nouvel exemple, un X rouge s'affiche en regard du champ.

g. Cliquez sur **Suivant**.

8. Sélectionnez une action devant être prise par Messaging Security Agent lors du déclenchement d'une règle (pour obtenir des descriptions, voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*) :

- Remplacer par un texte/fichier

Remarque

Vous ne pouvez pas remplacer le texte des champs De, À, Cc ou Objet.

- Mettre la totalité du message en quarantaine
- Mettre en quarantaine une partie du message
- Supprimer la totalité du message
- Archivage
- Ignorer la totalité du message

9. Sélectionnez **Notifier les destinaires** pour que Messaging Security Agent avertisse les destinataires prévus lorsque la fonction de prévention de la perte de données prend des mesures contre un e-mail spécifique.

   Vous souhaitez peut-être, pour diverses raisons, ne pas indiquer aux destinataires externes qu'un message contenant des informations sensibles a été bloqué. Sélectionnez **Ne pas notifier les destinataires externes** pour envoyer les notifications aux destinataires internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

10. Sélectionnez **Notifier les expéditeurs** pour que Messaging Security Agent avertisse les expéditeurs prévus lorsque la prévention de la perte des données prend des mesures à l'encontre d'un message électronique spécifique.

    Vous souhaitez peut-être, pour diverses raisons, ne pas indiquer aux expéditeurs externes qu'un message contenant des informations sensibles a été bloqué. Sélectionnez **Ne pas notifier les expéditeurs externes** pour envoyer les notifications aux expéditeurs internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

11. Dans la section **Options avancées**, cliquez sur l'icône plus (+) pour développer la sous-section **Configuration d'archive**.

    a. Dans le champ **Répertoire de quarantaine**, saisissez le chemin d'accès au dossier dans lequel la fonction de prévention contre la perte de données doit placer les e-mails mis en quarantaine ou acceptez la valeur par défaut : `<Dossier d'installation de Messaging Security Agent>\storage\quarantine`

b. Dans le champ **Répertoire d'archivage**, saisissez le chemin d'accès au dossier dans lequel la fonction de prévention contre la perte de données doit placer les e-mails archivés ou acceptez la valeur par défaut : `<Dossier d'installation de Messaging Security Agent>\storage\sauvegarde du filtrage de contenu`

12. Cliquez sur l'icône plus (+) pour développer la sous-section **Paramètres de remplacement**.

    a. Dans le champ **Nom du fichier de remplacement**, saisissez le nom du fichier que la fonction de prévention de la perte de données doit utiliser pour remplacer un e-mail lorsqu'une règle utilisant l'action « Remplacer par un texte/fichier » est déclenchée ou acceptez la valeur par défaut :

    b. Dans le champ **Texte de remplacement**, saisissez ou collez le contenu du texte de remplacement que la fonction de prévention de la perte de données doit utiliser lorsqu'un e-mail déclenche une règle dont l'action est « Remplacer par un texte/fichier » ou acceptez le texte par défaut :

13. Cliquez sur **Terminer**.

    L'assistant se ferme et l'écran Prévention de la perte de données s'affiche.

Blocage des pièces jointes

Le blocage des pièces jointes empêche que les pièces jointes aux e-mails ne soient transmises à Microsoft Exchange Information Store. Configurez Messaging Security Agent pour qu'il bloque les pièces jointes en fonction de leur type ou de leur nom, puis pour qu'il remplace, mette en quarantaine ou supprime tous les messages contenant des pièces jointes répondant à ces critères.

Le blocage peut être appliqué au cours du scan en temps réel, manuel ou programmé, mais les actions de suppression et de mise en quarantaine ne sont pas disponibles pour les scans manuels et programmés.

L'extension d'une pièce jointe identifie le type de fichier, par exemple `.txt`, `.exe` ou `.dll`. Cependant, Messaging Security Agent examine l'en-tête du fichier plutôt que le nom du fichier afin de vérifier le type de fichier véritable. De nombreux virus/programmes malveillants sont étroitement associés à certains types de fichiers. En configurant Messaging Security Agent de façon à bloquer les pièces jointes en fonction du type de fichier, vous pouvez réduire les risques qu'engendrent ces types de fichiers pour la sécurité de vos serveurs Microsoft Exchange. De même, les attaques spécifiques sont souvent associées à un nom de fichier spécifique.

Conseil

le blocage est un moyen efficace de contrôler les épidémies virales. Vous pouvez temporairement mettre en quarantaine les types de fichiers à haut risque ou ceux dont le nom caractéristique est associé à un virus/programme malveillant connu. Par la suite, vous pourrez examiner le dossier de quarantaine et entreprendre une action sur les fichiers détectés.

Configuration du blocage des pièces jointes

La configuration des options de blocage des pièces jointes pour les serveurs Microsoft Exchange implique de définir les règles pour bloquer les messages contenant certaines pièces jointes.

- Pour le scan en temps réel :

  Dispositifs > **{Agent Messaging Security Agent}** > **Configurer la stratégie** > **Blocage des pièces jointes**

- Pour le scan manuel :

  Scans > **Manuel** > **{Développer l'agent Messaging Security Agent}** > **Blocage des pièces jointes**

- Pour le scan programmé :

  Scans > **Programmé** > **{Développer l'agent Messaging Security Agent}** > **Blocage des pièces jointes**

Procédure

1. Sous l'onglet **Cible**, mettez à jour les éléments suivants si nécessaire :

   - **Toutes les pièces jointes** : l'agent peut bloquer tous les e-mails contenant des pièces jointes. Cependant, ce type de scan requiert un niveau de traitement avancé. Affinez ce type de scan en sélectionnant les types ou les noms de pièces jointes à exclure.

     - **Types de pièces jointes à exclure**

     - **Noms des pièces jointes à exclure**

   - **Pièces jointes spécifiques** : lorsque vous sélectionnez ce type de scan, l'agent scanne uniquement les e-mails contenant des pièces jointes que vous identifiez. Ce type de scan peut être très exclusif et convient parfaitement aux courriers électroniques contenant des pièces jointes représentant une menace. Ce scan s'effectue très rapidement lorsque vous spécifiez un petit nombre de noms ou de types de pièces jointes.

     - **Types des pièces jointes** : l'agent examine l'en-tête du fichier plutôt que son nom afin de vérifier le type de fichier.

     - **Noms des pièces jointes** : par défaut, l'agent examine l'en-tête du fichier plutôt que son nom afin de vérifier le type de fichier. Lorsque vous définissez le blocage des pièces jointes de façon à scanner des noms spécifiques, l'agent détectera les types de pièces jointes en fonction de leur nom.

   - **Bloquer les noms ou types des pièces jointes contenues dans les fichiers compressés**

2. Cliquez sur l'onglet **Action** pour définir les mesures prises par Messaging Security Agent lorsqu'il détecte des pièces jointes. Messaging Security Agent peut exécuter les actions suivantes (pour des descriptions, voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*) :

   - Remplacer par un texte/fichier

- Mettre la totalité du message en quarantaine
- Mettre en quarantaine une partie du message
- Supprimer la totalité du message

3. Sélectionnez **Notifier les destinaires** pour que Messaging Security Agent avertisse les destinataires prévus des e-mails contenant des pièces jointes.

   Sélectionnez **Ne pas notifier les destinataires externes** pour envoyer les notifications aux destinataires internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

4. Sélectionnez **Notifier les expéditeurs** pour que Messaging Security Agent avertisse les expéditeurs des e-mails contenant des pièces jointes.

   Sélectionnez **Ne pas notifier les expéditeurs externes** pour envoyer les notifications aux expéditeurs internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

5. Cliquez sur l'icône plus (+) pour développer la sous-section **Paramètres de remplacement**.

   a. Dans le champ **Nom du fichier de remplacement**, saisissez le nom du fichier que la fonction de blocage des pièces jointes doit utiliser pour remplacer un e-mail lorsqu'une règle utilisant l'action « Remplacer par un texte/fichier » est déclenchée ou acceptez la valeur par défaut :

   b. Dans le champ **Texte de remplacement**, saisissez ou collez le contenu du texte de remplacement que la fonction de blocage des pièces jointes doit utiliser lorsqu'un e-mail déclenche une règle dont l'action est « Remplacer par un texte/fichier » ou acceptez le texte par défaut :

6. Cliquez sur **Enregistrer**.

Réputation de sites Web

La réputation de sites Web contribue à empêcher l'accès aux URL sur le Web ou incorporés dans des messages électroniques qui représentent des risques potentiels. La réputation de sites Web vérifie la réputation de l'URL sur les serveurs de réputation de sites Web de Trend Micro, puis la corrèle avec la stratégie de réputation Web spécifique appliquée sur le client. Selon la stratégie utilisée :

- Security Agent doit bloquer ou autoriser l'accès à un site Web.
- Messaging Security Agent (Advanced uniquement) mettra en quarantaine, supprimera ou marquera le message contenant des URL malveillantes ou autorisera l'envoi du message si les URL sont sûres.

La réputation de sites Web envoie à la fois une notification par e-mail à l'administrateur et une notification en ligne à l'utilisateur pour les détections.

Selon l'emplacement (Au bureau/Hors du bureau) du client, configurez un niveau de sécurité différent pour les agents Security Agent.

Si la réputation de sites Web bloque une URL que vous pensez sûre, ajoutez-le à la liste des URL approuvées.

Conseil

Pour économiser la bande passante, Trend Micro recommande d'ajouter les sites Web internes de l'entreprise à la liste des URL approuvées établie par la fonction de réputation de sites Web.

Score de réputation

Le « score de réputation » d'une URL détermine s'il s'agit d'une menace Internet ou non. Trend Micro calcule le score à l'aide de mesures propriétaires.

Trend Micro considère une URL comme étant une menace Internet si le score atteint se situe dans la plage définie et comme sûre si le score dépasse le seuil.

Un agent Security Agent dispose de trois niveaux de sécurité en fonction desquels il autorise ou bloque l'accès à une URL.

- **Élevé** : Bloque les pages qui sont :
  - **Dangereux :** caractère frauduleux avéré ou sources de menaces connues
  - **Hautement suspect** : caractère frauduleux suspecté ou sources de menaces possibles
  - **Suspect** : associées à du spam ou potentiellement compromises
  - **Non testée** : Bien que Trend Micro teste activement la sécurité des pages Web, les utilisateurs peuvent rencontrer des pages non testées lorsqu'ils visitent des sites Web nouveaux ou peu consultés. Le blocage de l'accès aux pages non testées peut améliorer la sécurité, mais il peut également empêcher l'accès à des pages sûres.
- **Moyen** : Bloque les pages qui sont :
  - **Dangereux :** caractère frauduleux avéré ou sources de menaces connues
  - **Hautement suspect** : caractère frauduleux suspecté ou sources de menaces possibles
- **Faible** : Bloque les pages qui sont :
  - **Dangereux :** caractère frauduleux avéré ou sources de menaces connues

Configuration de la réputation de sites Web pour les agents Messaging Security Agent

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.

3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Réputation de sites Web**.

   Un nouvel écran s'affiche.

5. Mettez à jour les éléments suivants, si nécessaire :

   - **Activer la réputation des sites Web**
   - Niveau de sécurité : **Élevé**, **Moyen** ou **Faible**
   - URL approuvées
     - **URL à approuver** : séparez les URL multiples par des points-virgules (;). Cliquez sur **Ajouter**.

       Remarque

       l'approbation d'un URL implique l'approbation de tous ses sous-domaines.

       Utilisez les caractères de substitution avec prudence, car ils risquent d'autoriser des groupes importants d'URL.

     - **Liste des URL approuvées** : les URL de cette liste ne seront pas bloquées.

6. Cliquez sur l'onglet **Action**, puis sélectionnez une action que l'agent Messaging Security Agent doit prendre lorsqu'une stratégie de réputation de sites Web est déclenchée (pour des descriptions, voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*) :

   - Remplacer par un texte/fichier

     Remarque

     Vous ne pouvez pas remplacer le texte des champs De, À, Cc ou Objet.

   - Mise en quarantaine du message dans le dossier de spams de l'utilisateur

- Supprimer la totalité du message
- Marquer et envoyer

7. Sélectionnez **Effectuer l'action sur les URL qui n'ont pas été évaluées par Trend Micro** pour traiter les URL non classées comme suspicieuses. La même action que celle spécifiée dans l'étape précédente sera exécutée pour les e-mails contenant des URL non classées.

8. Sélectionnez **Notifier les destinaires** pour que Messaging Security Agent avertisse les destinataires prévus lorsque la fonction de réputation de sites Web prend des mesures contre un e-mail spécifique.

   Vous souhaitez peut-être, pour diverses raisons, ne pas indiquer aux destinataires externes qu'un message contenant des URL malveillantes a été bloqué. Sélectionnez **Ne pas notifier les destinataires externes** pour envoyer les notifications aux destinataires internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

9. Sélectionnez **Notifier les expéditeurs** pour que Messaging Security Agent avertisse les expéditeurs prévus lorsque la réputation des sites Web prend des mesures à l'encontre d'un message électronique spécifique.

   Vous souhaitez peut-être, pour diverses raisons, ne pas indiquer aux expéditeurs externes qu'un message contenant des URL malveillantes a été bloqué. Sélectionnez **Ne pas notifier les expéditeurs externes** pour envoyer les notifications aux expéditeurs internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

10. Cliquez sur **Enregistrer**.

Mobile Security

Les paramètres Mobile Security visent à empêcher les dispositifs non autorisés à accéder aux informations de Microsoft Exchange Server et à les

télécharger. Les administrateurs identifient les dispositifs autorisés à accéder à Microsoft Exchange Server avant d'identifier les utilisateurs de ces mêmes dispositifs autorisés à télécharger ou à mettre à jour leur messagerie, leur calendrier, leurs contacts ou leurs tâches.

Les administrateurs peuvent également appliquer des stratégies de sécurité aux dispositifs. Ces stratégies contrôlent la longueur et la complexité des mots de passe, déterminent si les dispositifs doivent être verrouillés au bout d'un certain temps d'inactivité, s'ils doivent utiliser le chiffrement et si les données des dispositifs doivent être effacées après une série de tentatives de connexion infructueuses.

Assistance technique Mobile Security

TABLEAU 6-5. Assistance technique sur les dispositifs mobiles

SYSTÈME D'EXPLOITATION	VERSION D'IIS	STRATÉGIES DE PROTECTION DES DONNÉES DE DISPOSITIF		CONTRÔLE DE L'ACCÈS		
		EXCHANGE 2007 (OU VERSION ULTÉRIEURE) 64 BITS	EXCHANGE 2003 (32 BITS)	EXCHANGE 2010 (ET VERSION ULTÉRIEURE) 64 BITS	EXCHANGE 2007 (64 BITS)	EXCHANGE 2003 (32 BITS)
• Windows 2008 (64 bits) • SBS 2008 (64 bits)	7 +	Oui	Incompatible	Oui	Non	Incompatible

Système d'exploitation	Version d'IIS	Stratégies de protection des données de dispositif		Contrôle de l'accès		
		Exchange 2007 (ou version ultérieure) 64 bits	Exchange 2003 (32 bits)	Exchange 2010 (et version ultérieure) 64 bits	Exchange 2007 (64 bits)	Exchange 2003 (32 bits)
Windows 2003 (64 bits)	6.0	Oui	Incompatible	Non	Non	Incompatible
• Windows 2003 (32 bits) • SBS 2003 (32 bits)	6.0	Incompatible	Non	Incompatible	Incompatible	Non

Tableau 6-6. Assistance technique sur les systèmes d'exploitation pour dispositifs mobiles

Système d'exploitation mobile	Version de SE
iOS	3.0 - 6.1 (4.3 - 7.0)
Android	2.2 - 4.2
WM/WP (Windows)	7.0 - 8.0
BB (BlackBerry)	7.0 - 10.1

Configuration du contrôle d'accès aux dispositifs

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.
4. Cliquez sur **Mobile Security** > **Contrôle d'accès aux dispositifs**.

   Un nouvel écran s'affiche.
5. Sélectionnez **Activer le contrôle d'accès aux dispositifs**.
6. Cliquez sur **Ajouter**.
7. Saisissez un nom de stratégie, ainsi qu'une description significative de la stratégie.
8. Sélectionnez les dispositifs dont l'accès à Microsoft Exchange Server doit être autorisé/bloqué en identifiant le ou les propriétaires des dispositifs :
   - **N'importe qui**
   - **Spécifier les propriétaires des dispositifs**
9. Si **Spécifier les propriétaires des dispositifs** est sélectionné :
   a. Saisissez le nom du propriétaire d'un dispositif et cliquez sur **Rechercher** pour rechercher le propriétaire du dispositif dans la liste d'adresses globale de Microsoft Exchange Server.
   b. Sélectionnez le propriétaire du dispositif, puis cliquez sur **Ajouter**.
10. S'il est connu, sélectionnez le système d'exploitation du dispositif dans la liste déroulante **Type**.
11. S'il est connu, sélectionnez **Spécifier la plage de numéros de version** et identifiez les versions autorisées de ce système d'exploitation.

12. Indiquez si Messaging Security Agent doit autoriser ou bloquer l'accès à la messagerie, au calendrier, aux contacts ou aux tâches du propriétaire du dispositif.
13. Cliquez sur **Enregistrer**.

Annulation d'une réinitialisation de dispositif en attente

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.
4. Cliquez sur **Mobile Security** > **Réinitialisation de dispositif**.

   Un nouvel écran s'affiche.
5. Identifiez le dispositif dans le tableau de réinitialisation de dispositif, puis cliquez sur **Annuler la réinitialisation**.
6. Cliquez sur **OK**.

Réinitialisation manuelle des dispositifs

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Mobile Security** > **Réinitialisation de dispositif**.

   Un nouvel écran s'affiche.

5. Cliquez sur **Sélectionner des dispositifs**.

   Un nouvel écran s'affiche.

6. Saisissez le nom du propriétaire d'un dispositif, puis cliquez sur **Rechercher** pour rechercher le dispositif en question.

7. Si le dispositif peut être réinitialisé, sélectionnez-le, puis cliquez sur **Réinitialiser**.

Remarque

Vous ne pouvez pas sélectionner un dispositif dont l'état à l'issue d'une recherche est **Réinitialisation réussie** ou **Réinitialisation en attente**.

Configuration des stratégies de sécurité

Worry-Free Business Security utilise la stratégie par défaut de Microsoft Exchange comme stratégie par défaut. La stratégie par défaut figure dans la liste Stratégie de sécurité.

Worry-Free Business Security ne conserve pas les stratégies ajoutées via la console de gestion Microsoft Exchange ou de l'applet de commande Exchange et qui ne correspondent pas à des stratégies par défaut.

Trend Micro recommande aux administrateurs de gérer les stratégies de sécurité à partir de la console de gestion Worry-Free Business Security ou de Microsoft Exchange.

Procédure

1. Accédez à **Dispositifs**.

2. Sélectionnez un agent Messaging Security Agent.

3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Mobile Security** > **Stratégies de sécurité**.

   Un nouvel écran s'affiche.

5. Cliquez sur **Ajouter**.

6. Saisissez un nom de stratégie, ainsi qu'une description significative de la stratégie.

7. Saisissez le nom du propriétaire d'un dispositif et cliquez sur **Rechercher** pour rechercher le propriétaire du dispositif dans la liste d'adresses globale de Microsoft Exchange Server.

8. Sélectionnez le propriétaire du dispositif, puis cliquez sur **Ajouter**.

9. Sélectionnez les critères de sécurité à appliquer au dispositif :

   - **Longueur minimale du mot de passe** : pour obtenir des instructions sur les mots de passe de dispositif mobile, voir *Exigences de complexité des mots de passe à la page 6-62*.
   - **Nombre minimal de jeux de caractères requis** : pour obtenir des instructions sur les mots de passe de dispositif mobile, voir *Exigences de complexité des mots de passe à la page 6-62*.
   - **Temps d'inactivité avant verrouillage du dispositif**
   - **Exiger le chiffrement sur le dispositif** : le dispositif mobile doit prendre en charge le chiffrement.
   - **Nombre d'échecs de connexion avant réinitialisation du dispositif**

10. Cliquez sur **Enregistrer**.

Exigences de complexité des mots de passe

Les exigences en matière de complexité des mots de passe varient selon le type de dispositif et le système d'exploitation.

Les tableaux suivants répertorient le comportement de chaque « Option » de complexité pour les dispositifs testés avant la publication de Worry-Free Business Security 9.0 SP3.

Remarque

Le fonctionnement de la complexité des mots de passe dépend du type de dispositif et de la version du système d'exploitation. Si le mot de passe spécifié ne répond pas aux exigences de complexité, la plupart des dispositifs présentent un message indiquant aux utilisateurs les exigences propres au dispositif.

TABLEAU 6-7. Dispositifs Android

NIVEAU DE COMPLEXITÉ	EXIGENCES DE COMPLEXITÉ	
	ANDROID 4	ANDROID 2
Option 1	Une combinaison des types de caractères suivants : • Au moins un caractère majuscule (A-Z) ou minuscule (a-z) • Au moins un chiffre (0-9) ou un caractère spécial (!@#$ %^&*()_-=+~ ` []{}|;:'"?/<>,.)	Caractère alphanumérique
Option 2	Une combinaison des types de caractères suivants : • Au moins un caractère majuscule (A-Z) ou minuscule (a-z) • Au moins deux chiffres (0-9) ou deux caractères spéciaux (!@#$ %^&*()_-=+~ ` []{}|;:'"?/<>,.)	Une combinaison des types de caractères suivants : • Caractère alphanumérique • Au moins deux chiffres (0-9) ou deux caractères spéciaux (!@#$ %^&*()_-=+~ ` []{}|;:'"?/<>,.)

Niveau de complexité	Exigences de complexité	
	Android 4	Android 2
Option 3	Une combinaison des types de caractères suivants : • Au moins un caractère majuscule (A-Z) ou minuscule (a-z) • Au moins trois chiffres (0-9) ou trois caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Une combinaison des types de caractères suivants : • Caractère alphanumérique • Au moins trois chiffres (0-9) ou trois caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 4	Une combinaison des types de caractères suivants : • Au moins un caractère majuscule (A-Z) ou minuscule (a-z) • Au moins quatre chiffres (0-9) ou quatre caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Une combinaison des types de caractères suivants : • Caractère alphanumérique • Au moins quatre chiffres (0-9) ou quatre caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Tableau 6-8. Dispositifs iOS

Niveau de complexité	Exigences de complexité
Option 1	Une combinaison des types de caractères suivants : • Caractère alphanumérique • Au moins un caractère spécial (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 2	Une combinaison des types de caractères suivants : • Caractère alphanumérique • Au moins deux caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 3	Une combinaison des types de caractères suivants : • Caractère alphanumérique • Au moins trois caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

NIVEAU DE COMPLEXITÉ	EXIGENCES DE COMPLEXITÉ
Option 4	Une combinaison des types de caractères suivants : • Caractère alphanumérique • Au moins quatre caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

TABLEAU 6-9. Dispositifs Windows Phone

NIVEAU DE COMPLEXITÉ	EXIGENCES DE COMPLEXITÉ	
	WINDOWS PHONE 8	WINDOWS PHONE 7
Option 1	Au moins un des types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Une combinaison d'au moins deux des types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 2	Une combinaison d'au moins deux des types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Une combinaison d'au moins deux des types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Niveau de complexité	Exigences de complexité	
	Windows Phone 8	Windows Phone 7
Option 3	Une combinaison d'au mois trois des types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Une combinaison d'au mois trois des types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 4	Une combinaison de tous les types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Une combinaison de tous les types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Tableau 6-10. Dispositifs BlackBerry

Niveau de complexité	Exigences de complexité
Option 1	Au moins un caractère majuscule (A-Z) ou minuscule (a-z)
Option 2	Une combinaison d'au moins deux des types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

Niveau de complexité	Exigences de complexité
Option 3	Une combinaison d'au mois trois des types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 4	Une combinaison de tous les types de caractères suivants : • Caractères majuscules (A-Z) • Caractères minuscules (a-z) • Caractères numériques (0-9) • Caractères spéciaux (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

Mise en quarantaine pour les agents Messaging Security Agent

Lorsque l'agent Messaging Security Agent détecte une menace, du spam, des pièces jointes restreintes et/ou du contenu restreint dans des messages électroniques, il peut déplacer ces messages vers un dossier de quarantaine. Ce processus constitue une alternative à la suppression de message/pièce jointe, empêche les utilisateurs d'ouvrir le message infecté et de répandre la menace.

Le dossier de quarantaine par défaut de Message Security Agent est :

```
<Dossier d'installation de Messaging Security Agent>\storage
\quarantine
```

Les fichiers en quarantaine sont chiffrés pour plus de sécurité. Pour ouvrir un fichier chiffré, utilisez l'outil Restaurer les virus et spywares encodés (`VSEncode.exe`). Voir *Restauration des fichiers chiffrés à la page 14-19*.

Les administrateurs peuvent interroger la base de données de mise en quarantaine pour rassembler des informations sur les messages mis en quarantaine.

Utilisez la mise en quarantaine pour :

- Éliminer le risque de suppression permanente des messages importants, s'ils sont détectés par erreur par des filtres agressifs
- Contrôler les messages qui déclenchent les filtres de contenu afin de déterminer la gravité de l'infraction à la règle
- Conserver des preuves démontrant qu'un employé utilise mal le système de messagerie de votre entreprise

Remarque

Ne confondez pas le dossier de quarantaine avec le dossier de spam de l'utilisateur final. Le dossier de quarantaine est un dossier en mode fichiers. Dès qu'un agent Messaging Security Agent met en quarantaine un message électronique, il l'envoie vers le dossier de quarantaine. Le dossier de spam de l'utilisateur final se trouve dans la banque d'informations de la boîte aux lettres de chaque utilisateur. Le dossier de spam de l'utilisateur final reçoit uniquement les messages électroniques résultant d'une mise en quarantaine anti-spam vers le dossier de spam d'un utilisateur, mais pas des actions de mise en quarantaine résultant du filtrage de contenu, de l'antivirus/anti-spyware ou des stratégies de blocage des pièces jointes.

Interrogation des répertoires de quarantaine

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Quarantaine** > **Requête**.

   Un nouvel écran s'affiche.

5. Mettez à jour les éléments suivants, si nécessaire :

   - Intervalle de date/heure
   - Motifs de la mise en quarantaine
     - **Tous les motifs**
     - **Types spécifiés** : choisissez Scan antivirus, Anti-spam, Filtrage de contenu, Blocage des pièces jointes et/ou Parties de messages non scannables.
   - État du renvoi
     - **Jamais renvoyé**
     - **Renvoyé au moins une fois**
     - **Les deux ci-dessus**
   - Critères avancés
     - **Expéditeur** : messages d'expéditeurs spécifiques. Utilisez des caractères génériques, si nécessaire.
     - **Destinataire** : messages de destinataires spécifiques. Utilisez des caractères génériques, si nécessaire.
     - **Objet** : messages avec des objets spécifiques. Utilisez des caractères génériques, si nécessaire.
     - **Classer par** : configurez l'ordre de tri de la page de résultats.
     - **Affichage** : nombre de résultats par page.

6. Cliquez sur **Rechercher**. Voir *Affichage des résultats de requête et exécution d'une action à la page 6-70*.

Affichage des résultats de requête et exécution d'une action

L'écran **Résultats de la requête de quarantaine** affiche les informations suivantes au sujet des messages:

- **Heure du scan**
- **Expéditeur**
- **Destinataire**
- **Objet**
- **Cause** : la cause de la mise en quarantaine du message.
- **Nom du fichier** : le nom du fichier bloqué du message.
- **Chemin de quarantaine** : l'emplacement de mise en quarantaine du message. Les administrateurs peuvent décoder le fichier à l'aide de l'outil VSEncoder.exe (Voir *Restauration des fichiers chiffrés à la page 14-19*), puis le renommer avec une extension `.eml` pour l'afficher.

  AVERTISSEMENT!

  L'affichage de fichiers infectés peut propager l'infection.

- **État du renvoi**

Procédure

1. Si vous trouvez un message suspect, supprimez-le.

   AVERTISSEMENT!

   Le dossier de quarantaine contient les messages électroniques à haut risque d'infection. Lorsque vous traitez les messages électroniques du dossier de quarantaine, prenez garde à ne pas infecter accidentellement le client.

2. Si vous trouvez un message suspect, sélectionnez le message et cliquez sur l'icône de renvoi ().

Remarque

Si vous renvoyez un message en quarantaine qui avait été envoyé à l'aide de Microsoft Outlook, il se peut que le destinataire reçoive plusieurs copies du même message. Cela peut se produire parce que le moteur de scan antivirus divise chaque message qu'il scanne en plusieurs sections.

3. Si vous ne parvenez pas à renvoyer le message, il est possible que le compte de l'administrateur système sur le serveur Microsoft Exchange n'existe pas.

   a. À l'aide de l'Éditeur du Registre Windows, ouvrez l'entrée de Registre suivante sur le serveur :

      `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\VersionActuelle`

   b. Modifiez l'entrée comme suit :

      AVERTISSEMENT!

      La modification incorrecte du Registre peut gravement endommager le système. Avant d'apporter des modifications au Registre, sauvegardez toutes les données importantes de votre ordinateur.

      - `ResendMailbox {Administrator Mailbox}`

        Exemple : `admin@example.com`

      - `ResendMailboxDomain {Administrator's Domain}`

        Exemple : `exemple.com`

      - `ResendMailSender {Administrator's Email Account}`

        Exemple : `admin`

   c. Fermez l'Éditeur du Registre.

Maintenance des répertoires de quarantaine

Utilisez cette fonction pour supprimer manuellement ou automatiquement des messages en quarantaine. Cette fonction permet de supprimer tous les messages, les messages qui ont été renvoyés et les messages qui ne l'ont pas été.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.
4. Cliquez sur **Quarantaine** > **Maintenance**.

   Un nouvel écran s'affiche.
5. Mettez à jour les éléments suivants, si nécessaire :
   - **Activer la maintenance automatique** : disponible uniquement pour la maintenance automatique.
   - Fichiers à supprimer
     - **Tous les fichiers mis en quarantaine**
     - **Fichiers en quarantaine n'ayant jamais été renvoyés**
     - **Fichiers en quarantaine renvoyés au moins une fois**
   - **Action** : nombre de jours de stockage des messages. Par exemple, si la date est le 21 novembre et que vous avez saisi `10` dans le champ **Supprimer les fichiers sélectionnés datant de plus de**, Messaging Security Agent supprime tous les fichiers antérieurs au 11 novembre lorsque qu'il procède à la suppression automatique.
6. Cliquez sur **Enregistrer**.

Configuration des répertoires de quarantaine

Configurez les répertoires de quarantaine sur le serveur Microsoft Exchange. Le répertoire de quarantaine est exclu du scan.

Remarque

les répertoires de quarantaine reposent sur des fichiers et ne se trouvent pas dans la banque d'informations.

Messaging Security Agent met les messages électroniques en quarantaine en fonction des actions configurées. Voici les répertoires de quarantaine :

- **Antivirus** : met en quarantaine les messages électroniques qui contiennent des virus/programmes malveillants, spywares/graywares, vers, chevaux de Troie et autres menaces malveillantes.
- **Anti-spam** : met en quarantaine les messages de spam et de phishing.
- **Blocage des pièces jointes** : met en quarantaine les messages électroniques qui contiennent des pièces jointes faisant l'objet de restrictions.
- **Filtrage de contenu** : met en quarantaine les messages électroniques qui présentent du contenu faisant l'objet de restrictions.

Par défaut, tous les répertoires ont le même chemin (`<dossier d'installation de Messaging Security Agent>\storage\quarantine`). Vous pouvez modifier le chemin de chacun ou de tous les répertoires.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Quarantaine** > **Répertoire**.

   Un nouvel écran s'affiche.

5. Définissez le chemin des répertoires de quarantaine suivants :
   - **Antivirus**
   - **Anti-spam**
   - **Filtrage de contenu**
   - **Blocage des pièces jointes**
6. Cliquez sur **Enregistrer**.

Paramètres de notification pour les agents Messaging Security Agent

Worry-Free Business Security peut envoyer des notifications sous forme de messages électroniques pour diverses alertes.

Vous pouvez configurer certaines notifications de telle façon qu'elles ne s'appliquent qu'aux messages électroniques internes à l'aide de définitions de messages internes personnalisées. Ces définitions sont utiles si votre entreprise dispose d'au moins deux domaines et que vous souhaitez traiter les messages électroniques émanant de ces domaines en tant que messages internes. Par exemple, exemple.com et exemple.net.

Les destinataires de votre liste de définitions de messages internes recevront des messages de notifications si vous cochez la case **Ne pas notifier les destinataires externes** sous les paramètres de notifications relatifs à l'**antivirus**, le **filtrage de contenu** et le **blocage de pièce jointe**. Ne confondez pas la liste de définitions de messages internes avec la liste d'expéditeurs approuvés.

Pour éviter que les adresses e-mail des domaines externes soient considérées comme du spam, ajoutez les adresses e-mail externes dans les listes d'anti-spam **Expéditeurs approuvés**

À propos des définitions de messages internes personnalisées

Messaging Security Agent divise le trafic du courrier électronique en deux catégories de réseau : interne et externe. L'agent interroge le serveur Microsoft Exchange pour savoir comment les adresses internes et externes sont spécifiées. Toutes les adresses internes partagent un domaine commun, dont sont exclues toutes les adresses externes.

Par exemple, si l'adresse du domaine interne est « @trend_1.com », Messaging Security Agent classe les adresses du type « abc@trend_1.com » et « xyz@trend_1.com » comme adresses internes. L'agent classe toutes les autres adresses dans la catégorie externe, comme « abc@trend_2.com » et « jondoe@123.com ».

Vous ne pouvez définir qu'un domaine comme adresse interne de Messaging Security Agent. Si vous utilisez Microsoft Exchange System Manager pour changer votre adresse principale sur un serveur, Messaging Security Agent ne reconnaît pas la nouvelle adresse comme adresse interne, car il ne peut pas détecter que la règle du destinataire a changé.

Par exemple, votre entreprise dispose de deux adresses de domaine : @exemple_1.com et @exemple2.com. Vous définissez @exemple_1.com comme adresse principale. Messaging Security Agent considère que les messages électroniques correspondant à l'adresse principale sont internes (par exemple, abc@exemple_1.com ou xyz@exemple_1.com est interne). Vous utilisez ensuite Microsoft Exchange System Manager pour remplacer l'adresse principale par @exemple2.com. Cela signifie que Microsoft Exchange identifie désormais les adresses telles qu'abc@exemple2.com et xyz@exemple2.com comme des adresses internes.

Configuration des paramètres de notification pour les agents Messaging Security Agent

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.

3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Opérations** > **Paramètres de notification**.

   Un nouvel écran s'affiche.

5. Mettez à jour les éléments suivants, si nécessaire :

   - **Adresse électronique** : adresse à partir de laquelle Worry-Free Business Security enverra des messages de notification.
   - **Définition des messages internes**
     - **Par défaut** : Worry-Free Business Security traitera les e-mails du même domaine comme des e-mails internes.
     - **Personnalisée** : indiquez des adresses électroniques ou des domaines individuels à traiter comme des messages électroniques internes.

6. Cliquez sur **Enregistrer**.

Configuration de la maintenance des spams

L'écran **Maintenance des spams** vous permet de configurer les paramètres pour l'outil End User Quarantine (EUQ) ou pour la mise en quarantaine côté serveur.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.

4. Cliquez sur **Opérations** > **Maintenance des spams**.

   Un nouvel écran s'affiche.

5. Cliquez sur **Activer l'outil End User Quarantine**.

   Lorsque vous activez cet outil, un dossier de quarantaine est créé dans la boîte de réception de chaque client côté serveur et un dossier de `spam` apparaît dans l'arborescence de dossiers d'Outlook de l'utilisateur final. Après l'activation d'EUQ et la création des dossiers de spam, EUQ filtre les messages de spam et les déplace vers le dossier de spam de l'utilisateur. Pour plus de détails, voir *Gestion de l'outil End User Quarantine à la page 6-78*.

   Conseil

   Si vous sélectionnez cette option, Trend Micro recommande de désactiver l'option de la barre d'outils Trend Micro Anti-Spam sur les agents pour augmenter les performances des clients.

   Désactivez la case **Activer l'outil End User Quarantine** afin de désactiver l'outil End User Quarantine pour toutes les boîtes aux lettres de votre serveur Microsoft Exchange. Lorsque vous désactivez l'outil EUQ, les dossiers de messages de spam de l'utilisateur seront conservés, mais les messages identifiés comme spam ne seront pas déplacés vers les dossiers de messages de spam.

6. Cliquez sur **Créer un dossier de spam et supprimer les messages de spam** pour créer (immédiatement) des dossiers de messages de spam pour les clients de messagerie récemment créés et pour les clients de messagerie ayant supprimé leur dossier de spam. Pour les autres clients de messagerie, cet outil permet de supprimer les messages de spam datant d'un nombre de jours supérieur à celui spécifié dans le champ Paramètres du dossier spam du client.

7. Dans **Supprimer les spams datant de plus de {nombre} jours**, modifiez la durée pendant laquelle Messaging Security Agent conserve les spams. La valeur par défaut est 14 jours et le délai maximal est 30 jours.

8. Pour désactiver l'outil End User Quarantine pour les utilisateurs sélectionnés :

a. Sous **Liste d'exceptions de l'outil End User Quarantine**, saisissez l'adresse électronique de l'utilisateur final pour lequel vous souhaitez désactiver EUQ.

b. Cliquez sur **Ajouter**.

   L'adresse électronique de l'utilisateur final est ajoutée à la liste d'adresses pour lesquelles EUQ est désactivé.

   Pour supprimer un utilisateur final de la liste et restaurer le service EUQ, sélectionnez l'adresse électronique dans la liste et cliquez sur **Supprimer**.

9. Cliquez sur **Enregistrer**.

Gestion de l'outil End User Quarantine

Au cours de l'installation, Messaging Security Agent ajoute un dossier, `Messages de spam`, dans la boîte de réception de chaque utilisateur côté serveur. Lors de l'arrivée de messages de spam, le système les place en quarantaine dans ce dossier en respectant les règles de filtrage de spam prédéfinies par Messaging Security Agent. Les utilisateurs finaux peuvent accéder à ce dossier de spam afin d'ouvrir, de lire ou de supprimer les messages électroniques suspects. Voir *Configuration de la maintenance des spams à la page 6-76*.

Les administrateurs ont également la possibilité de créer le dossier de messages de spam sur Microsoft Exchange. Lorsqu'un administrateur crée un compte de messagerie, l'entité de boîte aux lettres n'est pas immédiatement créée sur le serveur Microsoft Exchange, mais sera créée dans les conditions suivantes :

- Un utilisateur final se connecte à la boîte aux lettres pour la première fois.
- Le premier message électronique arrive dans la boîte aux lettres.

L'administrateur doit commencer par créer l'entité de boîte aux lettres avant que EUQ ne crée le dossier de spam.

Dossier de spam côté client

Les utilisateurs finaux peuvent ouvrir les messages mis en quarantaine dans le dossier de spam. Lorsqu'ils ouvrent l'un de ces messages, deux boutons s'affichent sur le message lui-même : **Expéditeur approuvé** et **Afficher la liste d'expéditeurs approuvés**.

- Lorsqu'un utilisateur final ouvre un message électronique à partir du dossier de spam et clique sur le bouton **Expéditeur approuvé**, l'adresse de l'expéditeur de ce message électronique est ajoutée à la liste **Expéditeurs approuvés**.
- Si l'utilisateur final clique sur le bouton **Afficher la liste d'expéditeurs approuvés**, un autre écran s'ouvre et lui permet d'afficher et de modifier sa liste d'expéditeurs approuvés par adresse électronique ou par domaine.

Expéditeurs approuvés

Lorsque l'utilisateur final reçoit un courrier électronique dans le dossier de spam et clique sur le bouton **Expéditeur approuvé**, Messaging Security Agent déplace le message vers sa boîte de réception et ajoute l'adresse de l'expéditeur à sa liste personnelle d'expéditeurs approuvés. Messaging Security Agent consigne l'événement dans un journal.

Lorsque le serveur Microsoft Exchange reçoit des messages depuis les adresses figurant dans la liste des expéditeurs approuvés de l'utilisateur final, il les transmet à sa boîte de réception, quel que soit l'en-tête ou le contenu du message.

Remarque

Messaging Security Agent fournit également aux administrateurs une liste des expéditeurs approuvés et bloqués. Messaging Security Agent applique la liste des expéditeurs approuvés et bloqués de l'administrateur avant de tenir compte de celle de l'utilisateur final.

Fonction de gestion interne dans End User Quarantine

La fonction de gestion interne de Messaging Security Agent réalise les tâches suivantes toutes les 24 heures à 2h30 (heure par défaut).

- Suppression automatique des messages de spam
- Nouvelle génération du dossier de spam lorsqu'il est supprimé
- Création des dossiers de spam pour les comptes de messagerie récemment créés
- Maintenance des règles de messages électroniques

La fonction de gestion interne fait partie intégrante de l'agent Messaging Security Agent et ne requiert aucune configuration.

Assistance/Débogage Trend Micro

L'assistance/le débogage vous aide à déboguer ou simplement à communiquer l'état des processus de Messaging Security Agent. Lorsque vous rencontrez des difficultés inattendues, vous pouvez utiliser le débogueur pour créer des rapports de bogues et les envoyer pour analyse à l'assistance technique de Trend Micro.

Chaque Messaging Security Agent insère des messages dans le programme et enregistre l'action dans des fichiers journaux lors de son exécution. Vous pouvez faire suivre les journaux au personnel de l'assistance technique de Trend Micro pour les aider à déboguer le flux du programme concerné dans votre environnement.

Utilisez le débogueur pour générer des journaux sur les modules suivants :

- Service principal de Messaging Security Agent
- Serveur de configuration à distance de Messaging Security Agent
- Messaging Security Agent System Watcher
- Virus Scan API (VSAPI)
- Protocole SMTP (Simple Mail Transfer Protocol)
- Common Gateway Interface (CGI)

Par défaut, MSA conserve les journaux dans le répertoire suivant :

`<dossier d'installation de Messaging Security Agent>\Debug`.

Affichez la sortie à l'aide d'un éditeur de texte.

Génération de rapports de débogage système

Générez des rapports de débogage pour aider l'assistance de Trend Micro à résoudre votre problème.

Procédure

1. Accédez à **Dispositifs**.
2. Sélectionnez un agent Messaging Security Agent.
3. Cliquez sur **Configurer la stratégie**.

   Un nouvel écran s'affiche.
4. Cliquez sur **Opérations** > **Débogueur système**.

   Un nouvel écran s'affiche.
5. Sélectionnez les modules à surveiller :
   - **Service principal** de Messaging Security Agent
   - **Serveur de configuration à distance** de Messaging Security Agent
   - **System Watcher** de Messaging Security Agent
   - **VSAPI (Virus Scan API)** dans Exchange Server 2003, 2007 ou 2010
   - **Scan au niveau du magasin** dans Exchange Server 2013
   - **Protocole SMTP (Simple Mail Transfer Protocol)** dans Exchange Server 2003
   - **Service de transport** dans Exchange Server 2007, 2010 ou 2013
   - **Common Gateway Interface (CGI)**

6. Cliquez sur **Appliquer**.

   Le débogueur commence à recueillir des données pour les modules sélectionnés.

Surveillance en temps réel

La surveillance en temps réel affiche les informations actuelles sur le serveur Microsoft Exchange sélectionné et son agent Messaging Security Agent. Elle fournit des informations sur les messages scannés et les statistiques de la protection y compris le nombre de virus et de spam détectés, de pièces jointes bloquées et de violations de contenu. Elle permet également de s'assurer que l'agent fonctionne correctement.

Utilisation de la surveillance en temps réel

Procédure

1. Pour accéder à la surveillance en temps réel depuis la console Web :
   a. Accédez à **Dispositifs**.
   b. Sélectionnez un agent Messaging Security Agent.
   c. Cliquez sur **Configurer la stratégie**.

      Un nouvel écran s'affiche.

   d. Cliquez sur le lien **Surveillance en temps réel** dans la partie supérieure droite de l'écran.
2. Pour accéder à la surveillance en temps réel depuis le menu Démarrer de Windows, cliquez sur **Tous les programmes** > **Trend Micro Messaging Security Agent** > **Surveillance en temps réel**.
3. Cliquez sur **Réinitialiser** pour remettre les statistiques de la protection à zéro.

4. Cliquez sur **Effacer le contenu** pour supprimer les informations obsolètes sur les messages scannés.

Ajout d'un avis de non-responsabilité aux e-mails sortants

Vous pouvez ajouter un avis de non-responsabilité aux e-mails sortants.

Procédure

1. Créez un fichier texte et saisissez le texte de l'avis de non-responsabilité.
2. Modifiez les clés suivantes dans le registre :
   - Première clé :

     Chemin : `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\VersionActuelle`

     Clé : `EnableDisclaimer`

     Type : `REG_DWORD`

     Valeur des données : `0 - Désactiver, 1 - Activer`
   - Deuxième clé :

     Chemin : `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\VersionActuelle`

     Clé : `DisclaimerSource`

     Type : `REG_SZ`

     Valeur : chemin complet du fichier contenant l'avis de non-responsabilité.

     Par exemple, `C:\Mes documents\Avis de non-responsabilité.txt`

Remarque

Worry-Free Business Security détectera par défaut si un e-mail sortant est envoyé à des domaines internes ou externes, et ajoutera un avis de non-responsabilité à chaque e-mail envoyé aux domaines externes. L'utilisateur peut écraser les paramètres par défaut et ajouter un avis de non-responsabilité à chaque e-mail sortant sauf aux domaines compris dans la clé de registre suivante :

- Troisième clé :

  Chemin : `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\VersionActuelle`

  Clé : `InternalDomains`

  Type : `REG_SZ`

  Valeur : saisissez les noms de domaines qui doivent être exclus. Utilisez un point-virgule (;) pour séparer plusieurs éléments.

  Par exemple : `domaine1.org;domaine2.org`

  Remarque

  Les noms de domaines sont ici les noms DNS des serveurs Exchange.

Chapitre 7

Gestion des scans

Ce chapitre décrit comment exécuter des scans sur les agents Security Agent et Messaging Security Agent (Advanced uniquement) pour protéger votre réseau et vos clients contre les menaces.

À propos des scans

Durant un scan, le moteur de scan Trend Micro s'associe au fichier de signatures afin de réaliser le premier niveau de détection en utilisant un processus appelé correspondance de signature. Comme chaque menace contient une signature ou une chaîne de caractères révélatrice unique la distinguant de tous les autres codes, des parties inertes de ce code sont capturées dans le fichier de signatures. Le moteur compare alors certaines parties de chaque fichier scanné aux signatures qui se trouvent dans le fichier de signatures, afin de rechercher les correspondances.

Lorsque le moteur de scan détecte un fichier contenant une menace, il exécute une action telle que nettoyer, mettre en quarantaine, supprimer ou remplacer par un texte/fichier (Advanced uniquement). Vous pouvez personnaliser ces actions lorsque vous définissez vos tâches de scan.

Worry-Free Business Security met en œuvre **trois types de scans**. Chaque scan a un but et une fonction qui lui sont propres, mais tous sont configurés de façon similaire.

- Scan en temps réel : Voir *Scan en temps réel à la page 7-3* pour obtenir des informations détaillées.
- Scan manuel : Voir *Scan manuel à la page 7-3* pour obtenir des informations détaillées.
- Scan programmé : Voir *Scan programmé à la page 7-7* pour obtenir des informations détaillées.

Les agents Security Agent utilisent l'une ou l'autre des deux méthodes de scan suivantes :

- Smart scan
- Scan traditionnel

Voir *Méthodes de scan à la page 5-3* pour obtenir des informations détaillées.

Scan en temps réel

Le scan en temps réel s'effectue en continu.

Chaque fois qu'un fichier est ouvert, téléchargé, copié ou modifié, le scan en temps réel dans l'agent **Security Agent** s'exécute pour détecter les menaces éventuelles. Pour obtenir des informations sur le scan en temps réel, voir *Configuration du scan en temps réel pour les agents Security Agent à la page 5-8*.

Dans le cas de messages électroniques, le scan en temps réel dans l'agent **Messaging Security Agent** (Advanced uniquement) protège tous les points d'entrée de virus connus grâce au scan en temps réel de tous les messages entrants, des messages SMTP, des documents publiés dans les dossiers publics et des fichiers répliqués à partir d'autres serveurs Microsoft Exchange. Pour obtenir des informations sur le scan en temps réel, voir *Configuration du scan en temps réel pour des agents Messaging Security Agent à la page 6-6*.

Scan manuel

Le scan manuel est un scan à la demande.

Le scan manuel sur les outils **Security Agent** permet d'éliminer les menaces présentes dans les fichiers, mais aussi de supprimer d'anciennes infections, le cas échéant, pour limiter les risques de réinfection.

Le scan manuel sur les outils **Messaging Security Agent** (Advanced uniquement) scanne tous les fichiers de la banque d'informations de votre serveur Microsoft Exchange.

Le temps nécessaire à l'exécution complète du scan dépend des ressources matérielles du client et du nombre de fichiers à scanner. Le déroulement d'un scan manuel peut être interrompu par l'administrateur Security Server si le scan a été lancé à distance depuis la console Web, ou par l'utilisateur s'il a été lancé directement sur l'ordinateur client.

Conseil

Trend Micro recommande d'exécuter des scans manuels après une épidémie virale.

Exécution de scans manuels

Cette procédure décrit comment les administrateurs Security Server peuvent lancer un scan manuel sur les agents **Security Agent** et **Messaging Security Agent** (Advanced uniquement) à partir de la console Web.

Remarque

Les opérations de scan manuel peuvent également être lancées directement depuis les clients ; pour cela, l'utilisateur doit effectuer un clic droit sur l'icône Security Agent située dans la barre des tâches Windows et cliquer sur **Scan immédiat**. Un scan manuel ne peut pas être lancé directement depuis un serveur Microsoft Exchange.

Procédure

1. Accédez à **Scans** > **Scan manuel**.
2. Personnalisez les paramètres de scan avant de lancer un scan manuel (facultatif).

Instructions et remarques	Paramètres de scan recommandés
Pour personnaliser les paramètres de scan pour l'agent **Security Agent**, cliquez sur un groupe de postes de travail ou de serveurs. Voir *Cibles de scan et actions des agents Security Agent à la page 7-10*. **Remarque** Les paramètres de scan pour les agents Security Agent sont également utilisés lorsque les utilisateurs lancent un scan manuel directement depuis les clients. Toutefois, si vous autorisez les utilisateurs à configurer leurs propres paramètres de scan, ce sont ces paramètres personnalisés qui seront pris en compte pendant l'opération.	Cible • Tous les fichiers scannables : Inclut tous les fichiers scannables. Les fichiers impossibles à analyser sont des fichiers protégés par un mot de passe, chiffrés ou dépassant les restrictions de scan définies par l'utilisateur • Scanner les fichiers compressés jusqu'à la couche 1 : scanne les fichiers compressés qui disposent d'une seule couche de compression. La valeur par défaut est « désactivé » pour le groupe de serveurs par défaut et « activé » pour le groupe de postes de travail par défaut. Exclusions • Ne pas scanner les répertoires d'installation des produits Trend Micro Paramètres avancés • Modifier la liste des spywares/graywares approuvés (pour l'anti-spyware uniquement)

Instructions et remarques	Paramètres de scan recommandés
Pour personnaliser les paramètres de scan de l'agent **Messaging Security Agent**, développez un agent et cliquez sur les paramètres suivants : • **Antivirus** : cliquez sur cette option pour que l'agent recherche des virus et autres programmes malveillants. Voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*. • **Filtrage de contenu** : cliquez sur cette option pour que l'agent recherche le contenu inapproprié dans les e-mails. Voir *Gestion des règles de filtrage de contenu à la page 6-17*. • **Blocage des pièces jointes** : cliquez sur cette option pour que l'agent recherche des violations de règles dans les pièces jointes des messages. Voir *Configuration du blocage des pièces jointes à la page 6-50*.	• L'agent scanne tous les fichiers scannables. Il inclut dans le scan les corps de message des messages électroniques. • Lorsque l'agent détecte un fichier contenant un virus ou tout autre programme malveillant, il nettoie le fichier. Lorsque le nettoyage du fichier est impossible, il remplace son contenu par un texte/un fichier. • Lorsque l'agent détecte un fichier contenant un cheval de Troie ou un ver, il remplace le cheval de Troie ou le ver par un texte ou un fichier. • Lorsque l'agent détecte un fichier contenant un utilitaire de compression, il remplace ce dernier par un texte ou un fichier. • L'agent ne nettoie pas les fichiers compressés infectés. Cela réduit le temps requis pour le scan en temps réel.

3. Sélectionner les groupes ou les agents Messaging Security Agent pour le scan
4. Cliquez sur **Scan immédiat**.

   Security Server envoie une notification aux agents leur demandant d'exécuter un scan manuel. L'écran Résultats de la notification de scan présente les agents ayant reçu la notification et ceux ne l'ayant pas reçue.
5. Pour interrompre un scan en cours; cliquez sur **Arrêter le scan**.

   Security Server envoie une autre notification aux agents leur demandant d'interrompre le scan manuel. L'écran Résultats de la notification de l'arrêt de scan présente les agents ayant reçu la notification et ceux ne l'ayant pas reçue. Les agents Security Agent peuvent ne pas recevoir la

notification s'ils se sont déconnectés depuis le début de l'opération ou si des interruptions réseau se sont produites.

Scan programmé

Un scan programmé est similaire à un scan manuel, mais scanne tous les fichiers et messages électroniques (Advanced uniquement) à l'heure prévue et selon la fréquence configurée. Utilisez les scans programmés pour automatiser les routines de scan sur les clients et améliorer l'efficacité de votre gestion des menaces.

Conseil

Exécutez les scans programmés en dehors des heures de pointe pour limiter les perturbations potentielles subies par les utilisateurs et le réseau.

Configuration des scans programmés

Trend Micro recommande de ne pas programmer un scan en même temps qu'une mise à jour programmée. Cela peut entraîner un arrêt prématuré du scan programmé. De la même manière, si vous commencez un scan manuel lors de l'exécution d'un scan programmé, ce dernier s'interrompt, mais son exécution reprend conformément à son calendrier de programmation.

Procédure

1. Accédez à **Scans** > **Scan programmé**.
2. Cliquez sur l'onglet **Programmation**.
   a. Configurez la fréquence (quotidienne, hebdomadaire ou mensuelle) et l'heure du scan. Chaque groupe ou Messaging Security Agent peut avoir sa propre programmation.

Remarque

Pour les scans mensuels programmés, si vous sélectionnez 31, 30 ou 29 jours et qu'un mois compte un nombre inférieur de jours, le scan ne s'exécutera pas ce mois-là.

b. (Facultatif) Sélectionnez **Arrêter le client à l'issue d'un scan programmé**.

c. Cliquez sur **Enregistrer**.

3. Cliquez sur l'onglet **Paramètres** et configurez les paramètres de scan programmé requis.

Instructions et remarques	Paramètres de scan recommandés
Pour personnaliser les paramètres de scan pour l'agent **Security Agent**, cliquez sur un groupe de postes de travail ou de serveurs. Voir *Cibles de scan et actions des agents Security Agent à la page 7-10*. **Remarque** Si vous autorisez les utilisateurs à configurer leurs propres paramètres de scan, ces derniers seront utilisés lors du scan.	Cible • Tous les fichiers scannables :Inclut tous les fichiers scannables. Les fichiers impossibles à analyser sont des fichiers protégés par un mot de passe, chiffrés ou dépassant les restrictions de scan définies par l'utilisateur • Scanner les fichiers compressés jusqu'à la couche 2 :scanne les fichiers compressés qui disposent de deux couches de compression.
	Exclusions • Ne pas scanner les répertoires d'installation des produits Trend Micro
	Paramètres avancés • Modifier la liste des spywares/graywares approuvés (pour l'anti-spyware uniquement)

Instructions et remarques	Paramètres de scan recommandés
Pour personnaliser les paramètres de scan de l'agent **Messaging Security Agent**, développez un agent et cliquez sur les paramètres suivants : • **Antivirus** :cliquez sur cette option pour que l'agent recherche des virus et autres programmes malveillants. Voir *Cibles du scan et actions des agents Messaging Security Agent à la page 7-18*. • **Filtrage de contenu** :cliquez sur cette option pour que l'agent recherche le contenu inapproprié dans les e-mails. Voir *Gestion des règles de filtrage de contenu à la page 6-17*. • **Blocage des pièces jointes** :cliquez sur cette option pour que l'agent recherche des violations de règles dans les pièces jointes des messages. Voir *Configuration du blocage des pièces jointes à la page 6-50*.	• L'agent effectue un scan chaque dimanche à 5:00. • Configurez cette programmation afin que le scan s'exécute lors d'une période de faible activité pour vos clients. L'agent scanne tous les fichiers scannables. Il inclut dans le scan les corps de message des messages électroniques. • Lorsque l'agent détecte un fichier contenant un virus ou tout autre programme malveillant, il nettoie le fichier. Lorsque le nettoyage du fichier est impossible, il remplace son contenu par un texte/un fichier. • Lorsque l'agent détecte un fichier contenant un cheval de Troie ou un ver, il remplace le cheval de Troie ou le ver par un texte ou un fichier. • Lorsque l'agent détecte un fichier contenant un utilitaire de compression, il le remplace par un texte/fichier. • L'agent ne nettoie pas les fichiers compressés infectés.

4. Sélectionnez les groupes ou les agents Messaging Security Agent appliquant les paramètres de scan programmé.

Remarque

Pour désactiver le scan programmé, décochez la case du groupe ou du Messaging Security Agent.

5. Cliquez sur **Enregistrer**.

Cibles de scan et actions des agents Security Agent

Configurez les paramètres suivants pour chaque type de scan (scan manuel, scan programmé ou scan en temps réel) :

Onglet Cible

Sélectionnez une méthode :

- **Tous les fichiers scannables** : inclut tous les fichiers scannables. Les fichiers impossibles à analyser sont des fichiers protégés par un mot de passe, chiffrés ou dépassant les restrictions de scan définies par l'utilisateur

  Remarque

  Cette option offre le meilleur niveau de sécurité possible. Cependant, le scan de chaque fichier nécessite beaucoup de temps et de ressources et peut s'avérer redondant dans certaines situations. Par conséquent, il peut être utile de limiter le nombre de fichiers que l'agent doit inclure dans le scan.

- **IntelliScan utilise un système d'identification du « véritable type de fichier »** : scanne les fichiers d'après le véritable type de fichier. Voir *IntelliScan à la page D-2*.

- **Scanner les fichiers dotés des extensions suivantes** : spécifiez manuellement les fichiers à scanner en fonction de leur extension. Séparez les entrées par une virgule.

Sélectionnez un modèle de déclenchement de scan :

- **Lecture** : scanne les fichiers dont le contenu est lu ; les fichiers sont lus lorsqu'ils sont ouverts, exécutés, copiés ou déplacés.

- **Écriture** : scanne les fichiers dont le contenu est en cours d'écriture ; le contenu d'un fichier est écrit lorsque le fichier est modifié, enregistré, téléchargé ou copié depuis un autre emplacement.

- **Lecture ou écriture**

Exclusions de scan

Les paramètres suivants sont configurables :

- Activer ou désactiver les exclusions
- Exclure les répertoires de produit Trend des scans
- Exclure d'autres répertoires des scans

  Tous les sous-répertoires contenus dans le chemin d'accès au répertoire spécifié sont également exclus
- Exclure des noms de fichier ou des noms de fichier avec chemin d'accès complet des scans
- Exclure les extensions de fichier

  Les caractères de substitution tels que « * » ne sont pas autorisés pour les extensions de fichier

Remarque

(Advanced uniquement) Si Microsoft Exchange Server est installé sur le client, Trend Micro vous recommande d'exclure du scan tous les dossiers Microsoft Exchange Server. Pour exclure du scan les dossiers de serveur Microsoft Exchange de façon globale, accédez à **Administration** > **Paramètres généraux** > **Poste de travail/serveur {onglet}** > **Paramètres de scan généraux**, puis sélectionnez **Exclure les dossiers de serveur Microsoft Exchange lors d'une installation sur serveur Microsoft Exchange**.

Paramètres avancés

TYPE DE SCAN	OPTION
Scan en temps réel	**Scanner les messages POP3** : par défaut, le scan de la messagerie ne peut traiter que les nouveaux messages envoyés via le port 110 dans les dossiers Boîte de réception et Courrier indésirable. Il ne prend pas en charge le protocole sécurisé POP3 (SSL-POP3). • Microsoft Outlook 2007, 2010 ou 2013 • Mozilla Thunderbird 1.5 ou version ultérieure Le scan de la messagerie ne peut pas détecter les risques de sécurité des messages IMAP. Utilisez Messaging Security Agent (Advanced uniquement) pour détecter les risques liés à la sécurité et le spam dans les messages IMAP.
Scan en temps réel, scan manuel	**Scanner les lecteurs mappés et les dossiers partagés sur le réseau** : sélectionnez cette option pour scanner les répertoires physiquement situés sur d'autres ordinateurs, mais mappés sur l'ordinateur local.
Scan en temps réel	**Scanner les disquettes pendant l'arrêt du système**
Scan en temps réel	**Activer IntelliTrap** : IntelliTrap détecte les codes malveillants tels que les logiciels robots dans les fichiers compressés. Voir *IntelliTrap à la page D-3*.
Scan en temps réel	**Mettre en quarantaine les variantes de programmes malveillants détectées en mémoire** : si le scan en temps réel et la surveillance des comportements sont activés et que cette option est sélectionnée, une recherche portant sur les programmes malveillants compressés est lancée dans la mémoire de processus en cours d'exécution. Les programmes malveillants compressés qui sont détectés par la surveillance des comportements sont mis en quarantaine.
le scan en temps réel, le scan manuel et le scan programmé.	**Scanner les fichiers compressés jusqu'à la couche __** : un fichier compressé comporte une couche pour chaque compression. Si un fichier infecté a été compressé sur plusieurs couches, le scan doit porter sur le nombre de couches spécifié pour que l'infection soit détectée. Cependant, le scan sur plusieurs couches exige davantage de ressources et de temps.

TYPE DE SCAN	OPTION
le scan en temps réel, le scan manuel et le scan programmé.	**Modifier la liste des spywares/graywares approuvés** : ce paramètre ne peut pas être configuré à partir de la console de l'agent.
Scan manuel, scan programmé	**Utilisation de l'UC/Vitesse du scan** : Security Agent peut s'interrompre entre chaque fichier scanné. Sélectionnez l'une des options suivantes : • **Élevé** : aucune interruption entre les scans • **Moyen** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 50% et pas d'interruption si elle est de 50% ou moins • **Faible** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 20% et pas d'interruption si elle est de 20% ou moins
Scan manuel, scan programmé	**Exécuter un nettoyage avancé** : Security Agent interrompt les activités de rogueware, connu également sous le nom de « FakeAV ». L'agent utilise également les règles de nettoyage avancé pour détecter et bloquer de manière proactive les applications présentant un comportement de faux antivirus. **Remarque** Tout en assurant une protection proactive, le nettoyage avancé génère également un nombre élevé de faux-positifs.

Liste des spywares/graywares approuvés

Certaines applications sont classées par Trend Micro comme spywares/graywares, non pas parce qu'elles risquent d'endommager le système sur lequel elles sont installées, mais parce qu'elles peuvent exposer le client ou le réseau à des attaques de pirates ou de programmes malveillants.

Worry-Free Business Security inclut une liste d'applications potentiellement dangereuses et est défini par défaut pour empêcher ces applications de s'exécuter au niveau des clients.

Si les clients doivent exécuter une application classée par Trend Micro comme spyware/grayware, vous devez ajouter le nom de cette application à la liste des spywares/graywares approuvés.

Onglet Action

Voici la liste des actions que les agents Security Agent peuvent effectuer pour lutter contre les virus/programmes malveillants :

TABLEAU 7-1. Actions de scan antivirus/programmes malveillants

ACTION	DESCRIPTION
Supprimer	Supprime un fichier infecté.
Quarantaine	Renomme puis déplace le fichier infecté vers un répertoire de quarantaine temporaire sur le client. Les agents Security Agent envoient ensuite les fichiers en quarantaine vers le répertoire de quarantaine spécifié, qui se trouve par défaut sur le serveur Security Server. Security Agent chiffre les fichiers en quarantaine envoyés à ce répertoire. Si vous devez restaurer un fichier mis en quarantaine, utilisez l'outil VSEncrypt.
Nettoyer	Nettoie le fichier infecté avant d'autoriser l'accès complet au fichier. Si le fichier n'est pas nettoyable, Security Agent effectue une seconde action qui peut être l'une des suivantes : Mettre en quarantaine, Supprimer, Renommer et Ignorer Cette action peut être effectuée sur tous les types de programmes malveillants, à l'exception des virus/programmes malveillants probables. **Remarque** Certains fichiers ne sont pas nettoyables. Pour plus de détails, voir *Fichiers non nettoyables à la page D-27*.

Action	Description
Renommer	Remplace l'extension du fichier infecté par « `vir` ». Initialement, les utilisateurs ne peuvent pas ouvrir le fichier renommé. Ils peuvent l'ouvrir s'ils associent le fichier à une application déterminée. Le virus/programme malveillant peut s'exécuter lors de l'ouverture du fichier infecté renommé.
Ignorer	Exécuté uniquement lors du scan manuel et du scan programmé. Security Agent ne peut pas utiliser cette action lors du scan en temps réel, car l'absence d'action lorsqu'une tentative d'ouverture ou d'exécution d'un fichier infecté est détectée permettra au virus/programme malveillant de s'exécuter. Toutes les autres actions de scan peuvent être utilisées lors du scan en temps réel.
Refuser l'accès	Effectué uniquement lors du scan en temps réel. Lorsque Security Agent détecte une tentative d'ouverture ou d'exécution d'un fichier infecté, il bloque immédiatement l'opération. Les utilisateurs peuvent supprimer manuellement le fichier infecté.

L'action de scan que Security Agent effectue dépend du type de scan qui a détecté le spyware/grayware. Si des actions spécifiques peuvent être configurées pour chaque type de virus/programme malveillant, une seule action peut l'être pour tous les types de spyware/grayware. Par exemple, lorsque Security Agent détecte un type de spyware/grayware lors d'un scan manuel (type de scan), il nettoie (action) les ressources système affectées.

Voici la liste des actions que les agents Security Agent peuvent effectuer pour lutter contre les spywares/graywares malveillants :

Tableau 7-2. Actions de scan anti-spywares/graywares

Action	Description
Nettoyer	Met fin aux processus ou supprime les registres, fichiers, cookies et raccourcis.

Action	Description
Ignorer	N'effectue aucune action sur les composants de spyware/grayware détectés, mais consigne la détection de spyware/grayware dans les journaux. Cette action est possible uniquement lors du scan manuel et du scan programmé. Lors du scan en temps réel, l'action est « Refuser l'accès ». Security Agent n'effectue aucune action si le spyware/grayware détecté fait partie de la liste approuvée.
Refuser l'accès	refuse l'accès (copie, ouverture) aux composants de spywares/graywares détectés. Cette action ne peut être effectuée que lors d'un scan en temps réel. Lors d'un scan manuel ou d'un scan programmé, l'action est « Ignorer ».

ActiveAction

À chaque type de virus/programme malveillant correspond une action de scan différente. Pour personnaliser les actions de scan, vous devez posséder les connaissances nécessaires sur les virus/programmes malveillants. Cette tâche peut être fastidieuse. L'Security Agent utilise ActiveAction pour pallier à ces problèmes.

ActiveAction est un ensemble d'actions de scan pré-configurées, destinées à lutter contre les virus et les programmes malveillants. Si les actions de scan ne vous sont pas familières ou si vous ignorez quelle action est la mieux adaptée à tel ou tel type de virus ou programme malveillant, l'utilisation de l'outil ActiveAction est recommandée.

ActiveAction offre les avantages suivants :

- ActiveAction applique les actions de scan recommandées par Trend Micro. Vous ne perdez plus votre temps à configurer vous-même les actions de scan.
- Les créateurs de virus/programmes malveillants modifient en permanence la manière dont leurs virus attaquent les Endpoints. Les paramètres d'ActiveAction sont mis à jour pour assurer une protection contre les menaces et les méthodes d'attaques les plus récentes des virus /programmes malveillants.

Le tableau suivant illustre comment ActiveAction traite chaque type de virus/programme malveillant :

TABLEAU 7-3. Actions de scan recommandées par Trend Micro contre les virus et les programmes malveillants

TYPE DE VIRUS/ PROGRAMMES MALVEILLANTS	SCAN EN TEMPS RÉEL		SCAN MANUEL/SCAN PROGRAMMÉ	
	PREMIÈRE ACTION	DEUXIÈME ACTION	PREMIÈRE ACTION	DEUXIÈME ACTION
Canular	Quarantaine	Supprimer	Quarantaine	Supprimer
Cheval de Troie/ Vers	Quarantaine	Supprimer	Quarantaine	Supprimer
Utilitaire de compression	Quarantaine	N/A	Quarantaine	N/A
Virus/programmes malveillants probables	Ignorer	N/A	Ignorer ou action configurée par l'utilisateur	N/A
Virus	Nettoyer	Quarantaine	Nettoyer	Quarantaine
Virus de test	Refuser l'accès	N/A	N/A	N/A
Autre programme malveillant	Nettoyer	Quarantaine	Nettoyer	Quarantaine

Remarque

- Certains fichiers ne sont pas nettoyables. Pour plus de détails, voir *Fichiers non nettoyables à la page D-27*.
- ActiveAction n'est pas disponible pour le scan anti-spywares/graywares.
- La valeur par défaut de ces paramètres peut changer à mesure que des nouveaux fichiers de signatures sont mis à disposition.

Paramètres avancés

Type de scan	Option
Scan en temps réel, scan programmé	**Afficher un message d'alerte sur le poste de travail ou le serveur lorsqu'un virus/programme espion est détecté**
Scan en temps réel, scan programmé	**Afficher un message d'alerte sur le poste de travail ou le serveur lors de la détection d'un virus ou d'un programme espion potentiel**
le scan manuel, le scan en temps réel et le scan programmé.	**Exécuter le nettoyage lors de la détection d'un programme malveillant ou d'un virus potentiel** : disponible uniquement si vous avez choisi ActiveAction et personnalisé l'action pour les virus/programmes malveillants probables.

Cibles du scan et actions des agents Messaging Security Agent

Configurez les paramètres suivants pour chaque type de scan (scan manuel, scan programmé ou scan en temps réel) :

Onglet **Cible**

- Cibles du scan
- Paramètres de recherche des menaces supplémentaires
- Exclusions de scan

Onglet **Action**

- Actions de scan/ActiveAction
- Notifications
- Paramètres avancés

Cibles du scan

Sélectionnez les cibles du scan :

- **Tous les fichiers en pièce jointe** : seuls les fichiers protégés par mot de passe ou chiffrés sont exclus.

Remarque

Cette option offre le meilleur niveau de sécurité possible. Cependant, le scan de chaque fichier nécessite beaucoup de temps et de ressources et peut s'avérer redondant dans certaines situations. Par conséquent, il peut être utile de limiter le nombre de fichiers que l'agent doit inclure dans le scan.

- **IntelliScan** : scanne les fichiers d'après le véritable type de fichier. Voir *IntelliScan à la page D-2*.

- **Types de fichiers spécifiques** : Worry-Free Business Security scannera les fichiers des types sélectionnés et avec les extensions choisies. Séparez les entrées multiples par un point-virgule (;).

Sélectionnez d'autres options :

- **Activer IntelliTrap** : IntelliTrap détecte les codes malveillants tels que les logiciels robots dans les fichiers compressés. Voir *IntelliTrap à la page D-3*.

- **Scanner le corps du message** : scanne le corps d'un message électronique qui pourrait contenir des menaces incorporées.

Paramètres de recherche des menaces supplémentaires

Sélectionnez d'autres menaces à rechercher par l'agent. Pour plus de détails sur ces menaces, consultez *Description des menaces à la page 1-9*.

Sélectionnez des options supplémentaires :

- **Sauvegarder le fichier infecté avant nettoyage** : Worry-Free Business Security effectue une sauvegarde de la menace avant le nettoyage. Le fichier sauvegardé est chiffré et stocké dans le répertoire suivant sur le client :

```
<dossier d'installation de Messaging Security Agent>
\storage\backup
```

Vous pouvez modifier ce répertoire dans la sous-section **Paramètre de sauvegarde** de la section **Options avancées**.

Pour déchiffrer le fichier, voir *Restauration des fichiers chiffrés à la page 14-19*

- **Ne pas nettoyer les fichiers compressés infectés afin d'optimiser les performances.**

Exclusions de scan

Dans l'onglet **Cible**, accédez à la section **Exclusions** et choisissez un des critères suivants, que l'agent utilisera lors de l'exclusion des messages électroniques des scans :

- **La taille du corps du message dépasse** : Messaging Security Agent scanne uniquement les messages électroniques dont la taille du corps de message est inférieure ou égale au nombre spécifié.
- **La taille de la pièce jointe dépasse** : Messaging Security Agent scanne uniquement les messages électroniques dont la taille des pièces jointes est inférieure ou égale au nombre spécifié.

Conseil

Trend Micro recommande une limite de 30 Mo.

- **Le nombre de fichiers décompressés dépasse** : Lorsque le nombre de fichiers décompressés dans le fichier compressé dépasse ce nombre, Messaging Security Agent scanne uniquement les fichiers ne dépassant pas la limite fixée par cette option.
- **La taille des fichiers décompressés dépasse** : Messaging Security Agent scanne uniquement les fichiers compressés dont la taille est inférieure ou égale à ce nombre après décompression.
- **Le nombre de couches de compression dépasse** : Messaging Security Agent scanne uniquement les fichiers compressés dont le nombre de couches de compression est inférieur ou égal au nombre spécifié. Par exemple, si vous limitez le nombre de couches de compression à 5, Messaging Security Agent scanne les 5 premières couches des fichiers

compressés, mais ne scanne pas les fichiers de 6 couches de compression ou plus.

- **La taille des fichiers décompressés équivaut à « x » fois la taille des fichiers compressés** : Messaging Security Agent scanne uniquement les fichiers compressés lorsque le rapport de la taille du fichier décompressé sur la taille du fichier compressé est inférieur à ce nombre. Cette fonction empêche Messaging Security Agent de scanner un fichier compressé susceptible de causer une attaque de refus de service (DoS). Une attaque de refus de service (DoS) se produit lorsque les ressources d'un serveur de messagerie sont surchargées de tâches inutiles. Empêcher Messaging Security Agent de scanner des fichiers qui s'avèrent très volumineux après décompression permet d'éviter ce problème.

  Exemple : Dans le tableau suivant, la valeur « x » saisie est 100.

Taille du fichier (non compressé)	Taille du fichier (non compressé)	Résultat
500 Ko	10 Ko (rapport de 50:1)	Scanné
1 000 Ko	10 Ko (rapport de 100:1)	Scanné
1 001 Ko	10 Ko (le rapport dépasse 100:1)	Non scanné *
2000 Ko	10 Ko (rapport de 200:1)	Non scanné *

  * Messaging Security Agent exécute l'action configurée pour les fichiers exclus.

Actions de scan

Les administrateurs peuvent configurer Messaging Security Agent de façon qu'il entreprenne des actions en fonction du type de menace que représentent les virus, les programmes malveillants, les chevaux de Troie et les vers. Si vous utilisez des actions personnalisées, définissez une action pour chaque type de menace.

TABLEAU 7-4. Actions personnalisées de Messaging Security Agent

ACTION	DESCRIPTION
Nettoyer	Supprime le code malveillant dans le corps du message et les pièces jointes qui sont infectées. Le texte restant du message, les éventuels fichiers non infectés et les fichiers nettoyés sont envoyés aux destinataires désignés. Trend Micro recommande d'utiliser l'action de scan par défaut Nettoyer pour les virus/programmes malveillants. Dans certains cas, Messaging Security Agent ne peut pas nettoyer le fichier. Au cours d'un scan manuel ou programmé, Messaging Security Agent met à jour la banque d'informations et remplace le fichier par celui qui a été nettoyé.
Remplacer par un texte/fichier	Supprime le contenu infecté et le remplace par du texte ou un fichier. Le message électronique est envoyé au bon destinataire, mais le texte de remplacement signale que le contenu d'origine a été infecté et remplacé. Pour le filtrage de contenu/prévention de la perte de données, vous pouvez uniquement remplacer du texte dans les champs Corps ou Pièce jointe (mais pas dans les champs De, À, Cc ou Objet).
Mettre la totalité du message en quarantaine	(Scan en temps réel uniquement) Seul le contenu infecté est mis en quarantaine dans le répertoire de quarantaine et le destinataire reçoit le message sans ce contenu. Pour le filtrage de contenu, la prévention de la perte de données et le blocage des pièces jointes, il déplace la totalité du message vers le répertoire de quarantaine.
Mettre en quarantaine une partie du message	(Scan en temps réel uniquement) Seul le contenu infecté ou filtré est mis en quarantaine dans le répertoire de quarantaine et le destinataire reçoit le message sans ce contenu.
Supprimer la totalité du message	(Scan en temps réel uniquement) Supprime la totalité du message électronique. Le destinataire désigné ne recevra pas le message.

Action	Description
Ignorer	Enregistre l'infection virale engendrée par des fichiers malveillants dans les journaux de virus, mais n'entreprend aucune action. les fichiers protégés par mot de passe, chiffrés ou exclus sont remis au destinataire sans mise à jour des journaux. Pour le filtrage de contenu, distribue le message tel qu'il est.
Archivage	Déplace le message vers le répertoire d'archivage et le transmet au destinataire d'origine.
Mise en quarantaine du message dans le dossier spam côté serveur	Envoie le message intégral au serveur Security Server pour quarantaine.
Mise en quarantaine du message dans le dossier spam de l'utilisateur	Envoie le message intégral vers le dossier spam de l'utilisateur pour quarantaine. Le dossier est situé côté serveur du magasin d'informations.
Marquer et envoyer	Ajoute une marque aux informations d'en-tête du message, ce qui permet de l'identifier en tant que spam, puis de le transférer au destinataire.

Outre ces actions, vous pouvez également configurer les éléments suivants :

- **Activer l'action sur le comportement de publipostage** : choisissez de nettoyer, remplacer par un texte/fichier, supprimer le message entier, ignorer ou mettre en quarantaine une partie du message pour le type de comportement de publipostage des menaces.
- **Prendre les mesures suivantes en cas d'échec du nettoyage** : Définissez l'action secondaire pour les tentatives de nettoyage infructueuses. Choisissez de remplacer par un texte/fichier, supprimer le message entier, ignorer ou mettre en quarantaine partie du message.

ActiveAction

Le tableau suivant illustre comment ActiveAction traite chaque type de virus/programme malveillant :

TABLEAU 7-5. Actions de scan recommandées par Trend Micro contre les virus et les programmes malveillants

TYPE DE VIRUS/ PROGRAMMES MALVEILLANTS	SCAN EN TEMPS RÉEL		SCAN MANUEL/SCAN PROGRAMMÉ	
	PREMIÈRE ACTION	DEUXIÈME ACTION	PREMIÈRE ACTION	DEUXIÈME ACTION
Virus	Nettoyer	Supprimer la totalité du message	Nettoyer	Remplacer par un texte/fichier
Cheval de Troie/ Vers	Remplacer par un texte/fichier	N/A	Remplacer par un texte/fichier	N/A
Utilitaire de compression	Mettre en quarantaine une partie du message	N/A	Mettre en quarantaine une partie du message	N/A
Autre code malveillant	Nettoyer	Supprimer la totalité du message	Nettoyer	Remplacer par un texte/fichier
Menaces supplémentaires	Mettre en quarantaine une partie du message	N/A	Remplacer par un texte/fichier	N/A
Comportement de type publipostage de masse	Supprimer la totalité du message	N/A	Remplacer par un texte/fichier	N/A

Notifications d'action de scan

Sélectionnez **Notifier les destinaires** pour que Messaging Security Agent avertisse les destinataires prévus lors de l'application d'une action à un message électronique spécifique. Vous souhaitez peut-être, pour diverses raisons, ne pas indiquer aux destinataires externes qu'un message contenant des informations sensibles a été bloqué. Sélectionnez **Ne pas notifier les destinataires externes** pour envoyer les notifications aux destinataires internes seulement. Définissez les adresses internes dans **Opérations** > **Paramètres de notification** > **Définition des messages internes**.

Vous pouvez également désactiver l'envoi des notifications aux destinataires externes des expéditeurs d'usurpation d'identité.

Paramètres avancés (Actions du scan)

Paramètres	Détails

Macros	les virus de macro sont des virus spécifiques aux applications qui infectent les utilitaires de macros des applications. Le scan de macro avancé utilise un niveau de scan heuristique afin de détecter les virus de macro ou supprime tous les codes macro détectés. Le scan heuristique est une méthode évaluative de détection des virus utilisant un système de reconnaissance de signatures et une technologie basée sur des règles pour rechercher les codes malveillants de macro. Cette méthode excelle dans la détection de nouveaux virus et menaces dont la signature de virus est inconnue.
	
	Messaging Security Agent agit contre le code de macro malveillant en fonction de l'action configurée.
	
	• **Niveau heuristique**
	  • Le niveau 1 utilise les critères les plus spécifiques mais détecte la plus petite quantité de codes macros.
	  • Le niveau 4 détecte le plus de codes macro mais utilise les critères les moins spécifiques et peut identifier par erreur un code de macro sécurisé en tant que code malveillant de macro.
	
	Conseil
	Trend Micro recommande de définir un niveau 2 de scan heuristique. Ce niveau offre un taux de détection élevé pour les virus de macro inconnus, assure un scan rapide et utilise uniquement les règles nécessaires pour vérifier les chaînes de virus. Le niveau 2 présente également un faible niveau de codes malveillants mal-identifiés parmi les codes macro sécurisés.
	
	• **Supprimer toutes les macros détectées par le scan de macro avancé** : Supprime tous les codes de macro des fichiers scannés

Paramètres	Détails
Parties de messages non scannables	définissez l'action et la condition de notification pour les fichiers protégés par mot de passe et/ou chiffrés. Comme action, choisissez parmi les options Remplacer par un texte/fichier, Mettre la totalité du message en quarantaine, Supprimer le message entier, Ignorer ou Mettre en quarantaine une partie du message.
Exclure les parties de messages	définissez l'action et la condition de notification pour les parties des messages qui ont été exclues. Comme action, choisissez parmi les options Remplacer par un texte/fichier, Mettre la totalité du message en quarantaine, Supprimer le message entier, Ignorer ou Mettre en quarantaine une partie du message.
Sauvegarder le paramètre	Emplacement d'enregistrement de la sauvegarde des fichiers infectés avant leur nettoyage par l'agent.
Paramètres de remplacement	configurez le texte et le fichier pour le texte de remplacement. Si l'action consiste à **remplacer par un texte/fichier**, Worry-Free Business Security remplace la menace par cette chaîne de texte et ce fichier.

Chapitre 8

Gestion des mises à jour

Ce chapitre décrit les composants et les procédures de mise à jour de Worry-Free Business Security.

Présentation des mises à jour

Toutes les mises à jour des composants proviennent du serveur ActiveUpdate de Trend Micro. Lorsque des mises à jour sont disponibles, le serveur Security Server télécharge les composants mis à jour, puis les distribue aux agents Security Agent et Messaging Security Agent (Advanced uniquement).

Si le serveur Security Server gère un grand nombre d'agents Security Agent, la mise à jour peut utiliser une quantité significative de ressources du serveur, ce qui nuit à la stabilité et aux performances de ce dernier. Pour résoudre ce problème, Worry-Free Business Security possède une fonction **d'agent de mise à jour** qui permet de répartir sur certains agents Security Agent la tâche de distribution des mises à jour vers d'autres agents Security Agent.

Le tableau suivant décrit les options de mise à jour des composants pour le serveur Security Server and ses agents, ainsi que les recommandations d'utilisation :

Tableau 8-1. Options de mise à jour

Séquence de mise à jour	Description	Recommandation
1. ActiveUpdate Server ou source de mise à jour personnalisée 2. Security Server 3. Agents	Trend Micro Security Server reçoit les composants mis à jour depuis le serveur ActiveUpdate ou une source de mise à jour et les déploie directement sur les agents (Security Agent et Messaging Security Agent).	Utilisez cette méthode s'il n'existe aucune section à faible bande passante entre le serveur Security Server et les agents.

Séquence de mise à jour	Description	Recommandation
1. ActiveUpdate Server ou source de mise à jour personnalisée 2. Security Server 3. Agents de mise à jour, agents Messaging Security Agent, agents Security Agent sans agents de mises à jour 4. Tous les autres agents Security Agent	Trend Micro Security Server reçoit les composants mis à jour depuis le serveur ActiveUpdate ou depuis une source de mise à jour et les déploie directement sur les composants suivants : • Agents de mise à jour • Agents Messaging Security Agent • Agents Security Agent sans agents de mises à jour Les agents de mises à jour déploient ensuite les composants sur leurs agents Security Agent respectifs. Si ces agents Security Agent ne peuvent pas effectuer la mise à jour, ils l'effectuent directement depuis le serveur Security Server.	Si votre réseau comporte des sections à faible bande passante situées entre le serveur Security Server et les agents Security Agent, utilisez cette méthode pour équilibrer le volume du trafic sur le réseau.
1. Serveur ActiveUpdate 2. Agents Security Agent	Les agents Security Agent dans l'impossibilité d'effectuer une mise à jour depuis n'importe quelle source, effectuent directement cette opération depuis le serveur ActiveUpdate. **Remarque** Les agents Messaging Security Agent n'effectuent jamais de mises à jour directement depuis le serveur ActiveUpdate. Si aucune source n'est disponible, Messaging Security Agent abandonne le processus de mise à jour.	Ce mécanisme est fourni uniquement en dernier recours et requiert les conditions suivantes : Activer **Utiliser ActiveUpdate de Trend Micro comme source de mises à jour secondaire** dans Mettre à jour les privilèges

Composants pouvant être mis à jour

Worry-Free Business Security utilise des composants pour protéger les agents contre les menaces les plus récentes. Pour les mettre à jour, exécutez des mises à jour manuelles ou programmées.

Vous pouvez afficher la liste des composants comme suit :

- Accédez à **Mises à jour** > **Manuel**.
- Accédez à **État actuel** et cliquez sur **Vérifier l'état du composant** dans le widget État de l'agent.

Les tableaux suivants répertorient les composants téléchargés par le Security Server à partir du serveur ActiveUpdate :

TABLEAU 8-2. Composants de messagerie (Advanced uniquement)

COMPOSANT	DISTRIBUÉ À	DESCRIPTION
Fichier de signatures anti-spam de Messaging Security Agent	Agents Messaging Security Agent	Le fichier de signatures anti-spam identifie les spams les plus récents dans les messages électroniques et leurs pièces jointes.
Moteur anti-spam 32/64 bits de Messaging Security Agent	Agents Messaging Security Agent	Le moteur anti-spam détecte les spams dans les messages électroniques et leurs pièces jointes.
Moteur de scan 32/64 bits de Messaging Security Agent	Agents Messaging Security Agent	Le moteur de scan détecte les vers Internet, les expéditeurs de courrier en masse, les chevaux de Troie, les sites de phishing, les logiciels espions, les formes d'exploitation du réseau et les virus dans les messages électroniques et leurs pièces jointes.

Composant	Distribué à	Description
Moteur de filtrage d'URL 32/64 bits de Messaging Security Agent	Agents Messaging Security Agent	Le moteur de filtrage d'URL facilite la communication entre Worry-Free Business Security et le service de filtrage d'URL de Trend Micro. Le service de filtrage d'URL est un système qui évalue les URL et fournit des informations d'évaluation à Worry-Free Business Security.

Tableau 8-3. Antivirus et smart scan

Composant	Distribué à	Description
Fichier de signatures de virus	Agents Security Agent utilisant le scan traditionnel	Le fichier de signatures de virus contient des informations qui aident les Agents Security Agent à identifier les virus, les programmes malveillants et les attaques mixtes les plus récents. 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.
Signature IntelliTrap	Agents Security Agent	Le fichier de signatures IntelliTrap détecte les fichiers de compression en temps réels compressés en tant que fichiers exécutables. Pour plus de détails, voir *IntelliTrap à la page D-3*.
Signature d'exception IntelliTrap	Agents Security Agent	Le fichier de signatures d'exceptions IntelliTrap contient une liste des fichiers de compression « approuvés »

Composant	Distribué à	Description
Moteur de scan antivirus 32/64 bits	Agents Security Agent	Initialement développé pour faire face aux premiers virus de fichier, le moteur de scan est la partie centrale de tous les produits Trend Micro. Le moteur de scan actuel est exceptionnellement sophistiqué et capable de détecter différents types de virus/ programmes malveillants. Il détecte également les virus contrôlés qui sont développés et utilisés à des fins de recherche. Au lieu d'analyser chaque fichier octet par octet, le moteur et le fichier de signatures fonctionnent ensemble pour identifier les éléments suivants : • les caractéristiques révélatrices du code de virus, • l'emplacement précis du virus dans un fichier.

Composant	Distribué à	Description
Signatures Smart Scan	Non distribué vers Agents Security Agent. Stocké sur le serveur Security Server, ce fichier de signatures est utilisé lors de la réponse aux requêtes de scan envoyées par les Agents Security Agent.	En mode Smart Scan, les Agents Security Agent utilisent deux fichiers de signatures légers qui fonctionnent ensemble pour assurer la même protection que les fichiers de signatures anti-programmes malveillants et anti-spyware traditionnels. Le fichier **Signatures Smart Scan** contient la majorité des définitions de signatures. **Signatures de l'agent Smart Scan** contient toutes les autres définitions de signatures introuvables sur Signatures Smart Scan. Le Security Agent effectue un scan pour rechercher les menaces de sécurité à l'aide de **Signatures de l'agent Smart Scan**. Agents Security Agent qui ne parviennent pas à déterminer le risque que présente le fichier durant le scan vérifient ce risque en envoyant une requête de scan au serveur de scan, un service hébergé sur le serveur Security Server. Le serveur de scan vérifie le risque à l'aide du fichier **Signatures Smart Scan**. L'Security Agent met en mémoire cache le résultat de la requête fourni par le serveur de scan afin d'améliorer les performances du scan.
Signatures de l'agent Smart Scan	Agents Security Agent utilisant Smart Scan	
Modèle Damage Cleanup	Agents Security Agent	Le Modèle Damage Cleanup est utilisé par le Moteur Damage Cleanup pour identifier les fichiers et processus de chevaux de Troie afin de les éliminer.
Moteur Damage Cleanup 32/64 bits	Agents Security Agent	Le Moteur Damage Cleanup recherche et supprime les chevaux de Troie et leurs processus.

Composant	Distribué à	Description
Modèle d'inspection de mémoire	Agents Security Agent	Cette technologie améliore la détection des virus polymorphes et mutants et optimise les scans basés sur des signatures de virus en émulant l'exécution de fichiers. Les résultats sont ensuite analysés dans un environnement contrôlé pour prouver le caractère malveillant des éléments détectés, avec un faible impact sur les performances du système.
Moteur d'intelligence contextuelle 32/64 bits	Agents Security Agent	Le moteur d'intelligence contextuelle surveille le processus d'exécution des fichiers à faible prévalence et extrait les caractéristiques comportementales que le Gestionnaire de requêtes d'intelligence contextuelle envoie au moteur d'apprentissage automatique prédictif pour analyse.
Fichier de signatures d'intelligence contextuelle	Agents Security Agent	Le fichier de signatures d'intelligence contextuelle contient une liste de comportements « approuvés » qui ne correspondent à aucune menace connue.
Gestionnaire de requêtes d'intelligence contextuelle 32/64 bits	Agents Security Agent	Le gestionnaire de requêtes d'intelligence contextuelle traite les comportements identifiés par le moteur d'intelligence contextuelle et envoie le rapport au moteur d'apprentissage automatique prédictif.
Moteur de scan de menaces avancées 32/64 bits	Agents Security Agent	Le Moteur de scan de menaces avancées extrait des fonctionnalités de fichier à partir de fichiers à faible prévalence et envoie les informations au moteur d'apprentissage automatique prédictif.
Fichier de signatures de corrélation de menaces avancées	Agents Security Agent	Le fichier de signatures de corrélation de menaces avancées contient une liste de fonctionnalités de fichiers ne correspondant à aucune menace connue.

Composant	Distribué à	Description
Early Boot Cleanup Driver 32/64 bits	Agents Security Agent	Le Early Boot Cleanup Driver de Trend Micro se charge avant les pilotes du système d'exploitation afin de détecter et de bloquer les rootkits de démarrage. Une fois l'Security Agent chargé, le Early Boot Cleanup Driver Trend Micro appelle Damage Cleanup Services pour nettoyer le rootkit.

Tableau 8-4. Anti-spyware

Composant	Distribué à	Description
Moteur de scan anti-spywares/graywares v.6 32/64 bits	Agents Security Agent	Le moteur de scan anti-spyware/grayware recherche et exécute l'action de scan appropriée sur les spywares/graywares.
Fichier de signatures de spywares/ graywares v.6	Agents Security Agent	Le fichier de signatures de spywares/ graywares identifie les spywares/graywares dans les fichiers et programmes, les modules dans la mémoire, les base de registre Windows et les raccourcis d'URL.
Fichier de signatures de spywares/ graywares	Agents Security Agent	

Tableau 8-5. Virus réseau

Composant	Distribué à	Description
Fichier de signatures de pare-feu commun	Agents Security Agent	Comme le fichier de signatures de virus, le fichier de signatures de pare-feu commun aide les agents à identifier les signatures de virus, signatures uniques des bits et des octets signalant la présence d'un virus sur le réseau.

TABLEAU 8-6. Surveillance des comportements et contrôle des dispositifs

COMPOSANT	DISTRIBUÉ À	DESCRIPTION
Modèle de détection de surveillance des comportements 32/64 bits	Agents Security Agent	Ce modèle contient les règles pour la détection des comportements suspects.
Pilote principal de surveillance des comportements 32/64 bits	Agents Security Agent	Ce pilote de noyau contrôle les événements système et les transmet au Service principal de surveillance des comportements pour l'application des stratégies.
Service principal de surveillance des comportements 32/64 bits	Agents Security Agent	Ce service en mode utilisateur offre les fonctions suivantes : • Détection des rootkits • Régulation de l'accès aux dispositifs externes • Protection des fichiers, des clés de registres et des services
Modèle de configuration de surveillance des comportements	Agents Security Agent	Le Pilote de la surveillance des comportements utilise ce fichier de signatures pour identifier les événements système normaux et les exclure de l'application des stratégies.
Fichier de signatures de la récupération des dommages	Agents Security Agent	La Fichier de signatures de la récupération des dommages contient des stratégies utilisées pour surveiller des comportements suspects.
Fichier de signature numérique	Agents Security Agent	Ce fichier de signatures contient la liste de signatures numériques valides utilisées par le Service principal de surveillance des comportements afin de déterminer si un programme responsable d'un événement système ne présente pas de danger.

Composant	Distribué à	Description
Modèle de conformité aux stratégies	Agents Security Agent	Le service principal de surveillance des comportements contrôle les événements système en les comparant aux stratégies spécifiées dans ce modèle.
Modèle de déclenchement du scan de mémoire (32/64 bits)	Agents Security Agent	Le service de déclenchement du scan de mémoire exécute d'autres moteurs de scan lorsqu'il détecte que le processus en mémoire est décompressé.
Fichier de signatures de surveillance d'inspection des programmes	Agents Security Agent	La Fichier de signatures de surveillance d'inspection des programmes surveille et stocke des points d'inspection utilisés pour la surveillance des comportements.
Fichier de signatures de suivi des menaces 32/64 bits	Agents Security Agent	Le fichier de signatures de suivi des menaces identifie les attaques de programmes malveillants sans fichier.

Tableau 8-7. Exploitations de failles de navigateur

Composant	Distribué à	Description
Signature de prévention de l'exploitation des failles du navigateur	Agents Security Agent	Ce modèle identifie les dernières exploitations de failles de navigateur Web et empêche l'utilisation de ces exploitations pour éviter de compromettre le navigateur Web.
Fichier de signatures unifiées de l'analyseur de script	Agents Security Agent	Ce modèle analyse le script des pages Web et identifie le script malveillant.

Tableau 8-8. Apprentissage automatique prédictif

Composant	Distribué à	Description
Modèle de fichier local d'apprentissage automatique prédictif	Agents Security Agent	Le modèle de fichier local d'apprentissage automatique prédictif identifie les menaces de fichiers exécutables portables lorsque les endpoints se déconnectent d'Internet.

Correctifs de type Hot Fix, patchs et Service Packs

Après la publication officielle d'un produit, Trend Micro développe souvent les éléments suivants afin de corriger les problèmes, d'améliorer les performances des produits ou d'y ajouter de nouvelles fonctionnalités.

- *Correctif critique à la page D-2*
- *Hot Fix à la page D-2*
- *Correctif à la page D-10*
- *Service Pack à la page D-26*

Votre revendeur ou technicien peut vous contacter lorsque ces éléments sont disponibles. Consultez le site Web de Trend Micro pour obtenir des informations sur les nouveaux correctifs de type hot fix, patchs et service packs :

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

Toutes les versions incluent un fichier Lisez-moi contenant des informations relatives à l'installation, au déploiement et à la configuration. Veuillez lire attentivement le fichier Lisez-moi avant d'exécuter l'installation.

Mises à jour du serveur Security Server

Mises à jour automatiques

Le serveur Security Server exécute automatiquement les mises à jour suivantes :

- Immédiatement après son installation, le serveur Security Server effectue une mise à jour depuis le serveur ActiveUpdate de Trend Micro.
- Chaque fois que le serveur Security Server démarre, il met à jour ses composants.
- Par défaut, les mises à jour programmées s'exécutent toutes les heures (la fréquence de mise à jour peut être modifiée dans la console Web).

Mises à jour manuelles

Vous pouvez effectuer manuellement des mises à jour depuis la console Web si la mise à jour est urgente.

Rappels et conseils de mise à jour de serveur

- Après une mise à jour, le serveur Security Server distribue automatiquement les mises à jour de composants aux agents. Pour plus d'informations sur les composants distribués aux agents, voir *Composants pouvant être mis à jour à la page 8-4*.
- Un serveur Security Server IPv6 pur ne peut pas effectuer les tâches suivantes :
  - Obtenir une mise à jour à partir du serveur ActiveUpdate de Trend Micro ou de toute autre source de mise à jour personnalisée IPv4 pure.
  - Distribuer des mises à jour directement aux agents IPv4 purs.

  De même, un serveur Security Server IPv4 pur ne peut effectuer directement de mises à jour à partir d'une source de mise à jour personnalisée IPv6 pure et distribuer de mise à jour aux agents IPv6 purs.

  Dans ces situations, un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur Security Server d'obtenir et de distribuer des mises à jour.
- Si vous utilisez un serveur proxy pour vous connecter à Internet, définissez les paramètres proxy appropriés dans **Administration** > **Paramètres généraux** > **Onglet Proxy** pour pouvoir télécharger les mises à jour.

Duplication des composants

Trend Micro publie des fichiers de signatures régulièrement pour maintenir à jour la protection des clients. De nouveaux fichiers de mise à jour étant régulièrement mis à disposition, le serveur Security Server utilise un mécanisme appelé **duplication des composants** permettant une mise à jour plus rapide des fichiers de signatures.

Lorsque la dernière version d'un fichier de signatures complet est disponible au téléchargement sur le serveur ActiveUpdate de Trend Micro, des fichiers de signatures incrémentiels deviennent également disponibles. Les fichiers de signatures incrémentiels constituent des versions moins volumineuses que le fichier de signatures complet et correspondent à la différence entre la version la plus récente et la version précédente du fichier de signatures complet. Par exemple, si la version la plus récente est la version 175, le fichier de signatures incrémentiel v_173.175 contient les signatures de la version 175 absentes de la version 173 (la version 173 est la version précédente du fichier de signatures complet, puisque les numéros des fichiers de signatures sont déterminés par incrémentation de 2). Le fichier de signatures incrémentiel v_171.175 contient les signatures de la version 175 absentes de la version 171.

Pour réduire le trafic réseau généré lors du téléchargement du fichier de signatures le plus récent, le serveur Security Server effectue une duplication des composants, une méthode de mise à jour par laquelle le serveur télécharge uniquement les fichiers de signatures incrémentiels. Afin de tirer parti de la duplication des composants, assurez-vous que le serveur Security Server est régulièrement mis à jour. Sinon, le serveur devra télécharger le fichier de signatures complet.

La duplication des composants s'applique aux composants suivants :

- Fichier de signatures de virus
- Signatures de l'agent Smart Scan
- Modèle Damage Cleanup
- Signature d'exception IntelliTrap
- Fichier de signatures de spywares

Configuration de la source de mise à jour du serveur Security Server

Avant de commencer

Par défaut, le serveur Security Server obtient les mises à jour depuis le serveur ActiveUpdate de Trend Micro. Indiquez une source de mise à jour

personnalisée si le serveur Security Server est dans l'impossibilité d'accéder directement au serveur ActiveUpdate.

- Si la source est le **serveur ActiveUpdate de Trend Micro**, assurez-vous que Security Server dispose d'une connexion Internet et, si vous utilisez un serveur proxy, testez la connexion Internet pour voir si elle peut être établie en utilisant les paramètres du proxy. Pour plus de détails, voir *Configuration des paramètres de proxy Internet à la page 11-3*.
- S'il s'agit d'une source de mise à jour personnalisée (**Emplacement Intranet contenant une copie du fichier actuel** ou **Source de mise à jour alternative**), définissez l'environnement et les ressources de mise à jour appropriés pour cette source de mise à jour. Assurez-vous également qu'il existe une connexion opérationnelle entre le serveur Security Server et cette source de mise à jour. Si vous avez besoin d'aide pour définir une source de mise à jour, contactez votre service d'assistance.
- Un serveur Security Server IPv6 ne peut pas directement effectuer de mises à jour à partir du serveur ActiveUpdate de Trend Micro ou toute autre source de mise à jour personnalisée IPv4 pure. De même, un serveur Security Server IPv4 pur ne peut pas effectuer directement de mises à jour à partir de sources de mise à jour personnalisées IPv6 pures. Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur Security Server de se connecter aux sources de mises à jour.

Procédure

1. Accédez à **Mises à jour** > **Source**.
2. Dans l'onglet **Serveur**, sélectionnez une source de mise à jour.
   - **Serveur ActiveUpdate de Trend Micro**
   - **Emplacement Intranet contenant une copie du fichier actuel** : Saisissez le chemin UNC (Universal Naming Convention) de la source, tel que `\\Web\ActiveUpdate`. Spécifiez également les informations de connexion (nom d'utilisateur et mot de passe) que le serveur Security Server utilisera pour se connecter à cette source.

- **Source de mise à jour alternative** : Saisissez l'URL de cette source. Assurez-vous que le répertoire virtuel HTTP (partage Web) cible est accessible par le serveur Security Server.

3. Cliquez sur **Enregistrer**.

Mise à jour manuelle du serveur Security Server

Mettez à jour manuellement les composants sur le serveur Security Server après l'installation ou la mise à niveau du serveur et en cas d'épidémie.

Procédure

1. Il existe deux types de mises à jour manuelles :

   - Accédez à **Mises à jour** > **Manuel**.
   - Accédez à **État actuel** et cliquez sur **Vérifier l'état du composant** dans le widget État de l'agent.

   L'écran **Mise à jour manuelle** s'affiche.

2. Sélectionnez les composants à mettre à jour.

   Pour plus d'informations sur les composants, voir *Composants pouvant être mis à jour à la page 8-4*.

3. Cliquez sur **Mettre à jour maintenant**.

   La fenêtre indiquant l'état de la mise à jour s'affiche. Lorsque la mise à jour a réussi, Security Server déploie les composants mis à jour vers les agents.

Configuration des mises à jour programmées du serveur Security Server

Configurez Security Server afin de vérifier régulièrement la source de mise à jour et de télécharger automatiquement les mises à jour disponibles. La mise

à jour programmée est un moyen simple et efficace de garantir que votre protection contre les menaces est à jour en permanence.

au cours d'épidémies de virus/programmes malveillants, Trend Micro réagit rapidement pour mettre à jour les fichiers de signatures de virus (les mises à jour peuvent être publiées plus d'une fois par semaine). Le moteur de scan et les autres composants sont également mis à jour régulièrement. Trend Micro recommande de mettre à jour vos composants quotidiennement, voire plusieurs fois par jour lors d'épidémies de virus/programmes malveillants, afin que l'agent dispose des derniers composants mis à jour.

Important

Évitez de programmer l'exécution d'un scan et d'une mise à jour en même temps. Cela peut entraîner un arrêt inattendu du scan programmé.

Procédure

1. Accédez à **Mises à jour** > **Programmées**.
2. Sélectionnez les composants à mettre à jour.

   Pour plus de détails sur les composants, voir *Composants pouvant être mis à jour à la page 8-4*.
3. Cliquez sur l'onglet **Programmation**, puis spécifiez la programmation de la mise à jour.

   - **Les mises à jour de scan traditionnelles** incluent tous les composants, sauf les signatures Smart Scan et les signatures de l'agent Smart Scan. Effectuez votre choix parmi les mises à jour quotidiennes, hebdomadaires et mensuelles, puis spécifiez une valeur pour **Mettre à jour pour une période de**, soit le nombre d'heures durant lesquelles le serveur Security Server effectue la mise à jour. Le serveur Security Server procède à la mise à jour à tout moment pendant cette période.

Remarque

Pour les mises à jour programmées mensuelles, si vous sélectionnez 31, 30 ou 29 jours et qu'un mois compte un nombre inférieur de jours, la mise à jour ne s'exécutera pas ce mois-là.

- **Les mises à jour smart scan** incluent uniquement les signatures Smart Scan et les signatures de l'agent Smart Scan. Si aucun de vos agents n'utilise smart scan, ignorez cet élément.

4. Cliquez sur **Enregistrer**.

Rétrogradation des composants

Rétrograder signifie revenir à une version précédente du fichier de signatures de virus, du fichier signatures de l'agent Smart Scan et du moteur de scan antivirus. Si ces composants ne fonctionnent pas correctement, rétrogradez-les vers leur version précédente. Le Security Server conserve les versions actuelles et précédentes du moteur de scan antivirus et les trois dernières versions du fichier de signatures de virus et de Signatures de l'agent Smart Scan.

Remarque

Seuls les composants mentionnés ci-dessus peuvent être rétrogradés.

Worry-Free Business Security utilise des moteurs de scan différents selon que les agents exécutent des plates-formes 32 ou 64 bits. Il est nécessaire de rétrograder ces moteurs de scan séparément. La procédure de rétrogradation est identique pour tous les types de moteurs.

Procédure

1. Accédez à **Mises à jour** > **Rétrograder**.
2. Cliquez sur **Synchroniser** pour un composant spécifique afin d'indiquer aux agents de procéder à la synchronisation des versions de leur composant sur la version du serveur.

3. Cliquez sur **Rétrograder** pour un composant spécifique afin de rétrograder ce composant sur le Security Server et ses agents.

Mise à jour des agents Security Agent et Messaging Security Agent

Mises à jour automatiques

Les agents Security Agent et Messaging Security Agent (Advanced uniquement) effectuent automatiquement les mises à jour suivantes :

- Immédiatement après l'installation, les agents effectuent des mises à jour à partir de Security Server.
- Lors de chaque mise à jour effectuée par Security Server, les mises à jour sont automatiquement envoyées aux agents.
- Lors de chaque mise à jour effectuée par l'agent de mise à jour, les mises à jour sont automatiquement envoyées aux agents Security Agent respectifs.
- Par défaut, les mises à jour planifiées s'exécutent :
  - Toutes les 8 heures sur les agents In Office Security Agent ;
  - Toutes les 2 heures sur les agents Out of Office Security Agent.
- Par défaut, les agents Messaging Security Agent exécutent une mise à jour programmée toutes les 24 heures, à midi.

Exécution d'une mise à jour manuelle

Security Agent reçoit automatiquement les mises à jour de Security Server.

Vous pouvez effectuer une mise à jour manuelle après une déconnexion temporaire du réseau d'entreprise ou si vous devez bénéficier rapidement de

la protection la plus récente contre les menaces de sécurité (par exemple, après une épidémie).

Si vous utilisez un serveur proxy pour vous connecter à Internet, vérifiez que les paramètres de proxy sont corrects.

Procédure

1. Ouvrez la console principale et cliquez sur **Mise à jour**.

   Remarque

   Vous pouvez également effectuer une mise à jour manuelle en cliquant avec le bouton droit sur l'icône dans la barre des tâches Windows, puis en sélectionnant Security Agent dans la barre des tâches Windows, puis en sélectionnant **Mettre à jour maintenant**.

2. Cliquez sur **Fermer** lorsque la mise à jour est complète.

Rappels et astuces sur la mise à jour d'agents

- Les agents Security Agent effectuent des mises à jour depuis Security Server, les agents de mise à jour ou le serveur ActiveUpdate de Trend Micro.

  Les agents Messaging Security Agent effectuent uniquement des mises à jour depuis Security Server.

  Pour plus d'informations sur le processus de mise à jour, voir *Présentation des mises à jour à la page 8-2*.

- Un agent IPv6 pur ne peut pas obtenir de mises à jour directement depuis un serveur Security Server/un agent de mise à jour IPv4 pur, ni depuis le serveur ActiveUpdate de Trend Micro.

  De même, un agent IPv4 pur ne peut pas obtenir de mises à jour directement depuis un serveur Security Server/un agent de mise à jour IPv6 pur.

En pareil cas, un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux clients d'obtenir des mises à jour.

- Pour plus d'informations sur les composants mis à jour par les agents, voir *Composants pouvant être mis à jour à la page 8-4*.
- Outre les composants, les agents reçoivent également des fichiers de configuration mis à jour lors de la mise à jour depuis Security Server. Les agents ont besoin des fichiers de configuration pour appliquer de nouveaux paramètres. À chaque fois que vous modifiez les paramètres de l'agent via la console Web, les fichiers de configuration sont modifiés.

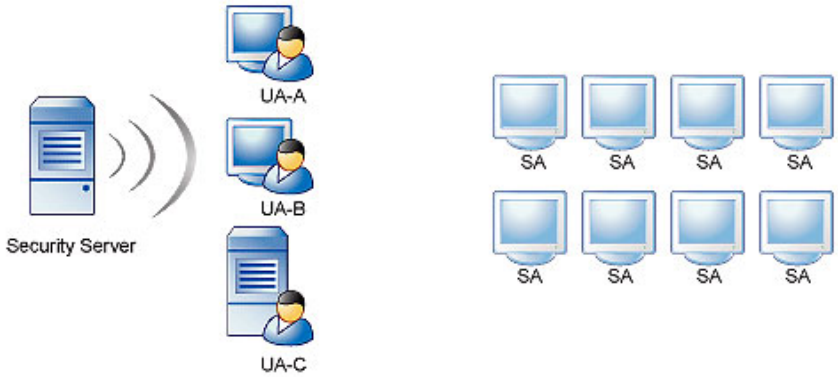
Agents de mise à jour

Les agents de mise à jour sont des agents Security Agent qui peuvent recevoir des composants mis à jour depuis le serveur Security Server ou le serveur ActiveUpdate, et les déployer sur d'autres agents.

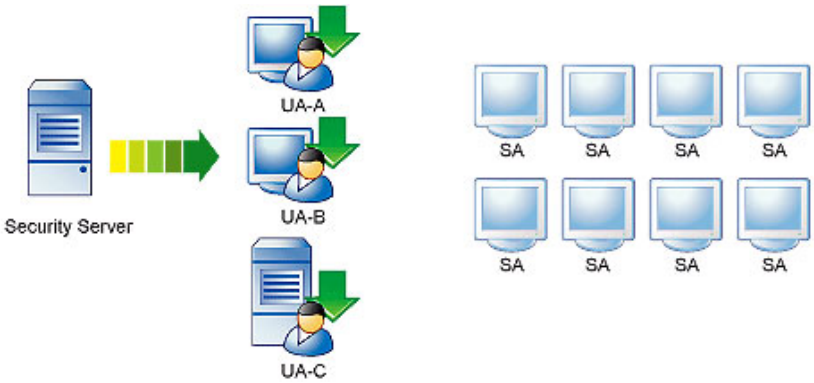
Si vous identifiez des sections de votre réseau entre les clients et Trend Micro Security Server comme étant « à faible bande passante » ou « à trafic élevé », vous pouvez indiquer que les agents Security Agent agissent en tant qu'agents de mise à jour. Les agents de mise à jour permettent de réduire la consommation de bande passante en évitant que tous les agents Security Agent aient besoin d'accéder au serveur Security Server pour mettre à jour les composants. Si votre réseau est segmenté par emplacement et si le lien réseau entre les segments présente un trafic élevé, Trend Micro recommande d'autoriser au moins un agent Security Agent sur chaque segment à agir comme agent de mise à jour.

Le processus de l'agent de mise à jour peut être décrit comme suit :

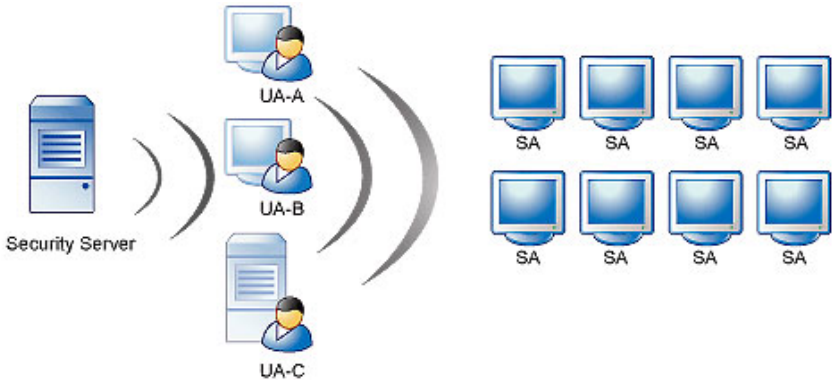
1. Security Server notifie les agents de mise à jour que de nouvelles mises à jour sont disponibles.



2. Les agents de mise à jour téléchargent toujours les composants mis à jour à partir du serveur Security Server.



3. Le serveur Security Server notifie alors aux agents Security Agent que les composants mis à jour sont disponibles.

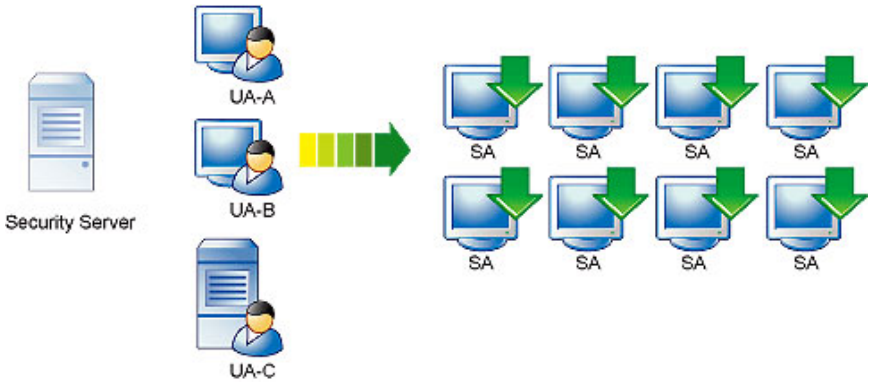


4. Chaque agent Security Agent télécharge une copie du tableau d'ordre des agents de mise à jour afin de déterminer la source de mise à jour appropriée. L'ordre des agents de mise à jour dans ce tableau est initialement déterminé par l'ordre d'ajout des agents en tant que sources alternatives de mise à jour sur la console Web. Chaque agent Security Agent consulte le tableau entrée par entrée, en commençant par la première, jusqu'à ce qu'il identifie sa source de mise à jour.

Tableau d'ordre des agents de mise à jour

Plage IP	Agent de mise à jour
10.1.1.1-10.1.1.10	UA-A
10.2.1.1-10.2.1.10	UA-B
10.3.1.1-10.3.1.10	UA-C

5. Les agents Security Agent téléchargent ensuite les composants à jour depuis leur agent de mise à jour attribué. Si pour une raison quelconque l'agent de mise à jour attribué n'est pas disponible, l'agent Security Agent tente de télécharger les composants à jour depuis le serveur Security Server.



Configuration des agents de mise à jour

Procédure

1. Accédez à **Mises à jour** > **Source**.
2. Cliquez sur l'onglet **Agents de mise à jour**.
3. Effectuez les actions suivantes :

TÂCHE	ÉTAPES
Affectez des agents Security Agent comme agents de mise à jour	a. Dans la section **Définir comme agent de mise à jour**, cliquez sur **Ajouter**. Un nouvel écran s'affiche. b. Dans la liste, sélectionnez un ou plusieurs agents devant agir comme agents de mise à jour. c. Cliquez sur **Enregistrer**. L'écran se ferme. d. De retour dans la section **Définir comme agent de mise à jour**, sélectionnez **Les agents de mise à jour ne se mettent toujours directement qu'à partir du serveur Security Server** si vous souhaitez que les agents de mise à jour télécharge toujours les composants mis à jour depuis le serveur Security Server plutôt que depuis un autre agent de mise à jour.

TÂCHE	ÉTAPES
Configurez la mise à jour des agents Security Agent depuis les agents de mise à jour	a. Dans la section **Sources alternatives de mise à jour**, sélectionnez **Activer des sources alternatives de mise à jour pour les agents Security Agent et les agents de mise à jour**. **Remarque** La désactivation de cette option empêche la mise à jour des agents Security Agent depuis les agents de mise à jour et les remplace par le serveur Security Server en tant que source de mise à jour. b. Cliquez sur **Ajouter**. Un nouvel écran s'affiche. c. Saisissez les adresses IP des agents Security Agent effectuant leur mise à jour depuis l'agent de mise à jour. • Saisissez une plage d'adresses IPv4. Pour spécifier un seul Security Agent, entrez l'adresse IP de l'agent Security Agent à la fois dans les champs **de** et **à**. • Pour IPv6, saisissez un préfixe et une longueur IP. d. Sélectionnez un agent de mise à jour dans la liste déroulante. Si la liste déroulante n'est pas accessible, cela signifie qu'aucun agent de sécurité n'est configuré. e. Cliquez sur **Enregistrer**. L'écran se ferme. f. Définissez davantage de plages d'IP si nécessaire. Si vous avez défini plusieurs plages d'IP, vous pouvez utiliser l'option **Réorganiser** pour définir la priorité de la plage d'IP. Lorsque le serveur Security Server notifie aux agents Security Agent que les mises à jour sont disponibles, ils scannent la liste des plages d'adresses IP pour identifier la bonne source de mise à jour. Security Agent scanne le premier élément de la liste et continue vers le bas de la liste jusqu'à ce qu'il identifie la bonne source de mise à jour.

TÂCHE	ÉTAPES
	Conseil Définissez plusieurs agents de mise à jour pour la même plage d'IP comme mesure de basculement. Cela signifie que si les agents Security Agent n'arrivent pas à effectuer une mise à jour à partir d'un agent de mise à jour, ils effectueront une nouvelle tentative auprès d'autres agents de mise à jour. Pour ce faire, créez deux (2) entrées possédant la même plage IP et assignez à chaque entrée un agent de mise à jour différent.
Supprimez des agents de mise à jour	Pour supprimer un agent de mise à jour et annuler l'affectation de tous les agents Security Agent associés, accédez à la section **Définir comme agent de mise à jour**, cochez la case correspondant au nom de l'ordinateur de l'agent de mises à jour, puis cliquez sur **Supprimer**. Cette action ne supprime pas la plage IP des agents Security Agent dans la section **Sources alternatives de mise à jour**. Elle entraînera simplement le basculement de la source de mise à jour des agents Security Agent « orphelins » vers le serveur Security Server. Si vous disposez d'un autre agent de mise à jour, vous pouvez l'affecter aux agents Security Agent orphelins.
Annuler l'affectation des agents Security Agent aux agents de mise à jour	Si vous souhaitez annuler l'appartenance d'agents Security Agent à une plage d'adresses IP dans le cadre des mises à jour à partir d'un agent de mise à jour, accédez à la section **Sources alternatives de mise à jour**, cochez la case correspondant à la plage d'adresses IP des agents Security Agent, puis cliquez sur **Supprimer**.

4. Cliquez sur **Enregistrer**.

Chapitre 9

Utilisation de l'État actuel

État actuel

Worry-Free Business Security fournit des widgets utilisés en tant que références visuelles rapides pour faciliter la gestion de l'agent Security Agent.

L'écran **État actuel** s'affiche lorsque vous ouvrez la console Web Worry-Free Business Security ou cliquez sur **État actuel** dans le menu principal.

TABLEAU 9-1. Widgets État actuel

WIDGET	DESCRIPTION
Centre d'actions	Ce widget affiche les événements pour lesquels les administrateurs doivent prendre des mesures pour résoudre les problèmes.
Risques de sécurité détectés dans le temps	Ce widget fournit une vue d'ensemble des terminaisons de votre réseau et présente les détections de menaces et les types de menaces qui ont infecté votre réseau suivant un intervalle de temps spécifié.
Résumé des logiciels de rançon	Ce widget fournit une vue d'ensemble de toutes les tentatives d'attaque par des logiciels de rançon suivant un intervalle de temps spécifié.
État de la licence	Ce widget fournit une vue d'ensemble du nombre de licences et de l'état d'expiration de vos licences.
Résumé du serveur Exchange	Ce widget donne un aperçu de l'état de connexion des agents Messaging Security Agent et la distribution des menaces détectées sur vos serveurs Exchange.
État de l'agent	Ce widget fournit une vue d'ensemble de la connexion et de l'état de mise à jour des agents Security Agent de votre réseau.

La fréquence d'actualisation des informations affichées sur l'écran **État actuel** varie selon les sections. Elle est généralement comprise entre 1 et 10 minutes. Pour actualiser manuellement les informations à l'écran, cliquez sur le bouton **Actualiser** de votre navigateur.

Centre de notifications

Ce widget affiche les événements pour lesquels les administrateurs doivent prendre des mesures pour résoudre les problèmes.

Certains événements s'accompagnent de boutons d'actions recommandées. Cliquez sur les boutons pour tenter de résoudre les problèmes ou cliquez sur les événements pour afficher plus de détails.

TABLEAU 9-2. Événements du centre de maintenance

ÉVÉNEMENT	RECOMMANDATION
Antivirus - Menaces non résolues	Exécuter un scan à l'aide de l'outil Trend Micro HouseCall.
Antivirus - Scan en temps réel désactivé sur les points finaux	Activez le scan en temps réel sur tous les dispositifs pour rester protégé.
Antivirus - Scan en temps réel désactivé sur les serveurs Exchange	Activez le scan en temps réel sur tous les serveurs Exchange pour rester protégé.
Antispyware - Détections nécessitant le redémarrage du périphérique	Redémarrez les périphériques afin de supprimer entièrement les menaces détectées.
Événements liés à la licence	Accédez à **Administration** > **Licence du produit** pour vérifier l'état de la licence.
Ressources insuffisantes - Espace disque disponible inférieur à %threshold%	Exécutez l'outil de nettoyage de disque pour supprimer les fichiers de sauvegarde, les fichiers journaux et les fichiers de signatures non utilisés. Pour plus d'informations, voir *Optimisation de l'espace disque à la page 14-15*.
Services Smart Protection - Service non disponible	Vérifiez l'état du serveur Smart Scan Server sur la console Worry-Free Business Security et assurez-vous que le serveur fonctionne correctement.

Événement	Recommandation
Mise à jour - Au moins un agent Messaging Security Agent obsolète une heure après la publication du fichier de signatures	Vérifiez que les mises à jour programmées des agents Messaging Security Agent sont activées sur le serveur Security Server et que les agents Messaging Security Agent peuvent se connecter à Internet.
Mise à jour – Taux de déploiement inférieur à %threshold% une heure après la publication du fichier de signatures	Vérifiez la connexion Internet de l'agent Security Agent et remettez les agents Security Agent à jour.
Mise à jour – Composants de Security Server non mis à jour depuis plus de %threshold% jours	Vérifiez que la mise à jour programmée des composants est activé sur le serveur Security Server et que ce dernier peut se connecter à Internet.
Mise à jour - Fichier de signatures Smart Scan non mis à jour depuis plus de %threshold% heures	Vérifiez que les mises à jour programmées du fichier de signatures Smart Scan sont activées sur le serveur Security Server et que ce dernier peut se connecter à Internet.

Antivirus : Menaces non résolues

Vous pouvez afficher ces informations en cliquant sur l'événement **Antivirus - Menaces non résolues : %N%** dans le centre d'actions. Worry-Free Business Security génère ou met à jour ces informations de journaux à chaque nouveau scan en temps réel, manuel ou programmé.

- Cliquez sur **Télécharger l'outil** pour télécharger l'outil Trend Micro HouseCall et utiliser l'outil pour exécuter un scan sur le périphérique concerné.
- Cliquez sur **Ignorer dans le centre de notifications** pour rediriger vers l'écran **État actuel** et supprimer l'événement de notification du centre d'actions. Les journaux liés aux événements de cet écran sont toujours disponibles via l'option Interroger le journal.
- Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure du dernier échec de tentative de nettoyage ou d'élimination du virus ou du programme malveillant
Nom du périphérique	Nom du périphérique affecté
Nom virus/prg malv	Nom du virus ou programme malveillant détecté Cliquez sur le lien pour être redirigé vers l'encyclopédie des menaces de Trend Micro afin d'obtenir une description approfondie de la menace ainsi que des instructions pour nettoyer manuellement des attaques correspondant à ce type de menace.
Nom du fichier	Nom du fichier corrompu par le virus ou programme malveillant
Chemin	Emplacement du fichier infecté
Type de scan	Type de scan utilisé pour détecter le virus ou le programme malveillant
Action entreprise	Action entreprise par Worry-Free Business Security en réponse à la détection de virus ou de programmes malveillants

Antivirus : scan en temps réel désactivé sur les endpoints

Pour afficher ces informations, cliquez sur l'événement **Antivirus - Scan en temps réel désactivé sur les endpoints : %N%** dans le centre de notifications.

- Cliquez sur **Activation le scan en temps réel** pour activer le scan sur tous les dispositifs.
- Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Nom du périphérique	Nom du dispositif pour lequel le scan en temps réel est désactivé
Nom de groupe	Nom du groupe auquel le périphérique appartient

Antivirus : scan en temps réel désactivé sur les serveurs Exchange

Pour afficher ces informations, cliquez sur l'événement **Antivirus - Scan en temps réel désactivé sur les serveurs Exchange : %N%** dans le centre de notifications.

- Cliquez sur **Activation le scan en temps réel** pour activer le scan de tous les serveurs Exchange.
- Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Nom du serveur Exchange	Nom du serveur Exchange pour lequel le scan en temps réel est désactivé

Anti-spyware : Détections nécessitant le redémarrage du périphérique

Vous pouvez afficher ces informations de journaux en cliquant sur **Anti-spyware - Détections nécessitant le redémarrage du périphérique : %N%** dans le centre d'actions.

- Cliquez sur **Ignorer dans le centre de notifications** pour rediriger vers l'écran **État actuel** et supprimer l'événement de notification du centre d'actions. Les journaux liés aux événements de cet écran sont toujours disponibles via l'option Interroger le journal.
- Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de détection de spywares ou graywares à Worry-Free Business Security
Nom du périphérique	Nom du périphérique affecté
Nom du spyware/grayware	Nom du spyware ou grayware détecté Cliquez sur le lien pour être redirigé vers l'encyclopédie des menaces de Trend Micro afin d'obtenir une description approfondie de la menace ainsi que des instructions pour nettoyer manuellement des attaques correspondant à ce type de menace.
Type de scan	Type de scan utilisé pour détecter le spyware ou le grayware

Ressources insuffisantes - Espace disque disponible

Vous pouvez afficher ces informations en cliquant sur l'événement **Ressources insuffisantes - Espace disque disponible inférieur à %threshold%** dans le centre de notifications.

Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Nom du serveur	Nom du serveur dont l'espace disque est insuffisant
Nom de groupe	Nom du groupe auquel appartient le serveur

Mise à jour : agents obsolètes

Vous pouvez afficher ces informations en cliquant sur l'événement **Mise à jour - Taux de déploiement inférieur à %threshold% une heure après la publication du fichier de signatures** dans le centre de notifications. Les agents Security Agent mentionnés sur cet écran nécessitent une mise à jour du moteur ou du fichier de signatures.

- Cliquez sur **Mettre à jour maintenant** pour indiquer aux agents Security Agent obsolètes de procéder à la mise à jour de leurs composants.
- Cliquez sur **Vérifier l'état du composant** pour ouvrir l'écran **Mise à jour manuelle**.
- Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Nom du périphérique	Nom du dispositif nécessitant une mise à jour des composants
Nom de groupe	Nom du groupe auquel le périphérique appartient
Méthode de scan	• Smart Scan • Scan traditionnel

Mise à jour - Agents Messaging Security Agent obsolètes

Vous pouvez afficher ces informations en cliquant sur l'événement **Mise à jour - Au moins un agent Messaging Security Agent obsolète une heure après la publication du fichier de signatures** dans le centre de notifications.

- Cliquez sur **Mettre à jour maintenant** pour indiquer aux agents Messaging Security obsolètes de procéder à la mise à jour de leurs composants.
- Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Nom du serveur Exchange	Nom du serveur Exchange nécessitant une mise à jour des composants

Risques de sécurité détectés dans le temps

Ce widget fournit une vue d'ensemble des terminaisons de votre réseau et présente les détections de menaces et les types de menaces qui ont infecté votre réseau suivant un intervalle de temps spécifié.

- Cliquez sur  ou  pour basculer entre les vues.
- Cliquez sur l'onglet **Menaces connues**, **Menaces inconnues** ou **Violations de stratégie** pour visualiser les informations de détection sur les menaces en particulier.

Afficher	Description
Graphique ()	• Cliquez sur les noms de types de menaces au bas du graphique pour afficher/masquer les informations de détection sur le graphique. • Survolez le ou les nœuds concernant un jour particulier pour consulter le nombre total de détections des types de menaces affichés. Cliquez sur un nœud pour accéder à l'écran de consignation du type de menaces mis en surbrillance dans la liste.
Tableau ()	• Cliquez sur le nombre de détections pour ouvrir l'écran de consignation qui répertorie les détails de détection.

Risques de sécurité détectés : virus/programmes malveillants

Vous pouvez afficher ces informations en cliquant sur l'un des liens suivants dans l'onglet **Menaces connues** du widget **Risques de sécurité détectés dans le temps** :

- Nombre de détections de **virus/programmes malveillants** dans le tableau
- N'importe quel nœud de **virus/programme malveillant** dans le graphique

Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure auxquelles l'agent Security Agent a signalé les informations de détection de virus/programme malveillant à Worry-Free Business Security
Nom du périphérique	Nom du périphérique affecté
Nom virus/prg malv	Nom du virus ou programme malveillant détecté Cliquez sur le lien pour être redirigé vers l'encyclopédie des menaces de Trend Micro afin d'obtenir une description approfondie de la menace ainsi que des instructions pour nettoyer manuellement des attaques correspondant à ce type de menace.
Nom du fichier	Nom du fichier corrompu par le virus ou programme malveillant
Chemin	Emplacement du fichier infecté
Type de scan	Type de scan utilisé pour détecter le virus ou le programme malveillant
Action entreprise	Action entreprise par Worry-Free Business Security en réponse à la détection de virus ou de programmes malveillants

Risques de sécurité détectés : spywares/graywares

Vous pouvez afficher ces informations en cliquant sur l'un des liens suivants dans l'onglet **Menaces connues** du widget **Risques de sécurité détectés dans le temps** :

- Nombre de détections de **spywares/graywares** dans le tableau
- N'importe quel nœud de **spywares/graywares** dans le graphique

Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de détection de spywares ou graywares à Worry-Free Business Security
Nom du périphérique	Nom du périphérique affecté Cliquez sur le nom pour afficher la liste des programmes espions ou graywares détectés sur ce dispositif.
Nom du spyware/grayware	Nom du spyware ou grayware détecté
Type de scan	Type de scan utilisé pour détecter le spyware ou le grayware
Action entreprise	Action entreprise par Worry-Free Business Security en réponse à la détection de spywares ou graywares

Risques de sécurité détectés : réputation de sites Web

Vous pouvez afficher ces informations en cliquant sur l'un des liens suivants dans l'onglet **Menaces connues** du widget **Risques de sécurité détectés dans le temps** :

- Nombre de détections de **réputation de sites Web** dans le tableau
- N'importe quel nœud de **réputation de sites Web** dans le graphique

Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de violation d'URL à Worry-Free Business Security
Nom du périphérique	Nom du périphérique tentant d'accéder à une URL interdite
URL	URL interdite

Colonne	Description
Niveau de risque	évaluation attribuée par les TrendLabs selon la facilité avec laquelle l'ordinateur a pu être infecté et en fonction des dommages potentiels.

Risques de sécurité détectés : Virus réseau

Vous pouvez afficher ces informations en cliquant sur l'un des liens suivants dans l'onglet **Menaces connues** du widget **Risques de sécurité détectés dans le temps** :

- Nombre de détections de **virus réseau** dans le tableau
- N'importe quel nœud de **virus réseau** dans le graphique

Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure auxquelles l'agent Security Agent a signalé les informations de détection de virus de réseau à Worry-Free Business Security
Nom du périphérique	Nom du périphérique affecté
IP de l'attaquant	Adresse IP de l'attaquant
IP de la victime	Adresse IP de la victime
Direction du paquet	Direction du paquet
Nom du virus de réseau	Nom du virus de réseau détecté
Nombre	Les virus de réseau sont comptabilisés à chaque fois qu'ils sont détectés.

Risques de sécurité détectés : surveillance des comportements

Vous pouvez afficher ces informations en cliquant sur l'un des liens suivants dans l'onglet **Menaces inconnues** du widget **Risques de sécurité détectés dans le temps** :

- Nombre de détections de **surveillance des comportements** dans le tableau
- N'importe quel nœud de **surveillance des comportements** dans le graphique

Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de violation de la surveillance des comportements à Worry-Free Business Security
Nom du périphérique	Nom du périphérique qui a déclenché une violation de stratégie
Menace de sécurité	Type de menace de sécurité
Sujet	Sujet de l'opération
Type d'événement	Événement système lié
Cible	Cible de l'opération
Opération	Opération effectuée par l'utilisateur qui a déclenché la violation
Résultat	Action entreprise par Worry-Free Business Security en réponse à la violation de la surveillance des comportements

Risques de sécurité détectés : apprentissage automatique prédictif

Vous pouvez afficher ces informations en cliquant sur l'un des liens suivants dans l'onglet **Menaces inconnues** du widget **Risques de sécurité détectés dans le temps** :

- Nombre de détections d'**apprentissage automatique prédictif** dans le tableau
- N'importe quel nœud d'**apprentissage automatique prédictif** dans le graphique

Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
 / 	Cliquez sur l'icône pour agrandir ou fermer les détails du journal sous la ligne du tableau.
Date/Heure	Date et heure auxquelles l'agent Security Agent a signalé les informations de détection à Worry-Free Business Security
Nom du périphérique	Nom du périphérique affecté
Nom de groupe	Nom du groupe auquel le périphérique appartient
Menace inconnue	Nom de la menace potentielle
Probabilité de la menace	Indique le niveau de correspondance entre le fichier/processus et le modèle de programme malveillant
Nom du fichier	Nom de l'objet de fichier ou du programme qui a exécuté le processus **Important** Le nom de fichier détecté ne peut pas être identique au nom de fichier détecté sur d'autres endpoints. L'apprentissage automatique prédictif associe les détections en fonction des valeurs de hachage de fichier et non en fonction de noms de fichiers spécifiques.
Chemin	Chemin de l'objet de fichier ou du programme qui a exécuté le processus
Canal d'infection	Canal d'origine de la menace

Colonne	Description
Action entreprise	Action entreprise par Worry-Free Business Security en réponse à la détection

Risques de sécurité détectés : informations sur l'apprentissage automatique prédictif

Vous pouvez afficher ces informations en cliquant sur n'importe quelle icône 
dans la première colonne de l'écran de journaux **Risques de sécurité détectés : apprentissage automatique prédictif**.

La section Détails de journaux se compose de deux onglets :

- **Menace inconnue** : fournit les résultats de l'analyse de l'apprentissage automatique prédictif.
- **Nom du fichier** : fournit des informations générales sur les propriétés du fichier et les informations sur le certificat de ce journal de détection spécifique.

> **Conseil**
>
> Cliquez sur **Ajouter à la liste d'exceptions** pour ajouter rapidement la valeur de hachage du fichier concerné à la liste d'exceptions de l'apprentissage automatique prédictif. La liste d'exceptions complète est disponible sur l'écran **Paramètres généraux**.
>
> Pour plus d'informations, voir *Configuration des paramètres de liste d'exceptions à la page 11-14*.

Le tableau suivant décrit les informations fournies dans l'onglet **Menace inconnue**.

TABLEAU 9-3. Détails de l'onglet Menace inconnue

PHASE	DESCRIPTION
Probabilité de la menace	Indique le niveau de correspondance entre le fichier/processus et le modèle de programme malveillant
Type de menace probable	Indique le type de menace le plus probable contenu dans le fichier une fois que l'apprentissage automatique prédictif a comparé l'analyse à d'autres menaces connues
Identificateurs de menace	Fournit une liste de fonctions API utilisées par le fichier/processus pouvant indiquer le type de menace détecté **Important** L'identification de la fonction API ne constitue qu'un seul facteur de la détermination du type de menace. L'apprentissage automatique prédictif utilise bon nombre d'autres fonctions de fichier et méthodes d'analyse pour calculer la probabilité de la menace et le type de menace probable.
Type de détection	Type d'objet ayant déclenché la détection (« Fichier » ou « Processus »)
Menaces connues similaires	Fournit une liste de types de menaces connus qui présentent des fonctions de fichier/processus similaires dans la détection

Risques de sécurité détectés : filtrage d'URL

Vous pouvez afficher ces informations en cliquant sur l'un des liens suivants dans l'onglet **Violations de stratégie** du widget **Risques de sécurité détectés dans le temps** :

- Nombre de détections de **filtrage d'URL** dans le tableau
- N'importe quel nœud de **filtrage d'URL** dans le graphique

Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de violation d'URL à Worry-Free Business Security
Nom du périphérique	Nom du périphérique tentant d'accéder à une URL interdite
URL	URL interdite

Risques de sécurité détectés : contrôle des dispositifs

Vous pouvez afficher ces informations en cliquant sur l'un des liens suivants dans l'onglet **Violations de stratégie** du widget **Risques de sécurité détectés dans le temps** :

- Nombre de détections de **contrôle des dispositifs** dans le tableau
- N'importe quel nœud de **contrôle des dispositifs** dans le graphique

Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure auxquelles l'agent Security Agent a signalé les informations de violation du contrôle des dispositifs à Worry-Free Business Security
Nom du périphérique	Nom du périphérique qui a déclenché une violation de stratégie
Type	Type de dispositif de stockage
Autorisation	Autorisation définie pour le dispositif de stockage
Sujet	Sujet de l'opération
Objet	Objet de l'opération
Opération	Opération effectuée

Résumé des logiciels de rançon

Ce widget fournit une vue d'ensemble de toutes les tentatives d'attaque par des logiciels de rançon suivant un intervalle de temps spécifié.

L'écran par défaut présente un résumé de toutes les détections de logiciels de rançon et classe les tentatives en fonction du canal d'infection.

- Cliquez sur le nombre de détection de logiciels de rançon sur l'écran par défaut pour ouvrir l'écran de consignation **Résumé des logiciels de rançon** qui répertorie les détails de détection des logiciels de rançon.
- Utilisez les listes déroulantes pour basculer entre les vues.

Cliquez sur  pour afficher les informations de détection dans un tableau.

- Survolez le ou les nœuds concernant un jour particulier pour consulter le nombre total de détections de la catégorie de détection affichée. Cliquez sur un nœud pour accéder à l'écran de consignation **Résumé des logiciels de rançon** qui répertorie les détails de détection des logiciels de rançon pour ce jour particulier.

Journaux de résumé des logiciels de rançon

Vous pouvez afficher ces informations en cliquant sur un nœud du graphique ou sur un nombre de détections du widget **Résumé des logiciels de rançon**.

- Utilisez les listes **Canal d'infection** et **Période** pour régler la vue.
- Cliquez sur **Exporter** pour enregistrer les événements de journaux dans un fichier CSV.

Colonne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de détection de logiciels de rançon à Worry-Free Business Security

Colonne	Description
Menace de sécurité	Type de logiciel de rançon • Nom du virus/programme malveillant : affiche le nom de la détection d'un fichier de logiciel de rançon connu • Chiffrement de fichier non autorisé : s'affiche lorsque Worry-Free Business Security détecte qu'un programme suspect a chiffré un fichier • <URL> : s'affiche lorsque Worry-Free Business Security détecte une URL associée au logiciel de rançon connu
Source	Type de scan qui a détecté la menace
Chemin/URL	• Chemin d'accès du logiciel de rançon • URL infectée par un logiciel de rançon
Action entreprise	Action entreprise par Worry-Free Business Security en réponse à la détection de logiciels de rançon
Nom du périphérique	Nom du périphérique affecté
Canal d'infection	Canal de détection du logiciel de rançon
Détails	Cliquez sur **Afficher** pour afficher les détails du journal.

Logiciel de rançon : détails des journaux de surveillance des comportements

Vous pouvez afficher ces informations en cliquant sur le lien **Afficher** dans la colonne **Détails** dans l'écran de consignation des résumés des logiciels de rançon.

Ligne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de violation de la surveillance des comportements à Worry-Free Business Security
Nom du périphérique	Nom du périphérique qui a déclenché une violation de stratégie

Ligne	Description
Menace de sécurité	Type de menace de sécurité
Sujet	Sujet de l'opération
Type d'événement	Événement système lié
Cible	Cible de l'opération
Opération	Opération effectuée par l'utilisateur qui a déclenché la violation
Résultat	Action entreprise par Worry-Free Business Security en réponse à la violation de la surveillance des comportements

Logiciels de rançon : Détails des journaux de filtrage des URL

Vous pouvez afficher ces informations en cliquant sur le lien **Afficher** dans la colonne **Détails** dans l'écran de consignation des résumés des logiciels de rançon.

Ligne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de violation d'URL à Worry-Free Business Security
Nom du périphérique	Nom du périphérique tentant d'accéder à une URL interdite
URL	URL interdite
Catégorie d'URL	Catégorie de l'URL interdite
Action entreprise	Action entreprise par Worry-Free Business Security en réponse à la violation d'URL

Logiciels de rançon : Détails des journaux de virus

Vous pouvez afficher ces informations en cliquant sur le lien **Afficher** dans la colonne **Détails** dans l'écran de consignation des résumés des logiciels de rançon.

Ligne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de détection de logiciels de rançon à Worry-Free Business Security
Nom du périphérique	Nom du périphérique affecté
Nom virus/prg malv	Nom du logiciel de rançon détecté Cliquez sur le lien pour être redirigé vers l'encyclopédie des menaces de Trend Micro afin d'obtenir une description approfondie de la menace ainsi que des instructions pour nettoyer manuellement des attaques correspondant à ce type de menace.
Nom du fichier	Nom du fichier corrompu par le logiciel de rançon
Chemin	Emplacement du fichier infecté
Canal d'infection	Moyen par lequel le logiciel de rançon parvient à accéder à l'endpoint
Type de scan	Type de scan utilisé pour détecter le logiciel de rançon
Action entreprise	Action entreprise par Worry-Free Business Security en réponse à la détection de logiciels de rançon

Logiciels de rançon : Détails des journaux de réputation de sites Web

Vous pouvez afficher ces informations en cliquant sur le lien **Afficher** dans la colonne **Détails** dans l'écran de consignation des résumés des logiciels de rançon.

Ligne	Description
Date/Heure	Date et heure auxquelles Security Agent a signalé les informations de violation d'URL à Worry-Free Business Security
Nom du périphérique	Nom du périphérique tentant d'accéder à une URL interdite
URL	URL interdite

Ligne	Description
Niveau de risque	évaluation attribuée par les TrendLabs selon la facilité avec laquelle l'ordinateur a pu être infecté et en fonction des dommages potentiels.
Action entreprise	Action entreprise par Worry-Free Business Security en réponse à la violation d'URL

État de la licence

Ce widget fournit une vue d'ensemble du nombre de licences et de l'état d'expiration de vos licences.

Résumé du serveur Exchange

Ce widget donne un aperçu de l'état de connexion des agents Messaging Security Agent et la distribution des menaces détectées sur vos serveurs Exchange.

Cliquez sur le niveau de sécurité pour configurer le niveau de détection de spams pour l'agent Messaging Security Agent.

Colonne	Description
Serveur	Nom du serveur Exchange
Événement	Type de spam
Pourcentage	Nombre de détections divisé par le nombre de messages scannés

État de l'agent

Ce widget fournit une vue d'ensemble de la connexion et de l'état de mise à jour des agents Security Agent de votre réseau.

- Si vous cliquez sur le nombre en regard de l'état, vous êtes redirigé vers l'écran **Dispositifs**, qui répertorie les détails des dispositifs pour cet état spécifique.
- Si vous cliquez sur **Ajouter des dispositifs**, vous êtes redirigé vers l'écran **Ajouter des dispositifs**, à partir duquel vous pouvez installer l'agent Security Agent sur d'autres dispositifs.

  Pour plus d'informations, voir *Installation des agents à la page 3-1*.
- Si vous cliquez sur **Vérifier l'état du composant**, vous êtes redirigé vers l'écran **Mise à jour manuelle**, sur lequel vous pouvez consulter les dernières informations relatives aux composants.

  Pour plus d'informations, voir *Composants pouvant être mis à jour à la page 8-4*.

Chapitre 10

Gestion des notifications

Ce chapitre explique comment utiliser les différentes options de notification.

Utilisation des Notifications

Pour réduire le temps consacré par les administrateurs à la surveillance de Worry-Free Business Security et pour vous assurer qu'ils reçoivent rapidement des avertissements par courrier électronique en cas d'épidémies imminentes, configurez le serveur pour qu'il envoie des notifications dès que des événements inhabituels se produisent sur le réseau.

Par défaut, tous les événements répertoriés sur l'écran **Notifications** sont sélectionnés et déclenchent l'envoi d'une notification aux administrateurs par le serveur.

TABLEAU 10-1. Notifications d'action requise

TYPE D'ÉVÉNEMENT	DESCRIPTION
Événements de menaces	
Antivirus - Menaces non résolues	Les mesures prises à l'encontre des menaces de virus/programmes malveillants ont échoué. Le nombre de détections n'inclut pas l'action de scan suivante : A ignoré un risque de sécurité potentiel
Antivirus - Scan en temps réel désactivé sur les points finaux	Le scan en temps réel est désactivé sur les endpoints.
Antivirus - Scan en temps réel désactivé sur les serveurs Exchange	Scan en temps réel désactivé sur les serveurs Exchange
Antispyware - Détections nécessitant le redémarrage du périphérique	Les endpoints avec détections de spywares/graywares doivent redémarrer pour supprimer définitivement les menaces.
Événements système	
Mise à jour - Agents obsolètes	Les agents Security Agent obsolètes requièrent la mise à jour de composants.
Mise à jour - Agents Messaging Security Agent obsolètes	Les agents Messaging Security Agent obsolètes nécessitent de mettre à jour des composants.

Type d'événement	Description
Mise à jour - Fichier de signatures Smart Scan obsolète	Le fichier de signatures Smart Scan nécessite une mise à jour.
Mise à jour - Composants de Security Server obsolètes	Le serveur Security Server obsolète nécessite de mettre à jour des composants.
Services Smart Protection - Service non disponible	Les clients configurés pour Smart Scan ne peuvent pas se connecter aux services Smart Protection ou le service n'est pas disponible.
Ressources insuffisantes - Espace disque disponible	L'espace disque disponible sur certains serveurs est inférieur au pourcentage spécifié.
Événements liés aux licences	
Licence - A expiré	La licence a expiré.
Licence - Expire dans moins de 60 jours	La licence va bientôt expirer.
Licence - Taux d'utilisation des licences supérieur à 110 %	L'utilisation des sièges de licence dépasse 110 %
Licence - Taux d'utilisation des licences supérieur à 100 %	L'utilisation des sièges de licence dépasse 100 %

Tableau 10-2. Notifications d’avertissement

Type d'événement	Description
Événements de menaces	
Antivirus - Nombre de virus détectés sur les endpoints supérieur à :	Le nombre de menaces de virus/programmes malveillants détectés sur les endpoints dépasse le nombre spécifié sur la période spécifiée.
Antivirus - Nombre de virus détectés sur les serveurs Exchange supérieur à :	Le nombre de menaces de virus/programmes malveillants détectés sur les serveurs Exchange dépasse le nombre spécifié dans la période de temps spécifiée.

Type d'événement	Description
Programme anti-espion - Nombre de spywares/ graywares détectés supérieur à :	Le nombre de menaces de spywares/graywares détectés sur les endpoints dépasse le nombre spécifié sur la période spécifiée.
Anti-spam - Nombre de spams détectés dans l'ensemble des messages reçus supérieur à :	Le nombre de détections de spam dans les messages reçus dépasse le poucentage spécifié.
Réputation de sites Web - Nombre de violations d'URL supérieur à :	Le nombre de violations d'URL dépasse le nombre spécifié sur la période spécifiée.
Filtrage d'URL - Nombre de violations d'URL supérieur à :	Le nombre de violations d'URL dépasse le nombre spécifié sur la période spécifiée.
Apprentissage automatique prédictif - Nombre de menaces inconnues détectées supérieur à :	Le nombre de détections de menaces inconnues dépasse le nombre spécifié sur la période spécifiée.
Surveillance des comportements - Nombre de violations de la surveillance des comportements supérieur à :	Le nombre de violations de la surveillance des comportements dépasse le nombre spécifié sur la période spécifiée.
Virus de réseau - Nombre de virus de réseau détectés supérieur à :	Le nombre de détections de virus de réseau dépasse le nombre spécifié sur la période spécifiée.
Contrôle des dispositifs - Nombre de violations de contrôle des dispositifs supérieur à :	Le nombre de violations du contrôle des dispositifs dépasse le nombre spécifié dans la période spécifiée.

Configuration d'événements pour les notifications

Worry-Free Business Security propose trois méthodes pour l'envoi de notifications :

- Notifications SNMP
- Journal des événements Windows.
- Notifications par e-mail

Procédure

1. Accédez à **Administration** > **Notifications**.
2. Pour recevoir des notifications SNMP, configurez la section **Destinataire de notification SNMP**.

   SNMP (Simple Network Management Protocol) est un protocole utilisé pour la gestion du réseau. Pour afficher les données du déroutement SNMP, utilisez un navigateur MIB (Management Information Base).

   a. Sélectionnez **Activer les notifications SNMP**.

   b. Spécifiez l'adresse IP du déroutement SNMP.

   c. Spécifiez la chaîne de communauté SNMP.
3. Pour recevoir des notifications du journal des événements Windows, sélectionnez **Écrire dans le journal des événements Windows** sous **Journalisation**.
4. Pour recevoir des notifications par e-mail, spécifiez l'expéditeur et les destinataires.

   Conseil

   Séparez les entrées multiples par des points-virgules.
5. Cliquez sur l'onglet **Action requise** ou **Avertissements**.
6. Cochez les cases correspondant aux types d'événements pour lesquels vous souhaitez recevoir des notifications dans la colonne **Notification par e-mail**.
7. Si la colonne **Seuil d'alerte** le permet, spécifiez le nombre de détections ou de violations au sein de chaque période déclenchant une notification.

8. Pour personnaliser la ligne d'objet et le corps du message de chaque notification d'événement, cliquez sur le lien de notification dans la colonne **Type**.

   Pour plus d'informations sur la personnalisation des notifications, voir *Variables de jetons à la page 10-6*.

9. Cliquez sur **Enregistrer**.

Variables de jetons

Utilisez des variables de jeton afin de personnaliser la ligne d'objet et le corps du message des notifications d'événements.

Pour éviter que les adresses e-mail des domaines externes soient considérées comme du spam, ajoutez les adresses e-mail externes dans les listes d'anti-spam Expéditeurs approuvés.

Les jetons suivants représentent les menaces détectées sur les ordinateurs/serveurs et sur les serveurs Microsoft Exchange.

Jeton	Description	Type d'alerte
%COUNT	Insère le nombre de détections.	Événements d'avertissement : Tout
$CSM_SERVERNAME	Insère le nom du serveur Security Server	Tout
%DATE	Insère le nombre de jours restants sur la licence.	Licence - A expiré Licence - Expire dans moins de 60 jours

Jeton	Description	Type d'alerte
%DATE_TIME	Insère la date et l'heure de l'événement.	Antivirus - Menaces non résolues Antivirus - Scan en temps réel désactivé sur les points finaux Antivirus - Scan en temps réel désactivé sur les serveurs Exchange Antispyware - Détections nécessitant le redémarrage du périphérique Mise à jour - Agents obsolètes Mise à jour - Agents Messaging Security Agent obsolètes Mise à jour - Composants de Security Server obsolètes Services Smart Protection - Service non disponible Ressources insuffisantes - Espace disque disponible

Jeton	Description	Type d'alerte
%DEVICE_COUNT	Insère le nombre de dispositifs affectés	Antivirus - Menaces non résolues Antivirus - Scan en temps réel désactivé sur les points finaux Antivirus - Scan en temps réel désactivé sur les serveurs Exchange Antispyware - Détections nécessitant le redémarrage du périphérique Mise à jour - Agents obsolètes Mise à jour - Agents Messaging Security Agent obsolètes Ressources insuffisantes - Espace disque disponible Tous les événements d'avertissement excepté : Anti-spam - Nombre de spams détectés dans l'ensemble des messages reçus supérieur à :
%FROM	Insère l'heure de début et la date de l'événement.	Tous les événements d'avertissement excepté : Anti-spam - Nombre de spams détectés dans l'ensemble des messages reçus supérieur à :

Jeton	Description	Type d'alerte
%NUMBER	Répertorie le nombre d'événements.	Antivirus - Menaces non résolues Antivirus - Scan en temps réel désactivé sur les points finaux Antivirus - Scan en temps réel désactivé sur les serveurs Exchange Antispyware - Détections nécessitant le redémarrage du périphérique Tous les événements d'avertissement excepté : Anti-spam - Nombre de spams détectés dans l'ensemble des messages reçus supérieur à :
%SEAT_IN_USE_COUNT	Insère le nombre de sièges de postes de travail/serveurs en cours d'utilisation.	Licence - L'utilisation de vos licences de poste dépasse 110 % Licence - L'utilisation de vos licences de poste dépasse 100 %
%SEAT_PURCHASED_COUNT	Insère le nombre de sièges de postes de travail/serveurs disponibles dans votre licence.	Licence - L'utilisation de vos licences de poste dépasse 110 % Licence - L'utilisation de vos licences de poste dépasse 100 %

Jeton	Description	Type d'alerte
%THRESHOLD%	Fournit le seuil d'un événement.	Mise à jour - Agents obsolètes Mise à jour - Fichier de signatures Smart Scan obsolète Mise à jour - Composants de Security Server obsolètes Services Smart Protection - Service non disponible Ressources insuffisantes - Espace disque disponible Licence - Taux d'utilisation des licences supérieur à 110 % Licence - Taux d'utilisation des licences supérieur à 100 % Événements d'avertissement : Tout
%TO	Insère la date et l'heure de fin de l'événement.	Tous les événements d'avertissement excepté : Anti-spam - Nombre de spams détectés dans l'ensemble des messages reçus supérieur à :

```
Objet : [Security Server - <$CSM_SERVERNAME>] [Action
requise] Antivirus - Menaces non résolues : %NUMBER
Message : Notification de Trend Micro Worry-Free Business Security
* Antivirus - Menaces non résolues : %NUMBER
* Heure du rapport : %DATE_TIME
* Dispositifs affectés : %DEVICE_COUNT
* Suggestion :
  Exécutez un scan via l'outil Trend Micro HouseCall.
```

```
Objet : [Security Server - Server A] [Action requise]
Antivirus - Menaces non résolues : 5
Message : Notification de Trend Micro Worry-Free Business Security
* Antivirus - Menaces non résolues : 5
* Heure du rapport : 14 février 2018
* Dispositifs affectés : 2
* Suggestion :
  Exécutez un scan via l'outil Trend Micro HouseCall.
```

Chapitre 11

Gestion des paramètres généraux

Ce chapitre aborde les paramètres généraux des agents et les paramètres système de Security Server.

Paramètres généraux

Dans la console Web, vous pouvez configurer les paramètres généraux de Security Server et des agents Security Agent.

Onglet	Description
Proxy	Si le réseau utilise un serveur proxy pour se connecter à Internet, spécifiez les paramètres de serveur proxy pour les services suivants : • Mises à jour de composants et notification de licences • Réputation de sites Web, surveillance des comportements et Smart Scan Pour plus de détails, voir *Configuration des paramètres de proxy Internet à la page 11-3*.
SMTP	Les paramètres du serveur SMTP s'appliquent à toutes les notifications et à tous les rapports générés par le serveur Security Server. Pour plus de détails, voir *Configuration des paramètres du serveur SMTP à la page 11-4*.
Poste de travail/serveur	Les paramètres de sécurité s'appliquent à tous les agents Security Agent. Pour plus de détails, voir *Configuration des paramètres des postes de travail/serveurs à la page 11-5*.
Système	Les paramètres système vous permettent de supprimer automatiquement les agents inactifs, de vérifier la connexion des agents et de gérer le dossier de quarantaine. Pour plus de détails, voir *Configuration des paramètres système à la page 11-10*.
Exceptions	Les listes d'exceptions vous permettent de remplacer les paramètres de stratégie définis dans la réputation des sites Web, le filtrage d'URL et l'apprentissage automatique prédictif. Pour plus d'informations, voir *Configuration des paramètres de liste d'exceptions à la page 11-14*.

Configuration des paramètres de proxy Internet

Si le serveur Security Server et les agents utilisent un serveur proxy pour la connexion à Internet, indiquez les paramètres de serveur proxy afin d'utiliser les fonctions et les services Trend Micro ci-dessous :

- **Security Server** : mises à jour de composants et maintenance de licences
- **Agents Security Agent** : réputation de sites Web, filtrage d'URL, surveillance des comportements, Smart Feedback et Smart Scan
- **Messaging Security Agent** (Advanced uniquement) : réputation de sites Web et anti-spam

Procédure

1. Accédez à **Administration** > **Paramètres généraux**.
2. Sous l'onglet **Proxy**, mettez à jour les éléments suivants, si nécessaire :
    - Serveur proxy Security Server

      Remarque

      Les agents Messaging Security Agent utilisent aussi les paramètres proxy de Security Server.

        - Utiliser un serveur proxy pour les notifications de mise à jour et de licence
        - Utiliser le protocole de serveur proxy SOCKS 4/5
        - Adresse : adresse IPv4/IPv6 ou nom d'hôte
        - Port
        - Authentification de serveur proxy
            - Nom de l'utilisateur

- Mot de passe

- Proxy Security Agent
  - Utiliser les informations spécifiées pour la mise à jour proxy

    Remarque

    Les agents Security Agent utilisent le serveur proxy et le port d'Internet Explorer pour se connecter à Internet. Sélectionnez cette option si Internet Explorer sur les clients et le serveur Security Server partagent les mêmes informations d'authentification.

  - Nom de l'utilisateur
  - Mot de passe

3. Cliquez sur **Enregistrer**.

Configuration des paramètres du serveur SMTP

Les paramètres du serveur SMTP s'appliquent à toutes les notifications et à tous les rapports générés par Worry-Free Business Security.

Procédure

1. Accédez à **Administration** > **Paramètres généraux**.
2. Cliquez sur l'onglet **SMTP** et mettez à jour les éléments suivants, si nécessaire :
   - **Serveur SMTP** : adresse IPv4/IPv6 ou nom du serveur SMTP.
   - **Port**
   - **Activer l'authentification du serveur SMTP**
     - Nom de l'utilisateur

- Mot de passe

3. Pour vérifier si les paramètres sont corrects, cliquez sur **Envoyer le message de test**. En cas d'échec de l'envoi, modifiez les paramètres ou vérifiez l'état du serveur SMTP.

4. Cliquez sur **Enregistrer**.

Configuration des paramètres des postes de travail/serveurs

Les options du poste de travail/serveur font partie des paramètres généraux de Worry-Free Business Security. Les paramètres des groupes individuels remplacent ces paramètres. Si vous n'avez pas configuré d'option particulière pour un groupe, les options du poste de travail/serveur sont utilisées. Par exemple, si aucun URL n'est appliqué pour un groupe particulier, tous les URL approuvés sur cet écran pourront être appliqués au groupe.

Procédure

1. Accédez à **Administration** > **Paramètres généraux**.

2. Cliquez sur l'onglet **Poste de travail/serveur** et mettez à jour les éléments suivants au besoin :

Paramètres	Description
Détection d'emplacement	Grâce à la détection d'emplacement, les administrateurs peuvent contrôler les paramètres de sécurité en fonction de la façon dont le client est connecté au réseau. La détection d'emplacement contrôle les paramètres de connexion au bureau/hors du bureau. Security Agent identifie automatiquement l'emplacement du client en fonction des informations de passerelle configurées dans la console Web, puis contrôle les sites Web auxquelles les

Paramètres	Description

	utilisateurs peuvent accéder. Les restrictions diffèrent en fonction de l'emplacement de l'utilisateur :
	• **Activer la détection d'emplacement** : ces paramètres affecteront les paramètres de connexion au bureau/hors du bureau du pare-feu, de la réputation de sites Web et de la fréquence des mises à jour programmées.
	• **Informations de passerelle** : les clients et connexions de cette liste utiliseront les paramètres de connexion interne lorsqu'ils se connecteront au réseau à distance (à l'aide d'un VPN) et que la détection d'emplacement sera activée.
	  • Adresse IP de passerelle
	  • Adresse MAC : l'ajout de l'adresse MAC améliore considérablement la sécurité en permettant uniquement au dispositif configuré de se connecter.
	Pour supprimer une entrée, cliquez sur l'icône de suppression (x) correspondante.

Avertissement du centre d'assistance	L'avertissement du centre d'assistance envoie une notification à l'agent Security Agent indiquant à l'utilisateur la personne à contacter pour obtenir de l'aide. Mettez à jour les éléments suivants, si nécessaire : • **Étiquette du centre d'assistance** • **Adresse e-mail du centre d'assistance** • **Informations complémentaires** : ces informations s'affichent lorsque l'utilisateur survole l'étiquette avec la souris.
Paramètres de scan généraux	• **Désactiver le service Smart Scan** : tous les agents Security Agent basculent en mode de scan traditionnel. Pour que Smart Scan soit à nouveau disponible, il doit être réactivé ici. Pour faire basculer un ou plusieurs groupes d'agents Security Agent, accédez à **Dispositifs** > **{Groupe}** > **Configurer la stratégie** > **Méthode de scan**.

Paramètres	Description
	Remarque Pour des instructions sur le changement de la méthode de scan des agents Security Agent, voir *Configuration des méthodes de scan à la page 5-5*. • **Activer le scan différé sur les opérations de fichier** : activez ce paramètre pour améliorer temporairement les performances du système. **AVERTISSEMENT!** L'activation du scan différé peut engendrer des risques de sécurité. • **Exclure les sections de clichés instantanés** : les services de Shadow Copy ou de Volume Snapshot (copies instantanées de volumes) effectuent des instantanés ou des copies de sauvegarde automatique ou manuelle d'un fichier ou d'un dossier sur un volume spécifique. • **Exclure la base de données du serveur Security Server** : empêche les agents installés sur le serveur Security Server de scanner sa base de données, uniquement durant les scans en temps réel. Par défaut, WFBS ne scanne pas sa propre base de données. Trend Micro recommande de garder cette case cochée afin d'éviter toute corruption éventuelle de la base de données susceptible de survenir lors du scan. • **Exclure les dossiers de serveur Microsoft Exchange lors d'une installation sur serveur Microsoft Exchange** : empêche les agents installés sur le serveur Microsoft Exchange de scanner les dossiers Microsoft Exchange. • **Exclure les dossiers de contrôleur de domaine Microsoft** : empêche les agents installés sur le contrôleur de domaine de scanner les dossiers de contrôleur de domaine. Ces dossiers stockent les informations relatives aux utilisateurs, noms d'utilisateurs, mots de passe et autres informations importantes.

Paramètres	Description
Paramètres de scan antivirus	• **Configurer les paramètres de scan des fichiers compressés volumineux** : indiquez la taille maximale du fichier extrait et le nombre de fichiers dans le fichier compressé que l'agent doit scanner. • **Nettoyer les fichiers compressés** : les agents essaieront de nettoyer les fichiers infectés d'un fichier compressé. • **Scanner jusqu'à { } couche(s) OLE** : les agents scanneront le nombre indiqué de couches OLE (Object Linking and Embedding). OLE permet aux utilisateurs de créer des objets dans une application puis de les lier ou de les imbriquer dans une autre application. Par exemple, un fichier .xls incorporé dans un fichier .doc. • **Ajouter le scan manuel au menu contextuel Windows sur les clients** : ajoute un lien **Scanner avec Security Agent** au menu contextuel. Ainsi, les utilisateurs peuvent cliquer avec le bouton droit sur un fichier ou un dossier (sur le Bureau ou dans l'Explorateur Windows) pour le scanner manuellement.
Paramètres de scan anti-spywares/ graywares	• **Recherche de cookies** : Security Agent recherche des cookies. • **Ajouter les détections de cookies au journal de programmes espions** : ajoute chaque cookie de programme espion détecté au journal de programmes espions.
Paramètres du pare-feu	Cochez la case **Désactiver le pare-feu et désinstaller les pilotes** pour désinstaller le pare-feu du client Worry-Free Business Security et supprimer les pilotes qui lui sont associés.  **Remarque** Si vous désactivez le pare-feu, les paramètres de celui-ci ne seront disponibles que lorsque vous l'activerez de nouveau.
Protection contre les menaces Web HTTPS	Activez cette fonction pour vérifier les URL HTTPS par rapport aux paramètres de réputation de sites Web et de filtrage d'URL dans Chrome, Firefox et Microsoft Edge.

PARAMÈTRES	DESCRIPTION
	Remarque Cette fonction ne requiert pas de module complémentaire de navigateur supplémentaire. Par défaut, Worry-Free Business Security vérifie les URL HTTPS sur Internet Explorer à l'aide de modules complémentaires de navigateur.
Paramètres d'alerte	**Afficher l'icône d'alerte dans la barre des tâches Windows si le fichier de signatures de virus n'a pas été mis à jour après {} jour(s)** : affiche une icône d'alerte sur les clients lorsque le fichier de signatures n'est pas mis à jour après un certain nombre de jours
Mot de passe de désinstallation de Security Agent	• **Autoriser l'utilisateur client à désinstaller Security Agent sans mot de passe.** • **Demander un mot de passe à l'utilisateur client lors de la désinstallation de Security Agent.**
Mot de passe de fermeture et de déverrouillage du programme Security Agent	• **Autoriser les utilisateurs clients à fermer et déverrouiller Security Agent sur leur ordinateur sans mot de passe.** • **Demander aux utilisateurs clients d'entrer un mot de passe pour fermer et déverrouiller Security Agent.** **Remarque** Le déverrouillage de l'agent Security Agent permet à l'utilisateur de remplacer tous les paramètres configurés sous **Dispositifs** > **{groupe}** > **Configurer la stratégie** > **Privilèges agent**.
Adresse IP de votre choix	Ce réglage n'est disponible que sur les serveurs Security Server à double pile et ne s'applique qu'aux agents à double pile. Après avoir installé ou mis à niveau les agents, ceux-ci s'enregistrent sur Security Server en utilisant une adresse IP. Sélectionnez l'une des options suivantes : • **IPv4 d'abord, puis IPv6** : les agents utilisent d'abord leur adresse IPv4. Si l'agent ne peut pas s'enregistrer en utilisant son adresse IPv4, il utilise alors son adresse IPv6. En cas

Paramètres	Description
	d'échec de l'enregistrement avec les deux adresses IP, l'agent essaye à nouveau en utilisant l'ordre de priorité établi. • **IPv6 d'abord, puis IPv4** : les agents utilisent d'abord leur adresse IPv6. Si l'agent ne peut pas s'enregistrer en utilisant son adresse IPv6, il utilise alors son adresse IPv4. En cas d'échec de l'enregistrement avec les deux adresses IP, l'agent essaye à nouveau en utilisant l'ordre de priorité établi.

3. Cliquez sur **Enregistrer**.

Configuration des paramètres système

La section **Système** de l'écran **Paramètres généraux** contient des options permettant de supprimer des agents inactifs, de vérifier la connexion des agents et d'effectuer la maintenance du dossier de quarantaine, de façon automatique.

Procédure

1. Accédez à **Administration** > **Paramètres généraux**.
2. Cliquez sur l'onglet **Système** et mettez à jour les éléments suivants, si nécessaire :

Paramètres	Description
Suppression des agents Security Agent inactifs	Lorsque vous utilisez le programme de désinstallation de Security Agent sur le client pour supprimer des agents d'un ordinateur client, le programme en informe automatiquement Security Server. Dès que Security Server reçoit cette notification, il supprime l'icône du client de l'arborescence des groupes de sécurité, indiquant ainsi que le client n'existe plus. Cependant, si Security Agent est supprimé d'une autre façon (reformatage du disque dur de l'ordinateur ou suppression manuelle des fichiers clients, par exemple), Security Server n'est pas informé de cette suppression et affiche Security Agent comme étant inactif. Si un utilisateur décharge ou désactive l'agent sur une longue période, Security Server affiche également Security Agent comme étant inactif. Pour que l'arborescence des groupes de sécurité affiche uniquement les clients actifs, vous pouvez configurer Security Server de telle sorte qu'il supprime automatiquement de l'arborescence des groupes de sécurité tous les agents Security Agent inactifs. • **Activer la suppression automatique de Security Agent lorsqu'il est inactif** : permet la suppression automatique des clients qui n'ont pas été en contact avec le serveur Security Server pendant le nombre de jours indiqué. • **Supprimer automatiquement un agent Security Agent s'il est inactif pendant {} jours** : nombre de jours pendant lequel un client peut rester inactif avant d'être supprimé à partir de la console Web.

Paramètres	Description

Vérification de la connexion de l'agent	Dans Worry-Free Business Security, l'état de la connexion du client est représenté par des icônes dans l'arborescence des groupes de sécurité. Cependant, dans certains cas, l'affichage de l'état de la connexion de l'agent dans l'arborescence des groupes de sécurité est impossible. Par exemple, si le câble réseau d'un client est accidentellement débranché, l'agent ne pourra pas informer Trend Micro Security Server qu'il se trouve hors ligne. Cet agent apparaîtra comme étant encore en ligne dans l'arborescence des groupes de sécurité.
	
	Vous pouvez vérifier la connexion agent-serveur manuellement ou par le biais d'une programmation à partir de la console Web.
	
	Remarque
	La vérification de la connexion ne permet pas de sélectionner des groupes ou agents spécifiques. Elle vérifie la connexion de tous les agents enregistrés auprès du serveur Security Server.
	
	• **Activer la vérification programmée** : active la vérification programmée de la connexion agent-serveur.
	  • **Horaire**
	  • **Quotidien**
	  • **Hebdomadaire, tous les**
	  • **Heure de début** : heure à laquelle la vérification doit commencer.
	• **Vérifier maintenant** : teste immédiatement la connectivité.

Paramètres	Description
Maintenance de la mise en quarantaine	Par défaut, les agents Security Agent transfèrent les fichiers infectés en quarantaine dans le répertoire suivant du serveur Security Server : `<Dossier d'installation de Security Server>\PCCSRV\Virus` Si vous devez modifier le répertoire (par exemple, s'il ne possède pas suffisamment d'espace disponible), saisissez un chemin absolu, tel que `D:\Quarantined Files`, dans le champ **Répertoire de quarantaine**. Le cas échéant, veuillez également appliquer les modifications dans **Dispositifs** > **{Groupe}** > **Configurer la stratégie** > **Quarantaine** ou les agents poursuivront l'envoi de fichiers dans `<dossier d'installation du serveur Security Server>\PCCSRV\Virus`. Par ailleurs, configurez les paramètres de maintenance suivants : • **Capacité du dossier de quarantaine** : taille du dossier de quarantaine en Mo. • **Taille maximale d'un fichier unique** : taille maximale d'un fichier unique stocké dans le dossier de quarantaine, en Mo. • **Supprimer tous les fichiers mis en quarantaine** : supprime tous les fichiers du dossier de quarantaine. Si le dossier est plein et qu'un nouveau fichier est téléchargé, il n'y est pas stocké. Si vous ne souhaitez pas que les agents envoient les fichiers en quarantaine sur le serveur Security Server, configurez le nouveau répertoire dans **Dispositifs** > **{Groupe}** > **Configurer la stratégie** > **Quarantine** et ignorez l'ensemble des paramètres de maintenance. Voir *Répertoire de quarantaine à la page 5-18* pour obtenir des instructions détaillées.

Paramètres	Description
Installation de Security Agent	**Répertoire d'installation de Security Agent** : lors de l'installation, vous êtes invité à saisir le répertoire d'installation de l'agent Security Agent, dans lequel le programme installe chaque agent Security Agent. Si nécessaire, modifiez le répertoire en saisissant un chemin absolu. Seuls les futurs agents seront installés dans le répertoire ; les agents existants conservent leur répertoire actuel. Utilisez l'une des variables suivantes pour définir le chemin d'installation : • `$BOOTDISK` : Lettre de lecteur du disque de démarrage • `$WINDIR` : Dossier d'installation de Windows • `$ProgramFiles` : Dossier des programmes

3. Cliquez sur **Enregistrer**.

Configuration des paramètres de liste d'exceptions

Procédure

1. Accédez à **Administration** > **Paramètres généraux**.
2. Cliquez sur l'onglet **Exceptions** et configurez les éléments suivants selon les besoins :

Section	Description
Réputation des sites Web et filtrage d'URL	• **Liste des URL approuvées** : sites Web (et leurs sous-domaines) exclus des vérifications de la réputation de sites Web et du filtrage d'URL.

Section	Description
	Remarque La liste des URL approuvées est prioritaire sur la liste des URL bloquées. Lorsqu'une URL correspond à une entrée de la liste approuvée, les agents autorisent toujours l'accès à cette URL, même si elle figure dans la liste des URL bloquées. La personnalisation des URL approuvées ou bloquées pour un groupe donné remplace les paramètres d'exception généraux. • **Liste des URL bloquées** : sites Web (et leurs sous-domaines) toujours bloqués lors du filtrage d'URL. • **Liste d'exceptions de processus** :traite les éléments exclus des vérifications Réputation de sites Web et Filtrage d'URL. Entrez les processus critiques que votre entreprise estime fiables. **Conseil** Lorsque vous mettez à jour la liste des exceptions de processus et que le serveur déploie la liste mise à jour sur les agents, toutes les connexions HTTP actives sur l'ordinateur client (par le port 80, 81 ou 8080) seront déconnectées pendant quelques secondes. Envisagez de mettre à jour la liste des exceptions de processus durant les heures de pointe. • **Liste d'exceptions IP** :adresses IP (par ex., 192.168.0.1) exclues des vérifications de la réputation des sites Web et du filtrage d'URL. Saisissez les adresses IP importantes que votre entreprise juge dignes de confiance. • **Envoyer des journaux de réputation de sites Web et de filtrage d'URL à Security Server**

Section	Description
Liste d'exceptions de l'apprentissage automatique prédictif	Configurez les exceptions globales des fichiers d'apprentissage automatique prédictif pour éviter que tous les agents Security Agent ne détectent un fichier comme malveillant. Entrez la valeur de hachage SHA-1 à exclure du scan. Vous pouvez éventuellement ajouter un commentaire justifiant l'exception ou décrivant les noms de fichier associés à la valeur de hachage.

3. Cliquez sur **Enregistrer**.

Chapitre 12

Utilisation des journaux et des rapports

Ce chapitre décrit comment utiliser les journaux et les rapports pour surveiller votre système et analyser votre mécanisme de protection.

Journaux

Worry-Free Business Security met à votre disposition des journaux complets concernant les incidents de virus/programmes malveillants et de spywares/graywares, les événements et les mises à jour. Utilisez ces journaux pour évaluer les stratégies de protection de votre entreprise, identifier les clients exposés à un risque d'infection plus élevé et vérifier que les mises à jour ont été correctement déployées.

Remarque

utilisez un tableur tel que Microsoft Excel pour afficher les fichiers journaux CSV.

Worry-Free Business Security répartit les journaux dans les catégories suivantes :

- Journaux des événements de la console Web
- Journaux de poste de travail/serveur
- Journaux du serveur Microsoft Exchange (Advanced uniquement)

TABLEAU 12-1. Type de journal et contenu

TYPE (ENTITÉ QUI A GÉNÉRÉ L'ENTRÉE DE JOURNAL)	CONTENU (TYPE DE JOURNAL DONT VOUS SOUHAITEZ OBTENIR LE CONTENU)
Événements de console d'administration	• Scan manuel (lancé à partir de la console Web) • Mise à jour (mises à jour de Security Server) • Événements de console

Type (entité qui a généré l'entrée de journal)	Contenu (type de journal dont vous souhaitez obtenir le contenu)

Poste de travail/serveur	• Journaux de virus
	  • Scan manuel
	  • Scan en temps réel
	  • Scan programmé
	• Journaux de spywares/graywares
	  • Scan manuel
	  • Scan en temps réel
	  • Scan programmé
	• Journaux de l'apprentissage automatique prédictif
	• Journaux de réputation de sites Web
	• Journaux de filtrage d'URL
	• Journaux de surveillance des comportements
	• Journaux de mise à jour
	• Journaux de virus de réseau
	• Journaux des événements
	• Journaux de contrôle des dispositifs
	• Journaux de déploiement des mises à jour
	• Journaux des logiciels de rançon
	  • Antivirus
	  • Surveillance des comportements
	  • Réputation de sites Web
	  • Filtrage d'URL
	  • Apprentissage automatique prédictif

Type (entité qui a généré l'entrée de journal)	Contenu (type de journal dont vous souhaitez obtenir le contenu)
Serveur Exchange (Advanced uniquement)	• Journaux de virus • Journaux de blocage de pièces jointes • Filtrage de contenu/prévention de la perte de données • Journaux de mise à jour • Journaux de sauvegarde • Journaux d'archives • Journaux des événements de scan • Journaux de parties de message non scannables • Journaux de réputation de sites Web • Journaux d'événements de dispositif mobile

Utilisation d'une demande de journal

Les demandes sur le journal permettent de collecter des informations dans la base de données du journal. L'écran **Requête de journal** permet de définir et d'exécuter ces demandes. Les résultats peuvent être exportés dans un fichier au format CSV ou imprimés.

Un agent Messaging Security Agent (Advanced uniquement) envoie ses journaux à Security Server toutes les cinq minutes (peu importe le moment de la génération du journal).

Procédure

1. Accédez à **Rapports** > **Requête de journal**.
2. Mettez à jour les options suivantes, comme indiqué :
   - **Intervalle de temps**
     - **Plage préconfigurée**

- **Plage spécifiée** : pour limiter la demande à certaines dates.

- **Type** : voir *Journaux à la page 12-2* pour afficher le contenu de chaque type de journal.
  - **Événements de console d'administration**
  - **Poste de travail/serveur**
  - **Serveur Exchange** (Advanced uniquement)
- **Contenu** : les options disponibles dépendent du **type** de journal.

3. Cliquez sur **Afficher les journaux**.
4. Pour enregistrer le journal en tant que fichier au format CSV, cliquez sur **Exporter**. Utilisez un tableur pour afficher les fichiers CSV.

Rapports

Vous pouvez générer manuellement des rapports à usage unique ou paramétrer Security Server afin de générer des rapports programmés.

Vous pouvez imprimer les rapports ou les envoyer par email à un administrateur ou à d'autres personnes.

La quantité de données contenues dans un rapport dépend du nombre de journaux disponibles sur le serveur Security Server au moment de la génération du rapport. Le nombre de journaux change à mesure que de nouveaux journaux sont ajoutés et que des journaux existants sont supprimés. Sous **Rapports** > **Maintenance**, vous pouvez supprimer manuellement des journaux ou définir une programmation de suppression des journaux.

Utilisation des rapports à usage unique

Procédure

1. Accédez à **Rapports** > **Rapports à usage unique**.
2. Effectuez les actions suivantes :

TÂCHE	ÉTAPES

Générer un rapport	a. Cliquez sur **Ajouter**.
	
	Un nouvel écran s'affiche.
	
	b. Configurez les éléments suivants :
	
	• **Nom du rapport**
	
	• **Intervalle de temps** : limite le rapport à certaines dates.
	
	• **Contenu** : pour sélectionner toutes les menaces, cochez la case **Tout sélectionner**. Pour sélectionner des menaces individuelles, cochez les cases correspondantes. Cliquez sur l'icône plus (+) pour développer la sélection.
	
	• **Envoyer le rapport à**
	
	  • **Destinataires** : séparez les adresses email par un point-virgule (;).
	
	  • **Format** : choisissez un PDF ou un lien vers un rapport HTML. Si vous choisissez un PDF, celui-ci sera joint à l'email.
	
	c. Cliquez sur **Ajouter**.

TÂCHE	ÉTAPES
Afficher le rapport	Dans la colonne Nom du rapport, cliquez sur les liens menant au rapport. Le premier lien permet d'ouvrir un rapport au format PDF et le second, un rapport au format HTML. La quantité de données contenues dans un rapport dépend du nombre de journaux disponibles sur le serveur Security Server au moment de la génération du rapport. Le nombre de journaux change à mesure que de nouveaux journaux sont ajoutés et que des journaux existants sont supprimés. Sous **Rapports** > **Maintenance**, vous pouvez supprimer manuellement des journaux ou définir une programmation de suppression des journaux. Pour obtenir plus d'informations sur le contenu du rapport, voir *Interprétation de rapports à la page 12-12*.
Supprimer des rapports	a. Sélectionnez la ligne contenant les liens menant aux rapports. b. Cliquez sur **Supprimer**. **Remarque** Pour supprimer automatiquement des rapports, accédez à **Rapports** > **Maintenance** > **onglet Rapports** et définissez le nombre maximal de rapports à usage unique que Worry-Free Business Security doit conserver. Le nombre par défaut est 10. Lorsque cette limite est dépassée, Security Server supprime des rapports en commençant par les plus anciens.

Utilisation des rapports programmés

Procédure

1. Accédez à **Rapports** > **Rapports programmés**.
2. Effectuez les actions suivantes :

TÂCHE	ÉTAPES
Créer un modèle de rapport programmé	a. Cliquez sur **Ajouter**. Un nouvel écran s'affiche. b. Configurez les éléments suivants : • **Nom du modèle de rapport** • **Programmation** : quotidienne, hebdomadaire ou mensuelle, et l'heure de génération du rapport. Pour les rapports mensuels, si vous sélectionnez 31, 30 ou 29 jours et qu'un mois comporte moins de jours que le nombre programmé, WFBS ne créera pas de rapport pour ce mois. • **Contenu** : pour sélectionner toutes les menaces, cochez la case **Tout sélectionner**. Pour sélectionner des menaces individuelles, cochez les cases correspondantes. Cliquez sur l'icône plus (+) pour développer la sélection. • **Envoyer le rapport à** • **Destinataires** : séparez les adresses email par un point-virgule (;). • **Format** : choisissez un PDF ou un lien vers un rapport HTML. Si vous choisissez un PDF, celui-ci sera joint à l'email. c. Cliquez sur **Ajouter**.

TÂCHE	ÉTAPES
Afficher les rapports programmés	a. Sur la ligne contenant le modèle à partir duquel les rapports programmés sont générés, cliquez sur **Historique de rapports**. Un nouvel écran s'affiche. b. Dans la colonne Affichage, cliquez sur les liens menant à un rapport. Le premier lien permet d'ouvrir un rapport au format PDF et le second, un rapport au format HTML. La quantité de données contenues dans un rapport dépend du nombre de journaux disponibles sur le serveur Security Server au moment de la génération du rapport. Le nombre de journaux change à mesure que de nouveaux journaux sont ajoutés et que des journaux existants sont supprimés. Sous **Rapports** > **Maintenance**, vous pouvez supprimer manuellement des journaux ou définir une programmation de suppression des journaux. Pour obtenir plus d'informations sur le contenu du rapport, voir *Interprétation de rapports à la page 12-12*.
Tâches de maintenance du modèle	
Modifier les paramètres du modèle	Cliquez sur le modèle et modifiez-en les paramètres dans l'écran qui s'affiche. Tous les rapports générés après l'enregistrement des modifications se baseront sur les nouveaux paramètres.
Activer/Désactiver un modèle	Cliquez sur l'icône dans la colonne Activé. Désactivez un modèle si vous souhaitez ne plus générer de rapports programmés et réactivez-le lorsque vous aurez à nouveau besoin de la fonction.

TÂCHE	ÉTAPES
Supprimer un modèle	Sélectionnez un modèle et cliquez sur **Supprimer**. Supprimer un modèle ne permet pas de supprimer également les rapports programmés qui en découlent ; en revanche, les liens menant aux rapports dans la console Web ne seront plus disponibles. Les rapports sont accessibles directement à partir de l'ordinateur Security Server. Les rapports ne seront supprimés que par une action manuelle à partir de l'ordinateur ou si le serveur Security Server supprime automatiquement les rapports conformément au paramètre de suppression automatique défini dans le rapport programmé dans **Rapports** > **Maintenance** > **onglet Rapports**. Pour supprimer automatiquement des modèles, accédez à **Rapports** > **Maintenance** > **onglet Rapports** et définissez le nombre maximal de modèles que Worry-Free Business Security doit conserver. La valeur par défaut est 10. Lorsque cette limite est dépassée, Security Server supprime des modèles en commençant par les plus anciens.
Tâches de maintenance de rapports	

TÂCHE	ÉTAPES
Envoyer un lien menant aux rapports programmés	Envoyez un email contenant un lien menant aux rapports programmés (au format PDF). Il suffit aux destinataires de cliquer sur le lien contenu dans le message pour accéder au fichier PDF. Assurez-vous que les destinataires arrivent à se connecter à l'ordinateur Security Server ; s'ils n'y parviennent pas, le fichier ne s'affichera pas. **Remarque** L'email ne contient qu'un lien menant au fichier PDF. Il ne contient pas le fichier lui-même en pièce jointe. a. Sur la ligne contenant le modèle à partir duquel les rapports programmés sont générés, cliquez sur **Historique de rapports**. Un nouvel écran s'affiche. b. Sélectionnez les rapports et cliquez sur **Envoyer**. Le client de messagerie par défaut, contenant le nouveau message et le lien menant au rapport, s'ouvre.
Supprimer des rapports programmés	a. Sur la ligne contenant le modèle à partir duquel les rapports programmés sont générés, cliquez sur **Historique de rapports**. Un nouvel écran s'affiche. b. Sélectionnez des rapports et cliquez sur **Supprimer**. **Remarque** Pour supprimer automatiquement des rapports, accédez à **Rapports** > **Maintenance** > **onglet Rapports** et définissez le nombre maximal de rapports programmés que Worry-Free Business Security doit conserver dans chaque modèle. Le nombre par défaut est 10. Lorsque cette limite est dépassée, Security Server supprime des rapports en commençant par les plus anciens.

Interprétation de rapports

Les rapports Worry-Free Business Security contiennent les informations suivantes. Les informations affichées dépendent des options sélectionnées.

TABLEAU 12-2. Contenu d'un rapport

ÉLÉMENT DE RAPPORT	DESCRIPTION
Antivirus	**Récapitulatif des virus sur les postes de travail et les serveurs** Les rapports sur les virus affichent des informations détaillées sur le nombre et le type de virus/programmes malveillants détectés par le moteur de scan ainsi que les actions antivirus entreprises. Le rapport répertorie également les noms des principaux virus/programmes malveillants. Cliquez sur les noms des virus/programmes malveillants pour ouvrir une nouvelle page Web et la rediriger vers l'encyclopédie des virus de Trend Micro afin d'en savoir plus sur ce virus/programme malveillant.
	5 principaux postes de travail/serveurs sur lesquels des virus ont été détectés Affiche les 5 premiers postes de travail ou serveurs sur lesquels des virus/programmes malveillants ont été détectés. La détection d'incidents de virus/programmes malveillants fréquents sur le même client peut indiquer que ce client représente un risque élevé pour la sécurité, nécessitant une investigation supplémentaire.

Élément de rapport	Description
Anti-spyware	**Récapitulatif des spywares/graywares sur les postes de travail/ serveurs** Le rapport sur les spywares/graywares affiche des informations détaillées sur les spywares/graywares détectés sur les clients, ainsi que le nombre de détections et les actions entreprises par WFBS contre ces menaces. Le rapport contient un diagramme circulaire affichant le pourcentage de chaque action de scan anti-spyware effectuée.
	5 principaux postes de travail/serveurs sur lesquels des spywares/ graywares ont été détectés Le rapport affiche également les cinq principales menaces de spywares/graywares détectées et les cinq postes de travail/serveurs sur lesquels ont été détectés le plus grand nombre de spywares/ graywares. Pour en savoir davantage sur les menaces de spywares/ graywares détectées, cliquez sur les noms des spywares/graywares. Une nouvelle page Web s'ouvre et affiche les informations relatives aux spywares/graywares sur le site Web de Trend Micro.
Récapitulatif anti-spam (Advanced uniquement)	**Récapitulatif des spams** Les rapports anti-spam affichent des informations relatives au nombre de messages de spam et de phishing détectés parmi le nombre total de messages scannés. Le récapitulatif répertorie les faux positifs signalés.
Apprentissage automatique prédictif	**5 principaux programmes qui violent les stratégies d'apprentissage automatique prédictif**
	10 principaux ordinateurs qui violent les stratégies d'apprentissage automatique prédictif
Réputation de sites Web	**10 principaux ordinateurs enfreignant les stratégies d'évaluation de la réputation des sites Web**

Élément de rapport	Description
Catégorie d'URL	**5 principales stratégies de catégories d'URL violées** Répertorie les catégories de sites Web les plus couramment visités qui enfreignent la stratégie.
	10 principaux ordinateurs enfreignant les stratégies de catégories d'URL
Surveillance des comportements	**5 principaux programmes enfreignant les stratégies de surveillance des comportements**
	10 principaux ordinateurs enfreignant les stratégies de surveillance des comportements
Contrôle des dispositifs	**10 principaux ordinateurs enfreignant la stratégie de contrôle des dispositifs**
Récapitulatif du filtrage du contenu (Advanced uniquement)	**Récapitulatif du filtrage de contenu** Les rapports du filtrage de contenu affichent des informations sur le nombre total de messages filtrés par Messaging Security Agent.
	10 principales transgressions de règles de filtrage de contenu Liste des 10 principaux cas de transgression de règles de filtrage de contenu. Utilisez ces informations pour ajuster les règles de filtrage.
Virus réseau	**10 principaux virus réseau détectés** Répertorie les 10 virus de réseau les plus fréquemment détectés par le pilote du pare-feu commun. Cliquez sur les noms de virus pour ouvrir une nouvelle page Web et la rediriger vers l'encyclopédie des virus de Trend Micro afin d'en savoir plus sur ce virus.
	10 principaux ordinateurs attaqués Répertorie les ordinateurs de votre réseau signalant les incidents viraux les plus fréquents.

Exécution de tâches de maintenance pour les rapports et les journaux

Procédure

1. Accédez à **Rapports** > **Maintenance**.
2. Effectuez les actions suivantes :

Tâche	Étapes
Définir le nombre maximum de rapports et de modèles	Vous pouvez définir le nombre maximal de rapports à usage unique, de rapports programmés (par modèle) et de modèles disponibles sur Security Server. Lorsque cette limite est dépassée, Security Server supprime des rapports/modèles en commençant par les plus anciens. a. Cliquez sur l'onglet **Rapports**. b. Saisissez le nombre maximal de rapports à usage unique, de rapports programmés et de modèles que vous souhaitez conserver.
Configurer la suppression automatique de journaux	a. Cliquez sur l'onglet **Suppression automatique de journaux**. b. Sélectionnez les types de journaux et indiquez une date de création maximale. Les journaux créés avant cette date seront supprimés.
Supprimer des journaux manuellement	a. Cliquez sur l'onglet **Suppression manuelle de journaux**. b. Indiquez une date de création maximale pour chaque type de journal. Les journaux créés avant cette date seront supprimés. Pour supprimer tous les journaux, tapez `0`. c. Cliquez sur **Supprimer**.

3. Cliquez sur **Enregistrer**.

Chapitre 13

Exécution des tâches administratives

Ce chapitre explique comment exécuter d'autres tâches administratives comme l'affichage de la licence du produit, l'utilisation de Plug-in Manager et la désinstallation de Security Server.

Modification du mot de passe de la console Web

Trend Micro recommande l'utilisation d'un mot de passe complexe pour la console Web. Un mot de passe complexe contient au moins huit caractères, au moins une majuscule (A-Z), au moins une minuscule (a-z), au moins un chiffre (0-9) et au moins un caractère spécial ou signe de ponctuation (!@#$ %^&,.:;?). Un mot de passe complexe n'est jamais similaire au nom de connexion de l'utilisateur et ne comprend jamais ce nom. Sont à exclure le nom usuel de l'utilisateur ou son nom de famille, sa date de naissance ou tout autre élément identifiant facilement l'utilisateur.

Procédure

1. Accédez à **Administration** > **Mot de passe**.
2. Mettez à jour les options suivantes, comme indiqué :
   - **Ancien mot de passe**
   - **Nouveau mot de passe**
   - **Confirmer le mot de passe** : Tapez à nouveau le mot de passe pour le confirmer.
3. Cliquez sur **Enregistrer**.

Utilisation de Plug-in Manager

Plug-in Manager affiche les programmes du serveur Security Server et des agents dans la console Web dès qu'ils sont disponibles. Vous pouvez ensuite installer et gérer les programmes depuis la console Web, ainsi que déployer les plug-ins clients aux agents. Téléchargez et installez Plug-in Manager depuis **Administration** > **Plug-ins**. Une fois l'installation terminée, vous pouvez vérifier les plug-ins disponibles. Pour plus d'informations, consultez la documentation relative à Plug-in Manager et aux plugiciels.

Gestion de la licence du produit

À partir de l'écran Licence du produit, vous pouvez renouveler, mettre à niveau ou afficher les détails de la licence correspondante.

L'écran Licence du produit affiche les détails de votre licence. En fonction des options choisies au cours de l'installation, vous disposez soit d'une version complète, soit d'une version d'évaluation. Dans les deux cas, votre licence vous donne droit à un contrat de maintenance. Une fois votre contrat de maintenance expiré, les clients de votre réseau disposeront d'une protection très limitée. Utilisez l'écran Licence du produit pour connaître la date d'expiration de votre licence afin de veiller à la renouveler avant qu'elle expire.

Remarque

Les licences attribuées aux divers composants des produits Trend Micro peuvent varier selon les régions. Après l'installation, vous pourrez consulter un récapitulatif des composants que votre clé d'enregistrement/code d'activation vous permet d'utiliser. Vérifiez avec votre revendeur ou votre distributeur les composants pour lesquels vous possédez des licences.

Renouvellement de la licence

Vous pouvez renouveler ou mettre à niveau votre licence avec une version complète de Worry-Free Business Security en achetant un renouvellement de votre contrat de maintenance. La version complète requiert un code d'activation.

Vous pouvez renouveler la licence du produit de deux manières :

- Dans la console Web, accédez à l'écran État actuel et suivez les instructions à l'écran. Ces instructions s'affichent 60 jours avant et 30 jours après l'expiration de la licence.
- Contactez votre revendeur local ou votre distributeur Trend Micro pour renouveler votre contrat de licence.

  Les revendeurs peuvent laisser leurs coordonnées dans un fichier sur Security Server. Consultez ce fichier dans le

```
{Dossier d'installation de Security Server}\PCCSRV\Private
\contact_info.ini
```

Remarque

Le `{Dossier d'installation de Security Server}` correspond généralement à `C:\Program Files\Trend Micro\Security Server`.

Un distributeur de Trend Micro met à jour vos informations d'enregistrement à l'aide de l'enregistrement des produits Trend Micro.

Security Server interroge le serveur d'enregistrement des produits et reçoit la nouvelle date d'expiration directement à partir du serveur d'enregistrement des produits. Il n'est pas nécessaire de saisir manuellement un nouveau code d'activation lors du renouvellement d'une licence.

Activation d'une nouvelle licence

Votre type de licence détermine votre code d'activation Worry-Free Business Security.

TABLEAU 13-1. Code d'activation par type de licence

TYPE DE LICENCE	CODE D'ACTIVATION
Version complète de Worry-Free Business Security Standard	CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx
Version complète de Worry-Free Business Security Advanced	CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

Remarque

Si vous avez des questions concernant le code d'activation, contactez le site Web d'assistance Trend Micro :

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

Utilisez l'écran Licence du produit pour changer votre type de licence en saisissant un nouveau code d'activation.

1. Accédez à **Administration** > **Licence du produit**.
2. Cliquez sur **Entrer un nouveau code**.
3. Saisissez votre nouveau code d'activation dans l'espace prévu à cet effet.
4. Cliquez sur **Activer**.

Configuration des paramètres de mise à jour de produit

Configurez Worry-Free Business Security pour automatiser les mises à jour de produit.

Procédure

1. Accédez à **Administration** > **Mise à jour de produit**.

   L'onglet **Paramètres** s'affiche.

2. Sous **Paramètres de mise à jour**, sélectionnez **Activer les téléchargements de mise à jour de produit**.
3. Spécifiez l'action à mettre en œuvre lorsqu'un nouveau package de mise à jour est disponible.
   - **Télécharger** : le package de mise à jour est téléchargé automatiquement dans le dossier de téléchargement à la fréquence configurée.
   - **Télécharger et installer** : le package de mise à jour est téléchargé et installé automatiquement à la fréquence configurée.
4. Indiquez à quel moment l'action doit être exécutée.

Remarque

L'installation du package de mise à jour et le redémarrage du serveur Security Server peuvent prendre un certain temps. Il est donc recommandé de choisir le moment auquel le processus impactera le moins votre activité.

5. Cliquez sur **Enregistrer**.

Configuration des notifications de mise à jour de produit

Worry-Free Business Security peut informer les utilisateurs des mises à jour de produit lorsqu'une nouvelle version, un Service Pack ou un correctif est disponible. Vous pouvez définir les types de notifications de mise à jour de produit suivantes :

- Security Agent : Affiche une notification près de la zone de notification sur le point final.
- Courrier électronique

Procédure

1. Accédez à **Administration** > **Mise à jour de produit**.
2. Cliquez sur **Notifications**.
3. Pour recevoir des notifications de l'agent Security Agent, configurez la section **Notification de Security Agent**.
   a. Cliquez sur **Ajouter**.
   b. Sélectionnez les agents Security Agent dans la liste.
   c. Cliquez sur **Enregistrer**.

4. Pour recevoir des notifications par e-mail relatives aux mises à jour de produit, spécifiez les destinataires dans la section **Notification par e-mail**.

Remarque

Pour recevoir des notifications par e-mail, vous devez configurer l'onglet **SMTP** dans **Administration** > **Paramètres généraux**.

5. Cliquez sur **Enregistrer**.

Participation au programme Smart Feedback

Pour plus d'informations sur Smart Feedback, voir *Smart Feedback à la page 1-6*.

Procédure

1. Accédez à **Administration** > **Smart Protection Network**.
2. Cliquez sur **Activer Trend Micro Smart Feedback**.
3. Pour envoyer des informations sur des menaces de sécurité potentielles figurant dans les fichiers de vos ordinateurs clients, activez la case à cocher **Activer le retour d'informations sur les fichiers programme suspects**.

Remarque

Les fichiers envoyés à Smart Feedback ne contiennent pas de données utilisateur et ne sont utilisés que pour l'analyse des menaces.

4. Pour aider Trend Micro à mieux connaître votre entreprise, sélectionnez son **secteur d'activité**.
5. Cliquez sur **Enregistrer**.

Modification de la langue d'interface de l'agent

Par défaut, la langue utilisée sur l'interface de l'agent correspond aux paramètres régionaux configurés sur le système d'exploitation du client. Les utilisateurs peuvent modifier la langue depuis l'interface de l'agent.

Enregistrement et restauration des paramètres du programme

Vous pouvez enregistrer une copie de la base de données du serveur Security Server et des fichiers de configuration importants pour rétrograder le serveur. Cela peut s'avérer utile si vous rencontrez des problèmes et que vous voulez réinstaller Security Server ou si vous souhaitez revenir à une configuration précédente.

Procédure

1. Arrêtez Trend Micro Security Server Master Service
2. Copiez manuellement les fichiers et dossiers suivants du dossier vers un autre emplacement :

AVERTISSEMENT!

N'utilisez pas d'outils ni d'applications de sauvegarde pour cette tâche.

`<Chemin d'installation de Security Server>\PCCSRV`

- `ofcscan.ini` : contient les paramètres généraux.
- `Ous.ini`: : Contient la table de la source de mise à jour pour le déploiement du composant antivirus.
- `Dossier` privé : Contient les paramètres du pare-feu et de la source de mise à jour.
- `Pccnt\Common\OfcPfw.dat` : Contient les paramètres de pare-feu.
- `Download\OfcPfw.dat` : Contient les paramètres de déploiement du pare-feu.
- `Dossier Log` : Contient les événements système et le journal de vérification de la connexion.
- `Dossier Virus` : Dossier dans lequel WFBS met les fichiers infectés en quarantaine.
- `Dossier HTTDB` : Contient la base de données WFBS.

3. Désinstallez le serveur Security Server. Voir *Désinstallation du serveur Security Server à la page 13-10*.
4. Effectuez une nouvelle installation. Consultez le *Guide d'installation et de mise à niveau* de Worry-Free Business Security.
5. Une fois que l'exécution du programme d'installation principal est terminée, arrêtez Trend Micro Security Server Master Service sur l'ordinateur cible.
6. Mettez à jour la version du fichier de signatures de virus à partir du fichier de sauvegarde :
   a. Recherchez la version du fichier de signatures de virus en cours sur le nouveau serveur :

```
<Chemin d'installation de Security Server>\PCCSRV
\Private\component.ini. [6101]

ComponentName=Virus pattern

Version=xxxxxx 0 0
```

b. Mettez à jour la version des signatures de virus dans le fichier sauvegardé :

```
\Private\component.ini
```

Remarque

Si vous changez le chemin d'installation de Security Server, vous devrez mettre à jour les informations de chemin dans les fichiers de sauvegarde `ofcscan.ini` et `\private\ofcserver.ini`.

7. Avec les sauvegardes que vous avez créées, remplacez la base de données Worry-Free Business Security et les fichiers et dossiers adéquats sur l'ordinateur cible, dans le dossier `PCCSRV`.

8. Redémarrez le service principal de Trend Micro Security Server.

Désinstallation du serveur Security Server

La désinstallation du serveur Security Server désinstalle également le serveur de scan.

Worry-Free Business Security utilise un programme de désinstallation pour supprimer Trend Micro Security Server de votre ordinateur en toute sécurité. Supprimez l'agent de tous les clients avant de supprimer Security Server.

la désinstallation de Trend Micro Security Server ne désinstalle pas les agents. Les administrateurs doivent désinstaller ou déplacer tous les agents vers un autre serveur Security Server avant de désinstaller Trend Micro Security Server. Voir *Suppression d'agents à la page 3-39*.

Procédure

1. Sur l'ordinateur que vous avez utilisé pour installer le serveur, cliquez sur **Démarrer** > **Panneau de configuration** > **Ajout/Suppression de programmes**.
2. Cliquez sur **Trend Micro Security Server**, puis sur **Modifier/Supprimer**.

   Un écran de confirmation s'affiche.
3. Cliquez sur **Suivant**.

   Le programme de désinstallation principal du serveur vous invite à saisir le mot de passe de l'administrateur.
4. Saisissez le mot de passe de l'administrateur dans la zone de texte, puis cliquez sur **OK**.

   Le programme de désinstallation commence alors la suppression des fichiers du serveur. Un message de confirmation apparaît une fois que Security Server est correctement désinstallé.
5. Cliquez sur **OK** pour fermer le programme de désinstallation.

Chapitre 14

Utilisation des outils de gestion

Ce chapitre explique comment utiliser les outils et les modules complémentaires d'administration et clients.

Types d'outils

Worry-Free Business Security comprend un ensemble d'outils permettant d'accomplir facilement différentes tâches, parmi lesquelles la configuration du serveur et la gestion des clients.

Remarque

Il est impossible de lancer les outils administratifs et client de la console Web. La console Web permet de télécharger les modules d'extension.

Pour obtenir des instructions sur le fonctionnement de ces outils, consultez les sections correspondantes ci-dessous.

Ces outils sont classés en trois catégories :

- **Outils administrateurs**
  - **Configuration du script de connexion** (`SetupUsr.exe`) : Automatise l'installation de Security Agent. Voir *Installation avec l'outil Configuration du script de connexion à la page 3-12*.
  - **Vulnerability Scanner** (`TMVS.exe`) : Localise les ordinateurs non protégés sur le réseau. Voir *Installation avec Vulnerability Scanner à la page 3-21*.
  - **Agent Remote Manager** : Permet aux revendeurs de gérer Worry-Free Business Security via une console Web centralisée. Voir *Installation de Trend Micro Remote Manager Agent (utilisateurs de Customer Licensing Portal) à la page 14-4*.
  - **Trend Micro Disk Cleaner** : Supprime les fichiers de sauvegarde Worry-Free Business Security inutiles, les fichiers journaux et les fichiers de signatures inutilisés. Voir *Optimisation de l'espace disque à la page 14-15*.
  - **Outil de déplacement de la base de données Scan Server** : permet de déplacer la base de données Scan Server en toute sécurité vers un autre disque. Voir *Déplacement de la base de données Scan Server à la page 14-18*.

- **Outils clients**
  - **Client Packager** (`ClnPack.exe`) : Crée un fichier auto-extractible contenant Security Agent et ses composants. Voir *Installation avec Client Packager à la page 3-14*.
  - **Restaurer les virus et spywares encodés** (`VSEncode.exe`) : Ouvre des fichiers infectés chiffrés par Worry-Free Business Security. Voir *Restauration des fichiers chiffrés à la page 14-19*.
  - **Outil Client Mover** (`IpXfer.exe`) : Transfère les agents d'un serveur Security Server à un autre. Voir *Déplacement d'agents à la page 4-12*.
  - **Régénérer l'ID client Security Agent** (`WFBS_WIN_All_ReGenID.exe`) : Utilisez l'utilitaire ReGenID pour regénérer l'ID client Security Agent, selon que l'agent est un ordinateur cloné ou une machine virtuelle. Voir *Utilisation de l'outil ReGenID à la page 14-24*.
- **Modules d'extension** : permettent aux administrateurs de visualiser en direct les informations relatives à la sécurité et au système depuis les consoles des systèmes d'exploitation Windows pris en charge. Il s'agit des mêmes informations de haut niveau visibles depuis l'écran État actuel. Voir *Gestion des modules d'extension SBS et EBS à la page 14-24*.

Remarque

certains outils disponibles dans les versions précédentes de Worry-Free Business Security ne sont pas disponibles dans cette version. Si vous devez utiliser ces outils, contactez l'assistance technique de Trend Micro.

Agent Trend Micro Remote Manager

Trend Micro Remote Manager Agent permet aux revendeurs de gérer Worry-Free Business Security avec Trend Micro Remote Manager. Vous pouvez installer Remote Manager Agent sur le serveur Security Server à l'issue de l'installation de Security Server ou ultérieurement.

Configuration requise pour l'installation :

- Identificateur global unique (GUID) de Remote Manager Agent
- Une connexion Internet active
- 50 Mo d'espace disque disponible

Suivez les procédures dans l'un des éléments suivants :

- *Installation de Trend Micro Remote Manager Agent (utilisateurs de Customer Licensing Portal) à la page 14-4*
- *Installation de Trend Micro Remote Manager Agent (Utilisateurs de Licensing Management Platform) à la page 14-6*

Installation de Trend Micro Remote Manager Agent (utilisateurs de Customer Licensing Portal)

Procédure

1. Récupérez le GUID de Remote Manager Agent
   a. Sur la console Web Remote Manager, accédez à **Clients**.
   b. Dans la colonne **Société**, cliquez sur le client.
   c. Dans l'onglet **Produits**, sélectionnez le produit Worry-Free Business Security.
   d. Copiez le GUID.
2. Accédez à Security Server et naviguez vers le dossier d'installation suivant :`PCCSRV\Admin\Utility\RmAgent`, puis lancez l'application `TMRMAgentforWFBS.exe`.

   Par exemple :`C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   Remarque

   Ignorez cette étape si vous lancez l'installation depuis l'écran de configuration de Security Server.

3. Dans l'assistant d'installation de Trend Micro Remote Manager Agent, lisez le contrat de licence. Si vous acceptez ces termes, sélectionnez **J'accepte les conditions du contrat de licence**, puis cliquez sur **Suivant**.

4. Cliquez sur **Oui** pour confirmer que vous êtes un partenaire certifié.

5. Sélectionnez **Je possède déjà un compte Trend Micro Remote Manager et je souhaite installer l'agent**, puis cliquez sur **Suivant**.

6. Déterminez votre scénario.

SCÉNARIO	ÉTAPES
Nouveau client	a. Sélectionnez **Associer à un nouveau client**. b. Cliquez sur **Suivant**. Saisissez les informations clients. **Remarque** Si le client existe déjà sur la console TMRM et que vous utilisez l'option ci-dessus pour l'associer à un nouveau client, deux clients portant le même nom apparaîtront dans l'arborescence réseau de TMRM. Pour éviter cela, utilisez la méthode ci-dessous.
Client existant	a. Sélectionnez **Ce produit existe déjà dans Remote Manager**. **Remarque** WFBS doit avoir été ajouté au préalable sur la console TMRM. Reportez-vous à la documentation TMRM pour obtenir des instructions. b. Saisissez le GUID.

7. Cliquez sur **Suivant**.

8. Sélectionnez **Région** et **Protocole**, puis saisissez les informations de proxy, le cas échéant.

9. Cliquez sur **Suivant**.

   L'écran Emplacement de l'installation apparaît.

10. Pour utiliser l'emplacement par défaut, cliquez sur **Suivant**.

11. Cliquez sur **Terminer**.

    Si l'installation a réussi et que les paramètres sont corrects, Remote Manager Agent doit être enregistré automatiquement sur le serveur Trend Micro Remote Manager. Remote Manager Agent doit afficher l'état En ligne sur la console Web Remote Manager.

Installation de Trend Micro Remote Manager Agent (Utilisateurs de Licensing Management Platform)

Procédure

1. Récupérez le code d'activation de votre logiciel Worry-Free Business Security.
   a. Sur la console Web Remote Manager, accédez à **Clients**.
   b. Dans la colonne **Société**, cliquez sur le client.
   c. Dans l'onglet **Produits**, sélectionnez le produit Worry-Free Business Security.
   d. Copiez le code d'activation.
2. Mettez à jour les informations sur la licence Worry-Free Business Security.
   a. Sur la console Web Worry-Free Business Security, accédez à **Administration** > **Licence du produit**.
   b. Sous **Informations sur la licence**, cliquez sur **Entrer un nouveau code**.
   c. Dans le champ **Nouveau code d'activation**, collez le code d'activation.
   d. Cliquez sur **Activer**.
   e. Cliquez sur **Actualiser les informations sur la licence**.

3. Accédez à Security Server et naviguez vers le dossier d'installation suivant :`PCCSRV\Admin\Utility\RmAgent`, puis lancez l'application `TMRMAgentforWFBS.exe`.

   Par exemple :`C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   Remarque

   Ignorez cette étape si vous lancez l'installation depuis l'écran de configuration de Security Server.

4. Sélectionnez **Je possède déjà un compte Trend Micro Remote Manager et je souhaite installer l'agent**, puis cliquez sur **Suivant**.

5. Sélectionnez **Associer à la licence Licensing Management Platform existante** et cliquez sur **Suivant**.

6. Spécifiez les informations de compte Remote Manager et cliquez sur **Suivant**.

7. Si nécessaire, spécifiez les informations de serveur proxy et cliquez sur **Suivant**.

8. Si nécessaire, spécifiez le dossier d'installation et cliquez sur **Suivant**.

9. Cliquez sur **Terminer**.

   Si l'installation a réussi et que les paramètres sont corrects, Remote Manager Agent doit être enregistré automatiquement sur le serveur Trend Micro Remote Manager. Remote Manager Agent doit afficher l'état En ligne sur la console Web Remote Manager.

Gestion des agents à partir du serveur géré

Cette section contient des informations sur la gestion des agents à partir du serveur géré.

Messages d'état de l'agent

Sur le serveur géré, l'agent affiche l'une des icônes de barre d'état système suivantes :

TABLEAU 14-1. Icônes de la barre d'état système

ICÔNE	DESCRIPTION
	Une icône verte indique que l'agent est connecté au serveur de communication de Remote Manager. L'agent fonctionne normalement.
	Une icône rouge indique que l'agent n'est pas connecté au serveur de communication de Remote Manager ou que la version de l'agent ne correspond pas à celle du serveur et doit être mise à jour.
	Une icône avec une flèche rouge indique que l'agent s'est déconnecté de Remote Manager.
	Une icône avec un « X » rouge signifie que l'agent a été désactivé.

Modification du GUID de l'agent sur le serveur géré

Si vous avez entré un identificateur global unique (GUID) incorrect pendant l'installation de Remote Manager Agent, supprimez l'agent et réinstallez-le en utilisant le GUID correct. S'il vous est impossible de suivre cette procédure, vous pouvez effectuer les opérations suivantes :

Procédure

1. Accédez à `C:\Program Files\Trend Micro\TMRMAgentForWFBS`.
2. Ouvrez le fichier `AgentSysConfig.xml` à l'aide d'un éditeur de texte.
3. Recherchez le GUID entre les paramètres `<AgentGUID>` et `</AgentGUID>`.
4. Modifiez le GUID et enregistrez le fichier.
5. Dans le même dossier, ouvrez le fichier `csmSysConfig.xml` à l'aide d'un éditeur de texte.

6. Recherchez le GUID entre les paramètres `<ProductGUID>` et `</ProductGUID>`.
7. Modifiez le GUID et enregistrez le fichier.
8. Cliquez avec le bouton droit sur l'icône Remote Manager Agent dans la barre des tâches, puis cliquez sur **Redémarrer le service**.

Utilisation de l'outil de configuration de l'agent

L'outil de configuration de l'agent permet d'effectuer des modifications sur les paramètres de configuration de Remote Manager Agent.

Accédez à **Démarrer** > **Programmes** > **Agent Trend Micro Remote Manager** > **Outil de configuration de l'agent** ou cliquez avec le bouton droit de la souris dans la barre d'état, puis cliquez sur **Configurer**.

Pour plus d'informations, voir *Configuration de l'agent à la page 14-9*.

Configuration de l'agent

Menu de configuration de l'agent

Pour configurer l'agent, cliquez avec le bouton droit sur l'icône de barre d'état pour ouvrir le menu suivant :

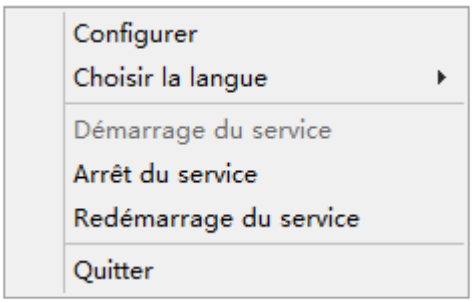


FIGURE 14-1. Menu contextuel de l'outil de configuration de l'agent

Les éléments suivants apparaissent :

- **Configurer** : ouvre l'écran de configuration de l'agent.
- **Choisir la langue** : outre les autres langues possibles, l'anglais est toujours disponible.
- **Service** : démarrer, arrêter, redémarrer.
- **Quitter** : si vous quittez l'outil, cela n'arrête pas le service Remote Manager. Il ferme uniquement l'outil de configuration et supprime l'icône de la barre des tâches. L'outil peut être redémarré à tout moment.

Boîte de dialogue principale de l'outil de configuration

Cliquez avec le bouton droit de la souris sur l'icône de la barre d'état, puis cliquez sur **Configurer** dans le menu de configuration de l'agent pour ouvrir l'onglet **Général** de l'outil de configuration de l'agent.

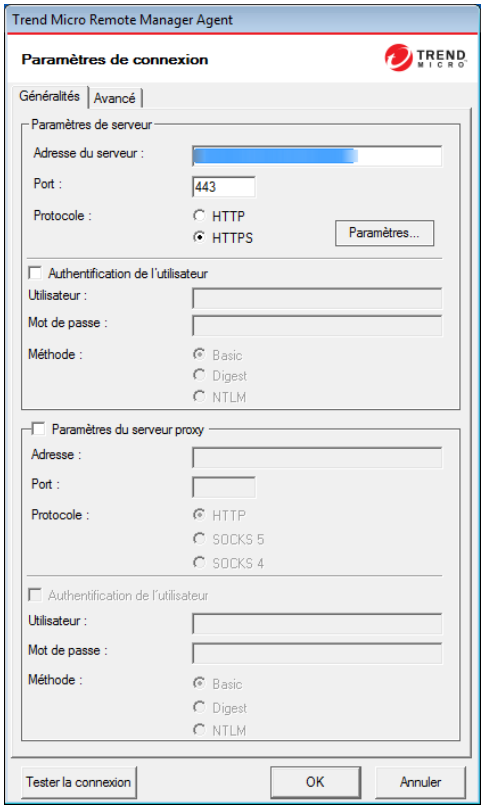


FIGURE 14-2. Onglet Général de l'outil de configuration de l'agent

Les sections suivantes de l'écran de configuration de l'agent sont les seules sections actuellement pertinentes de cet outil.

- **Paramètres de serveur** : Configurez la communication du serveur en définissant les éléments suivants :

- **Adresse du serveur** : nom de domaine complet (FQDN) du serveur de communication de Remote Manager. Le nom de domaine complet varie dans chaque région. Contactez votre service d'assistance technique si vous avez besoin de modifier les informations de l'adresse du serveur.
- **Port** : port utilisé par le serveur Remote Manager pour communiquer avec l'agent. Il doit s'agir du port 80 pour HTTP et du port 443 pour HTTPS.
- **Protocole** : protocole utilisé pour la communication entre le serveur et l'agent.

Important

Trend Micro ne recommande pas de modifier les informations concernant l'**adresse du serveur** ou le **port**, sauf si votre service d'assistance vous demande de le faire.

- **Paramètres du serveur proxy** : activez cette zone en cochant la case **Paramètres du serveur proxy** si le réseau de l'utilisateur nécessite un proxy pour communiquer avec le serveur Remote Manager.
  - **Adresse** : adresse IP du serveur proxy
  - **Port** : port ou serveur proxy
  - **Protocole**
- **Bouton Tester la connexion** : le bouton **Tester la connexion** est utilisé pour tester la communication entre l'agent et le serveur Remote Manager. Utilisez cette fonction pour tester le bon fonctionnement de la connexion de base au serveur de communication. Si le test échoue (une boîte de dialogue contextuelle s'affiche si l'outil ne parvient pas à se connecter au serveur), cela signifie qu'il existe peut-être un problème de base tel que l'adresse du serveur de communication et son port ou l'adresse du serveur proxy et son port.

Sauvegarde et restauration des paramètres de l'agent

Si vous devez désinstaller puis réinstaller l'agent à l'aide du même GUID en l'espace de trois jours, conservez les paramètres de l'agent pour éviter tout chevauchement de données. Pour cela, sauvegardez les fichiers de configuration manuellement, puis restaurez-les après la réinstallation de l'agent.

Sauvegarde des paramètres

Procédure

1. Sur le serveur géré, cliquez avec le bouton droit sur l'icône de la barre d'état système de l'agent, puis cliquez sur **Arrêt du service** pour arrêter le service d'agent.
2. Copiez tous les fichiers `.xml`, `.dat` et `.ini` du dossier d'installation : `C:\Program Files\Trend Micro\TMRMAgentForWFBS` ou `C:\Program Files (x86)\Trend Micro\TMRMAgentForWFBS`.
   - Fichiers `.xml`
     - `csmSysConfig.xml`
     - `csmLocalConfig.xml`
     - `csmLogDef.xml`
     - `AgentWorkConfig.xml`
     - `AgentSysConfig.xml`
     - `AgentStatus.xml`
     - `AgentLocalConfig.xml`
   - Fichiers `.dat`
     - `MSA.dat`
     - `logBuf.dat`

- `group.dat`
- `CSA.dat`
- `CriticalVA.dat`

- Fichiers `.ini`
  - `csmStatusData.ini`

3. Copiez tous les fichiers du dossier `\Cache`.
4. Redémarrez le service d'agent.

Restauration des paramètres

Procédure

1. Supprimez l'agent localement.

   Remarque

   Lorsque vous supprimez l'agent localement, celui-ci annule son enregistrement de Remote Manager, ce qui supprime automatiquement toutes les données associées à l'agent. Pour éviter que l'agent ne se désenregistre, modifiez la valeur Adresse du serveur sur l'interface de l'agent avant de le supprimer.

2. Réinstallez l'agent. Veillez à utiliser le même GUID, que vous retrouverez dans `agentSysConfig.xml`.
3. Sur le serveur géré, cliquez avec le bouton droit sur l'icône de la barre d'état système de l'agent, puis cliquez sur **Arrêt du service** pour arrêter le service d'agent.
4. Remplacez les fichiers de configuration par ceux sauvegardés.

5. Cliquez avec le bouton droit sur l'icône de la barre d'état système de l'agent et cliquez sur **Démarrage du service** pour redémarrer le service d'agent.

Optimisation de l'espace disque

Libérez de l'espace disque sur Security Server et sur les clients en exécutant le nettoyeur de disque.

Exécution du nettoyeur de disque sur Security Server

Avant de commencer

Pour économiser l'espace disque, l'outil Nettoyeur de disque (`TMDiskCleaner.exe`) identifie et supprime les fichiers de sauvegarde, les fichiers journaux et les fichiers de signatures inutilisés dans les répertoires suivants :

- `{Security Agent}\AU_Data\AU_Temp\*`
- `{Security Agent}\Reserve`
- `{Security Server}\PCCSRV\TEMP\* (sauf fichiers masqués)`
- `{Security Server}\PCCSRV\Web\Service\AU_Data\AU_Temp\*`
- `{Security Server}\PCCSRV\wss\*.log`
- `{Security Server}\PCCSRV\wss\AU_Data\AU_Temp\*`
- `{Security Server}\PCCSRV\Backup\*`
- `{Security Server}\PCCSRV\Virus\* (supprime les fichiers mis en quarantaine antérieurs à deux semaines, sauf le fichier NOTVIRUS)`
- `{Security Server}\PCCSRV\ssaptpn.xxx (conserve le dernier fichier de signatures uniquement)`

- `{Security Server}\PCCSRV\lpt$vpn.xxx (conserve les trois derniers fichiers de signatures uniquement)`
- `{Security Server}\PCCSRV\icrc$oth.xxx (conserve les trois derniers fichiers de signatures uniquement)`
- `{Security Server}\DBBackup\* (conserve les deux derniers sous-dossiers uniquement)`
- `{Messaging Security Agent}\AU_Data\AU_Temp\*`
- `{Messaging Security Agent}\Debug\*`
- `{Messaging Security Agent}\engine\vsapi\latest\pattern\*`

Procédure

1. Sur Security Server, accédez au répertoire suivant :

   `{Dossier d'installation du serveur}\PCCSRV\Admin\Utility\`

2. Cliquez deux fois sur **TMDiskCleaner.exe**.

   L'outil Nettoyeur de disque de Trend Micro Worry-Free Business Security s'affiche.

   Remarque

   Impossible de restaurer les fichiers.

3. Cliquez sur **Supprimer les fichiers** pour rechercher et supprimer les fichiers de sauvegarde, les fichiers journaux et les fichiers de signatures inutilisés.

Exécution du nettoyeur de disque sur Security Server à l'aide de l'interface de ligne de commande

Procédure

1. Sur le serveur Security Server, ouvrez une fenêtre d'invite de commande.
2. À l'invite de commande, exécutez la commande suivante :

   ```
   TMDiskCleaner.exe [/hide] [/log] [/allowundo]
   ```

   - `/hide` : exécute l'outil en tant que processus d'arrière-plan.
   - `/log` : enregistre un journal de l'opération dans le fichier DiskClean.log qui réside dans le dossier actuel.

     Remarque

     `/log` n'est disponible que lorsque le paramètre `/hide` est utilisé.

   - `/allowundo` : déplace les fichiers vers la Corbeille et ne les supprime pas définitivement.
3. Pour exécuter fréquemment l'outil Nettoyeur de disque, configurez une nouvelle tâche au moyen du programme Tâches planifiées de Windows. Pour obtenir des informations complémentaires, consultez la documentation Windows.

Optimisation de l'espace disque sur les clients

Procédure

- Sur les postes de travail/serveurs sur lesquels des agents Security Agent sont installés :
  - Nettoyez les fichiers mis en quarantaine.
  - Nettoyez les fichiers journaux.

- Exécutez l'utilitaire de nettoyage de disque de Windows.

- Sur les serveurs Microsoft Exchange sur lesquels des agents Messaging Security Agent sont installés :
  - Nettoyez les fichiers mis en quarantaine.
  - Nettoyez les fichiers journaux.
  - Exécutez l'utilitaire de nettoyage de disque de Windows.
  - Nettoyez les journaux d'archive.
  - Nettoyez les fichiers de sauvegarde.
  - Vérifiez la taille des journaux de base de données ou de transactions Microsoft Exchange.

Déplacement de la base de données Scan Server

Si le disque sur lequel Scan Server est installé ne dispose pas de suffisamment d'espace, utilisez l'outil de déplacement de la base de données Scan Server pour la déplacer en toute sécurité vers un autre disque.

Vérifiez que l'ordinateur Security Server comporte plusieurs disques et que le nouveau disque dispose d'au moins 3 Go d'espace disque disponible. Les lecteurs mappés ne sont pas acceptés. Ne déplacez pas la base de données manuellement ou n'utilisez pas d'autres outils.

Procédure

1. Sur l'ordinateur Security Server, accédez à : `<dossier d'installation du serveur Security Server>\PCCSRV\Admin\Utility`.
2. Lancez `ScanServerDBMover.exe`.
3. Cliquez sur **Modifier**.
4. Cliquez sur **Parcourir** et accédez au répertoire cible sur l'autre disque.

5. Cliquez sur **OK**, puis sur **Terminer** une fois la base de données déplacée.

Restauration des fichiers chiffrés

Pour empêcher l'ouverture d'un fichier infecté, Worry-Free Business Security chiffre ce fichier dans les cas suivants :

- Avant de placer un fichier en quarantaine
- Lors de la sauvegarde d'un fichier avant de le nettoyer

Worry-Free Business Security fournit un outil qui déchiffre puis restaure le fichier si vous devez absolument extraire les informations qu'il contient. Worry-Free Business Security peut déchiffrer et restaurer les fichiers suivants :

TABLEAU 14-2. Fichiers que Worry-Free Business Security peut décoder et restaurer

FICHIER	DESCRIPTION
Fichiers placés en quarantaine sur le client	Ces fichiers se trouvent dans les répertoires suivants : • `<dossier d'installation de Security Agent>\SUSPECT\Backup` ou `<dossier d'installation de Security Agent>\quarantine`, en fonction de celui qui est disponible. • `<Dossier d'installation de Messaging Security Agent>\storage\quarantine` Ces fichiers sont également téléchargés dans le répertoire de quarantaine désigné, généralement situé sur le serveur Security Server.
Fichiers placés en quarantaine dans le répertoire de quarantaine désigné	Par défaut, ce répertoire est situé sur l'ordinateur Security Server (`<dossier d'installation de Security Server>\PCCSRV\Virus`). Pour changer de répertoire, accédez à **Administration** > **Paramètres généraux** > **Onglet Système** et allez dans la section Maintenance de la mise en quarantaine.

Fichier	Description
Fichiers chiffrés sauvegardés	Il s'agit de la sauvegarde des fichiers infectés que les agents ont réussi à nettoyer. Ces fichiers se trouvent dans les dossiers suivants : • `<dossier d'installation de Security Agent>\Backup`. • `<dossier d'installation de Messaging Security Agent>\storage\backup` Pour restaurer ces fichiers, les utilisateurs doivent les déplacer dans le dossier de quarantaine du client.

AVERTISSEMENT!

Lorsque vous restaurez un fichier infecté, le virus/programme malveillant qu'il contient peut se propager à d'autres fichiers ou clients. Avant de restaurer le fichier, isolez le client infecté et déplacez les fichiers importants de ce client vers un emplacement de sauvegarde.

Décryptage et restauration des fichiers sur Security Agent

Procédure

1. Ouvrez une invite de commande et accédez au `<Dossier d'installation de Security Agent>`.
2. Exécutez `VSEncode.exe` en saisissant :

   ```
   VSEncode.exe /u
   ```

   Ce paramètre ouvre un écran contenant la liste des fichiers qui se trouvent sous `<Dossier d'installation de Security Agent>\SUSPECT\Backup`.

   Les administrateurs peuvent restorer les fichiers classés comme spywares/graywares sous l'onglet Spyware/grayware. L'écran affiche la liste des fichiers qui se trouvent sous : `<Dossier d'installation de Security Agent>\BackupAS`.

3. Sélectionnez un fichier à restaurer et cliquez sur **Restaurer**.

   Remarque

   L'outil ne peut restaurer qu'un seul fichier à la fois.

4. Dans l'écran qui s'affiche, indiquez le dossier dans lequel vous voulez restaurer le fichier.

5. Cliquez sur **OK**.

   Remarque

   Il se peut que l'agent scanne de nouveau le fichier et le considère comme infecté dès sa restauration. Pour éviter qu'il ne soit scanné, ajoutez-le à la liste d'exclusion de scan.

   Voir *Cibles de scan et actions des agents Security Agent à la page 7-10*.

   Le fichier est restauré dans le dossier spécifié.

6. Cliquez sur **Fermer**.

Décryptage et restauration des fichiers sur Security Server, un répertoire de quarantaine personnalisé ou Messaging Security Agent

Procédure

1. Si le fichier se trouve sur l'ordinateur Security Server, ouvrez une invite de commande et accédez à `<Dossier d'installation du serveur>\PCCSRV\Admin\Utility\VSEncrypt`.

   Si le fichier se trouve sur le client Messaging Security Agent ou dans un répertoire de quarantaine personnalisé, accédez à `<Dossier d'installation du serveur\PCCSRV>\Admin\Utility` et copiez le dossier `VSEncrypt` sur le client ou le répertoire de quarantaine personnalisé.

2. Créez un fichier texte, puis saisissez le chemin d'accès complet aux fichiers que vous souhaitez chiffrer ou déchiffrer.

   À titre d'exemple, vous pouvez saisir le chemin d'accès `C:\Mes documents\Reports, \*.* dans le fichier texte pour restaurer tous les fichiers contenus dans C:\Mes documents \Reports`.

   Les fichiers placés en quarantaine sur l'ordinateur du serveur Security Server se trouvent sous `<Dossier d'installation du serveur> \PCCSRV\Virus`.

3. Enregistrez le fichier texte avec une extension `INI` ou `TXT`. Par exemple, enregistrez-le sous `ForEncryption.ini` sur le lecteur `C:`.

4. Ouvrez une fenêtre d'invite et naviguez vers le répertoire dans lequel se trouve le dossier `VSEncrypt`.

5. Exécutez `VSEncode.exe` en saisissant :

   ```
   VSEncode.exe /d /i <emplacement du fichier INI ou TXT>
   ```

   Description :

   `<emplacement du fichier INI ou TXT>` est le chemin du fichier `INI` ou `TXT` que vous avez créé (par exemple, `C:\ForEncryption.ini`).

6. Utilisez les autres paramètres pour lancer diverses commandes.

TABLEAU 14-3. Paramètres de restauration

PARAMÈTRE	DESCRIPTION
Aucun (aucun paramètre)	Chiffrer les fichiers
`/d`	Décoder les fichiers
`/debug`	Créez un journal de débogage et enregistrez-le sur l'ordinateur. Sur le client, le journal de débogage `VSEncrypt.log` est créé dans le `<Dossier d'installation de l'agent>`.
`/o`	Remplacer un fichier encodé ou décodé s'il existe déjà

Paramètre	Description
`/f <nom de fichier>`	chiffre ou déchiffre un seul fichier.
`/nr`	Ne pas restaurer le nom de fichier original
`/v`	Afficher des informations concernant l'outil
`/u`	Lancer l'interface utilisateur de l'outil
`/r <Dossier de destination>`	Dossier dans lequel un fichier sera restauré
`/s <Nom de fichier d'origine>`	Nom du fichier chiffré original

Par exemple, saisissez la commande `VSEncode [/d] [/debug]` pour déchiffrer les fichiers du dossier `Suspect` et créer un journal de débogage. Lorsque vous décodez ou encodez un fichier, Worry-Free Business Security crée le fichier décodé ou encodé dans le même dossier que le fichier source. Avant de déchiffrer ou de chiffrer un fichier, assurez-vous qu'il n'est pas verrouillé.

Restauration des messages électroniques TNEF

Le format TNEF (Transport Neutral Encapsulation Format) est un format d'encapsulation des messages utilisé par Microsoft Exchange/Outlook. Généralement, ce format est empaqueté en tant que pièce jointe de message électronique nommée `Winmail.dat` et Outlook Express masque cette pièce jointe automatiquement.

Pour plus d'informations, voir https://support.microsoft.com/en-us/help/290809/.

Si l'agent Messaging Security Agent archive ce type d'email et si l'extension du fichier est remplacée par l'extension .EML, Outlook Express n'affichera que le corps du message électronique.

Utilisation de l'outil ReGenID

Chaque agent Security Agent requiert un identificateur global unique (GUID) permettant au serveur Security Server d'identifier les clients individuellement. Les identificateurs GUID en double se retrouvent généralement sur des clients clonés ou des machines virtuelles.

Si deux agents ou plus sont associés au même identificateur GUID, exécutez l'outil ReGenID pour générer un identificateur GUID unique pour chaque client.

Procédure

1. Sur Security Server, accédez au répertoire suivant :`<dossier d'installation du serveur>\PCCSRV\Admin\Utility`.
2. Copiez le fichier `WFBS_WIN_All_ReGenID.exe` dans un dossier temporaire sur le client où l'agent Security Agent est installé.

   Exemple :`C:\temp`
3. Double-cliquez sur `WFBS_WIN_All_ReGenID.exe` et suivez les instructions à l'écran.

   L'outil arrête l'agent Security Agent et supprime l'identificateur GUID du client.
4. Redémarrez l'agent Security Agent.

   L'agent Security Agent génère un nouvel identificateur GUID pour le client.

Gestion des modules d'extension SBS et EBS

Worry-Free Business Security propose des modules d'extension qui permettent aux administrateurs de visualiser en direct les informations relatives à la sécurité et à l'état de l'agent depuis les consoles des systèmes d'exploitation Windows suivants :

- Windows Small Business Server (SBS) 2008
- Windows Essential Business (EBS) Server 2008
- Windows SBS 2011 Standard/Essentials
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

Installation manuelle des modules d'extension SBS et EBS

Le module d'extension SBS ou EBS s'installe automatiquement lorsque vous installez le serveur Security Server sur un endpoint exécutant les systèmes d'exploitation pris en charge. Pour utiliser le module d'extension sur un autre endpoint exécutant ces systèmes d'exploitation, vous devez l'installer manuellement.

Procédure

1. Connectez-vous à la console Web du serveur Security Server.
2. Accédez à **Administration** > **Outils de gestion**.
3. Cliquez sur **Modules d'extension**.
4. Cliquez sur le lien **Télécharger** correspondant pour obtenir le programme d'installation.
5. Copiez et lancez le programme d'installation sur l'endpoint cible.

Utilisation des modules d'extension SBS ou EBS

Procédure

1. Ouvrez la console SBS ou EBS.

2. Sous l'onglet **Sécurité**, cliquez sur **Trend Micro Worry-Free Business Security** pour visualiser les informations relatives à l'état.

Annexe A

Icône de Security Agent

Cette annexe explique les différentes icônes de Security Agent qui s'affichent sur les clients.

Vérification de l'état de Security Agent

L'image suivante montre la console Security Agent avec tous les éléments à jour et opérationnels :

Le tableau suivant répertorie les icônes et leur signification dans l'interface utilisateur principale de la console Security Agent :

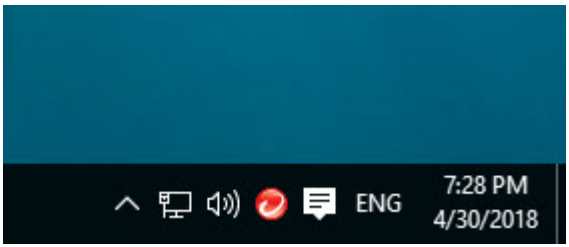
TABLEAU A-1. Icônes de l'interface utilisateur principale de Security Agent

ICÔNE	ÉTAT	EXPLICATION ET ACTION
	Protection activée : Vous êtes protégé et votre logiciel est à jour	Le logiciel est à jour et s'exécute correctement. Aucune action n'est requise.
	Redémarrer l'ordinateur : Redémarrez l'ordinateur pour terminer la correction des menaces de sécurité	Security Agent a détecté des menaces qu'il ne peut pas corriger immédiatement. Redémarrez l'ordinateur pour terminer la correction de ces menaces.
	La protection présente un risque : Contactez votre administrateur	Le scan en temps réel est désactivé ou votre protection présente un risque pour une autre raison. Activez le scan en temps réel et, si cela ne résout pas le problème, contactez l'assistance.
	Mettre à jour : vous n'avez pas reçu de mise à jour depuis (nombre) jours	Le fichier de signatures de virus date de plus de trois jours. Mettez à jour Security Agent immédiatement.

Icône	État	Explication et action
	Smart Scan indisponible : Vérifiez votre connexion Internet	Security Agent n'a pas eu accès au serveur de scan depuis plus de 15 minutes. Vérifiez que vous êtes connecté à votre réseau afin de lancer un scan avec les derniers fichiers de signatures.
	Redémarrer l'ordinateur : Redémarrez votre ordinateur pour terminer la mise à jour	Redémarrez votre ordinateur pour terminer la mise à jour.
	Mise à jour du programme : Votre logiciel de sécurité est en train de se mettre à jour	Une mise à jour est en cours. Ne vous déconnectez pas du réseau tant qu'elle n'est pas terminée.

Icônes de Security Agent dans la barre des tâches Windows

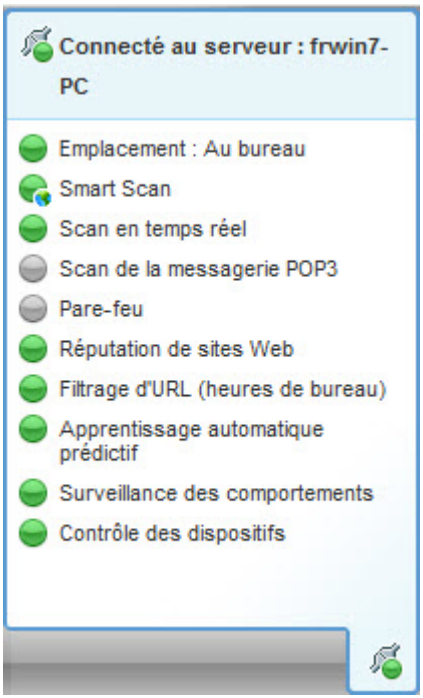
Les icônes de Security Agent suivantes s'affichent dans la barre des tâches Windows :



Icône	Signification
	État normal
	(Animé) Un scan manuel ou programmé est en cours. Security Agent utilise Scan traditionnel ou Smart Scan.
	Security Agent effectue une mise à jour.
	Une action est nécessaire : • Scan en temps réel désactivé • Un redémarrage est nécessaire pour supprimer complètement le programme malveillant. • Un redémarrage est nécessaire en raison de la mise à jour d'un moteur. • Un redémarrage est nécessaire pour restaurer les fichiers chiffrés par le logiciel de rançon. • Une mise à jour est nécessaire.  **Remarque** Ouvrez la console principale de Security Agent pour voir quelle action est requise.

Accès au survol de la console

Le survol de la console Security Agent s'ouvre lorsque vous placez le pointeur de la souris sur la petite icône située dans la partie inférieure droite de la console Security Agent.



Le tableau suivant répertorie les icônes de survol de la console et leur signification :

TABLEAU A-2. Icônes de survol de la console

FONCTION	ICÔNE	SIGNIFICATION
Connexion		Connecté à Security Server
		Non connecté à Security Server, mais le scan en temps réel est toujours en cours d'exécution. Le fichier de signatures n'est peut-être pas à jour. Faites un clic droit sur l'icône de l'agent dans la barre des tâches Windows, puis cliquez sur **Mettre à jour**.

Fonction	Icône	Signification
Emplacement		Au bureau (réseau interne)
		Hors du bureau (réseau externe)
Scan en temps réel		Activé
		Désactivé
Scan de la messagerie POP3		Activé
		Désactivé
Smart Scan		Connecté à Trend Micro Smart Protection Network
		Impossible de se connecter à Smart Protection Network ; la protection est réduite car les Agents Security Agent ne parviennent pas à envoyer de requêtes de scan. **Remarque** Vérifiez que le service Smart Scan TMiCRCScanService est en cours d'exécution et que les Agents Security Agent sont connectés à Security Server.
		Smart Scan est désactivé. Utilisation du scan traditionnel

Fonction	Icône	Signification
• Pare-feu • Réputation de sites Web • Filtrage d'URL • Surveillance des comportements • Contrôle des dispositifs • Apprentissage automatique prédictif		Activé
		Désactivé

Annexe B

Prise en charge d'IPv6 dans Worry-Free Business Security

Cette annexe doit être lue par les utilisateurs qui prévoient de déployer Worry-Free Business Security dans un environnement prenant en charge l'adressage IPv6. Cette annexe contient des informations sur le degré de prise en charge d'IPv6 dans Worry-Free Business Security.

Trend Micro suppose que le lecteur est familiarisé avec les concepts d'IPv6 et les tâches qu'implique la configuration d'un réseau prenant en charge l'adressage IPv6.

Prise en charge d'IPv6 pour Worry-Free Business Security et Agents Security Agent

La prise en charge d'IPv6 pour Worry-Free Business Security a commencé avec la version 8.0. Les versions antérieures de Worry-Free Business Security ne prennent pas en charge l'adressage IPv6. La prise en charge d'IPv6 est automatiquement activée après l'installation ou la mise à niveau du serveur Security Server, des agents Security Agent et Messaging Security Agent répondant aux conditions requises pour la prise en charge d'IPv6.

Conditions requises pour la prise en charge d'IPv6 sur Security Server

Les conditions requises pour la prise en charge d'IPv6 dans le serveur Security Server sont les suivantes :

- Si le serveur peut gérer les agents IPv4 et IPv6, il doit contenir les adresses IPv4 et IPv6 et doit être identifié par son nom d'hôte. Si un serveur est identifié par son adresse IPv4, les agents IPv6 purs ne peuvent pas s'y connecter. La même erreur se produit si les clients utilisant exclusivement IPv4 se connectent à un serveur identifié par ses adresses IPv6.
- Si le serveur ne gère que des agents IPv6, la configuration minimale requise est une adresse IPv6. Le serveur peut être identifié par son nom d'hôte ou son adresse IPv6. Lorsque le serveur est identifié par son nom d'hôte, il est préférable d'utiliser le nom de domaine complet (FQDN). En effet, dans un environnement exclusivement IPv6, un serveur WINS ne peut pas convertir un nom d'hôte en une adresse IPv6 correspondante.
- Vérifiez que l'adresse IPv6 ou IPv4 de l'ordinateur hôte peut être récupérée en utilisant, par exemple, la commande « `ping` » ou « `nslookup` ».
- Si vous installez le serveur Security Server sur un ordinateur IPv6 pur, installez un serveur proxy à double pile qui peut convertir les adresses IPv4 et IPv6 (par exemple, DeleGate). Positionnez le serveur proxy entre

le serveur Security Server et Internet pour permettre au serveur de se connecter aux services hébergés de Trend Micro, tels que le serveur ActiveUpdate, le site Web d'enregistrement en ligne et Smart Protection Network.

Configuration requise pour Messaging Security Agent

Messaging Security Agent (Advanced uniquement) doit être installé sur un serveur Microsoft Exchange à double pile ou IPv6 pur.

Il est préférable qu'un agent Messaging Security Agent possède à la fois des adresses IPv4 et IPv6, car certaines entités auxquelles il se connecte ne prennent en charge que l'adressage IPv4.

Limitations des serveurs IPv6 purs

Le tableau suivant répertorie les restrictions pour un serveur Security Server possédant uniquement des adresses IPv6.

TABLEAU B-1. Limitations des serveurs IPv6 purs

PHASE	RESTRICTION
Gestion des agents	Un serveur IPv6 ne peut : • Déployer des agents sur des clients IPv4 purs • Gérer des agents IPv4 purs
Mises à jour et gestion centralisée	Un serveur IPv6 pur ne peut effectuer de mises à jour à partir de sources de mise à jour IPv4 pures, telles que : • Serveur ActiveUpdate de Trend Micro • Toute source de mise à jour personnalisée IPv4 pure
Enregistrement, activation et renouvellement du produit	Un serveur IPv6 pur ne peut se connecter au serveur d'enregistrement en ligne de Trend Micro pour enregistrer le produit, obtenir la licence et activer/renouveler la licence.
Connexion Proxy	Un serveur IPv6 pur ne peut se connecter via un serveur proxy IPv4 pur.

Phase	Restriction
Solutions de plug-in	Un serveur IPv6 pur possède Plug-in Manager mais ne peut déployer aucune des solutions de plug-in pour : • les agents IPv4 purs ou les hôtes IPv4 purs (du fait de l'absence de connexion directe) ; • les agents IPv6 purs ou les hôtes IPv6 purs, car aucune des solutions de plug-in ne prend en charge IPv6.

La plupart de ces restrictions peuvent être surmontées en configurant un serveur proxy à double pile pouvant convertir les adresses IPv4 et IPv6 (tel que DeleGate). Positionnez le serveur proxy entre le serveur Security Server et les entités auxquelles il se connecte ou les entités qu'il dessert.

Limitations des Security Agent IPv6 purs

Le tableau suivant répertorie les restrictions pour un Security Agent possédant uniquement des adresses IPv6.

Tableau B-2. Limitations des Security Agent IPv6 purs

Phase	Restriction
Security Server parent	Les agents IPv6 purs ne peuvent être gérés par un serveur Security Server IPv4 pur.
Mises à jour	Un Security Agent IPv6 pur ne peut effectuer de mises à jour à partir de sources de mise à jour IPv4 pures, telles que : • Serveur ActiveUpdate de Trend Micro • Serveur Security Server IPv4 pur • un agent de mise à jour IPv4 pur • Toute source de mise à jour personnalisée IPv4 pure
Requêtes de scan et Smart Feedback	Un agent Security Agent IPv6 pur ne peut pas envoyer de requêtes à Trend Micro Smart Protection Network ni utiliser Smart Feedback.

Phase	Restriction
Solutions de plug-in	Les agents IPv6 purs ne peuvent installer de solutions de plug-in, car aucune des solutions de plug-in ne prend en charge IPv6.
Connexion Proxy	Un Security Agent IPv6 pur ne peut se connecter via un serveur proxy IPv4 pur.

La plupart de ces restrictions peuvent être surmontées en configurant un serveur proxy à double pile pouvant convertir les adresses IPv4 et IPv6 (tel que DeleGate). Placez le serveur proxy entre les Agents Security Agent et les entités auxquelles ils se connectent.

Configuration des adresses IPv6

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

- Worry-Free Business Security prend en charge les présentations d'adresses IPv6 standard.

  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`

- Worry-Free Business Security prend également en charge les adresses IPv6 avec un lien local, telles que :

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

AVERTISSEMENT!

Faites attention lors de la spécification d'une adresse IPv6 avec un lien local car, même si Worry-Free Business Security accepte cette adresse, il se peut qu'il ne fonctionne pas comme attendu dans certaines circonstances. Par exemple, les Agents Security Agent ne peuvent pas effectuer de mise à jour à partir d'une source de mise à jour si celle-ci se trouve sur un segment différent du réseau et est identifiée par son adresse IPv6 avec lien local.

- Lorsque l'adresse IPv6 fait partie d'une URL, placez-la entre crochets ([]).
- Pour les plages d'adresses IPv6, un préfixe et une longueur de préfixe sont généralement requis. Pour les configurations qui requièrent que le serveur interroge des adresses IP, des restrictions de longueur de préfixe s'appliquent afin d'empêcher tout problème de performance lorsque le serveur interroge un grand nombre d'adresses IP. Par exemple, pour la fonction de gestion des serveurs externes, la longueur du préfixe doit être comprise entre 112 (65,536 adresses IP) et 128 (2 adresses IP).
- Certains paramètres impliquant des adresses IPv6 ou des plages d'adresses IPv6 seront déployés vers les Agents Security Agent, mais les Agents Security Agent les ignoreront. Par exemple, si vous avez configuré la liste des sources Smart Protection et inclus un serveur Smart Protection Server identifié par son adresse IPv6, des Agents Security Agent avec une adresse IPv4 pure vont ignorer le serveur et se connecter à d'autres sources Smart Protection.

Écrans affichant les adresses IP

Cette rubrique dresse la liste des endroits de la console Web où sont affichées les adresses IP.

- Arborescence des groupes de sécurité

  Chaque fois que l'arborescence des groupes de sécurité s'affiche, les adresses IPv6 des agents IPv6 purs s'affichent dans la colonne **Adresse IP**. Les adresses IPv6 des agents à double pile s'affichent s'ils ont utilisé leur adresse IPv6 pour s'enregistrer sur le serveur.

Remarque

L'adresse IP utilisée par ces agents à double pile lors de l'enregistrement sur le serveur peut être contrôlée dans la section **Adresse IP préférée** dans **Administration** > **Paramètres généraux** > **Poste de travail/serveur**.

Lorsque vous exportez des paramètres d'agent vers un fichier, les adresses IPv6 s'affichent dans le fichier exporté.

- Journaux

  Les adresses IPv6 des agents à double pile et IPv6 purs apparaissent dans les journaux.

Annexe C

Assistance technique

Découvrez les rubriques suivantes :

Ressources de dépannage

Avant de contacter le service d'assistance technique, consultez les ressources d'aide en ligne suivantes fournies par Trend Micro.

Utilisation du portail d'assistance

Le portail d'assistance de Trend Micro est une ressource en ligne disponible 24 h/24 et 7 j/7 qui contient les informations les plus récentes à la fois sur les problèmes courants et exceptionnels.

Procédure

1. Accédez à https://success.trendmicro.com.
2. Sélectionnez un des produits disponibles ou cliquez sur le bouton approprié pour chercher des solutions.
3. Utilisez la zone **Recherche de support** pour rechercher les solutions disponibles.
4. Si aucune solution n'est trouvée, cliquez sur **Contactez l'Assistance** et sélectionnez le type d'assistance dont vous avez besoin.

   Conseil

   Pour envoyer une demande d'assistance en ligne, visitez l'adresse suivante :

   https://success.trendmicro.com/smb-new-request

   Un ingénieur d'assistance Trend Micro étudie le cas et répond en 24 heures maximum.

Encyclopédie des menaces

De nos jours, la plupart des programmes malveillants sont des menaces combinées : deux technologies ou plus qui sont combinées afin de

contourner les protocoles de sécurité des ordinateurs. Trend Micro lutte contre ces programmes malveillants complexes grâce à des produits qui créent une stratégie de défense personnalisée. L'Encyclopédie des menaces fournit une liste complète des noms et des symptômes de plusieurs menaces combinées, y compris les programmes malveillants, spams, URL malveillantes et failles connues.

Accédez à https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware pour en savoir plus sur :

- Les programmes malveillants et les codes mobiles malveillant actuellement actifs ou « en circulation »
- Les pages contenant des informations relatives aux menaces rassemblées pour former un historique complet des attaques Web
- Les informations sur les menaces Internet concernant les attaques ciblées et les menaces de sécurité
- Les informations sur les attaques Web et sur les tendances sur Internet
- Rapports hebdomadaires sur les programmes malveillants.

Comment contacter Trend Micro

Les revendeurs Trend Micro peuvent être contactés par téléphone ou courrier électronique :

Adresse	Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France
Téléphone	+33 (0) 1 76 68 65 00
Site Web	https://www.trendmicro.com

Adresse électronique	support@trendmicro.com

- Sites d'assistance à travers le monde :

  https://www.trendmicro.com/us/about-us/contact/index.html

- Comment contacter Trend Micro :

  http://www.trendmicro.fr/apropos/contact/index.html

- Documentation sur les produits Trend Micro :

  https://docs.trendmicro.com

Optimisation de la demande d'assistance

Pour améliorer la résolution de vos problèmes, préparez les informations suivantes :

- Étapes permettant de reproduire le problème
- Informations concernant l'appareil ou le réseau
- Marque de l'ordinateur, modèle et tout matériel complémentaire ou périphériques connectés
- Quantité de mémoire et d'espace disque disponible
- Version du système d'exploitation et du Service Pack
- Version de l'agent installé
- Numéro de série ou code d'activation
- Description détaillée de l'environnement d'installation
- Texte exact du message d'erreur affiché

Envoi de contenu suspect à Trend Micro

Plusieurs façons d'envoyer du contenu suspect à Trend Micro pour une analyse plus poussée sont à votre disposition.

services de réputation de messagerie (Email Reputation Services)

Lancez une interrogation de la réputation d'une adresse IP spécifique et indiquez un agent de transfert de messages à inclure dans la liste globale des éléments approuvés :

https://servicecentral.trendmicro.com/en-us/ers/

Reportez-vous à l'entrée suivante de la Base de connaissances pour envoyer des échantillons de messages à Trend Micro :

https://success.trendmicro.com/solution/1112106

Services de File Reputation

Collectez des informations système et envoyez le contenu de fichiers suspects à Trend Micro :

https://success.trendmicro.com/solution/1059565

Notez le numéro de dossier à des fins de suivi.

Services de réputation de sites Web

Lancez une interrogation de l'évaluation de sécurité et du type de contenu d'une URL que vous pensez correspondre à un site de phishing ou un autre « vecteur de menaces » (source de menaces Internet intentionnelles telles que les spywares et programmes malveillants) :

https://global.sitesafety.trendmicro.com/

Si l'évaluation attribuée est incorrecte, envoyez une demande de reclassification à Trend Micro.

Autres ressources

Outre les solutions et l'assistance disponibles en ligne, d'autres ressources, dont le but est de maintenir à jour vos systèmes, de vous informer des innovations les plus récentes et de vous faire connaître les dernières tendances en matière de sécurité, sont également consultables.

Centre de téléchargement

Trend Micro est susceptible de publier, de temps à autre, un patch corrigeant un problème connu ou une mise à niveau s'appliquant à un produit ou service particulier. Pour savoir si des patches sont disponibles, rendez-vous sur le site :

https://www.trendmicro.com/download/

Si l'un des patches disponibles n'a pas été appliqué (les patches sont datés), ouvrez le fichier Lisez-moi afin de déterminer s'il convient à votre environnement. Le fichier Lisez-moi contient également des instructions d'installation.

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°:

https://docs.trendmicro.com/en-us/survey.aspx

Annexe D

Terminologie et concepts du produit

Les éléments contenus dans cette annexe fournissent des informations complémentaires sur les produits et les technologies Trend Micro.

Correctif critique

Un correctif critique est centré sur les problèmes de sécurité pouvant être déployés sur tous les clients. Les correctifs critiques Windows comprennent un programme d'installation alors que les correctifs non issus de Windows disposent en général d'un script d'installation.

Hot Fix

Un correctif de type Hot Fix désigne une solution palliative à un problème spécifique signalé par un utilisateur. Les correctifs de type hotfix sont spécifiques aux problèmes et ne sont dès lors pas proposés à tous les clients. Les correctifs de types hotfix Windows comprennent un programme d'installation. Ce n'est pas le cas des correctifs de types hotfix qui ne sont pas issus de Windows (en général, vous devez arrêter les démons du programme, copier le fichier pour écraser son équivalent dans votre installation, puis redémarrer les démons).

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 agent, car il exploite au minimum les ressources système de l'ordinateur.
- Durée de scan réduite : comme IntelliScan est capable d'identifier le véritable type des fichiers, il ne scanne que les fichiers qui sont vulnérables aux infections. La durée du scan s'en trouve

considérablement réduite, puisque tous les fichiers ne sont pas concernés.

IntelliTrap

IntelliTrap est la technologie heuristique de Trend Micro utilisée pour découvrir les menaces qui utilisent la compression en temps réel ajoutée à d'autres caractéristiques des programmes malveillants, comme celles des utilitaires de compression. Il peut s'agir de virus/programmes malveillants, vers, chevaux de Troie, backdoors et zombies. Les auteurs de virus tentent souvent d'entraver le filtrage de virus/programmes malveillants grâce à différents systèmes de compression de fichiers. IntelliTrap est une technologie de moteur de scan en temps réel, basée sur des règles et qui utilise un système de reconnaissance des fichiers de signatures. Cette technologie permet de détecter et de supprimer les virus/programmes malveillants connus dans des fichiers compressés sur un maximum de 17 couches à l'aide de l'un des 16 types de compression courants.

Remarque

IntelliTrap utilise le même moteur de scan que le scan antivirus. Par conséquent, les règles de traitement de fichier et de scan pour IntelliTrap sont les mêmes que celles définies par l'administrateur pour le scan antivirus.

Les agents consignent les détections de logiciels robots et autres programmes malveillants dans le journal IntelliTrap. Vous pouvez exporter le contenu du journal IntelliTrap pour l'inclure dans des rapports.

IntelliTrap utilise les composants suivants pour rechercher les logiciels robots et autres programmes malveillants :

- Moteur de scan antivirus
- Signature IntelliTrap
- Signature d'exception IntelliTrap

Système de détection d'intrusion

Le système de détection d'intrusion (SDI) contribue à identifier les fichiers de signatures contenus dans des paquets réseau pouvant indiquer une attaque de l'endpoint.

Le système de détection d'intrusion (SDI) contribue à empêcher les intrusions bien connues suivantes :

Système	Description
Fragment trop important	Attaque de refus de service dans le cadre de laquelle un pirate dirige un paquet TCP/UDP surdimensionné vers un Endpoint cible. Cela peut entraîner un dépassement de mémoire tampon, ce qui risque de geler ou de redémarrer l'Endpoint.
Ping of Death	Attaque de refus de service dans le cadre de laquelle un pirate dirige un paquet ICMP/ICMPv6 surdimensionné vers un Endpoint cible. Cela peut entraîner un dépassement de mémoire tampon, ce qui risque de geler ou redémarrer l'Endpoint.
ARP conflictuel	Type d'attaque où un pirate envoie à un Endpoint cible une requête ARP (Address Resolution Protocol) avec des adresses IP source et de destination identiques. L'Endpoint cible s'envoie continuellement une réponse ARP (son adresse MAC), ce qui entraîne son gel ou son blocage.
Flux SYN	Attaque de refus de service dans le cadre de laquelle un programme envoie plusieurs paquets de synchronisation TCP (SYN) à un Endpoint. L'Endpoint envoie alors continuellement en réponse des accusés de réception de synchronisation (SYN/ACK). Cela peut épuiser la mémoire de l'Endpoint et finalement bloquer l'Endpoint.
Fragment de chevauchement	Similaire à une attaque Teardrop, cette attaque de refus de service envoie des fragments TCP de chevauchement à l'Endpoint. Par conséquent, les informations de l'en-tête sont écrasées dans le premier fragment TCP qui risque alors de passer à travers le pare-feu. Le pare-feu peut ensuite autoriser les fragments suivants contenant du code malveillant à atteindre l'Endpoint cible.

Système	Description
Teardrop	Similaire à une attaque de fragment de chevauchement, cette attaque de refus de service a trait à des fragments IP. Une valeur de décalage prêtant à confusion dans le deuxième fragment IP ou dans un fragment ultérieur peut provoquer le blocage du système d'exploitation de l'Endpoint récepteur lorsque celui-ci tente de réassembler les fragments.
attaque par fragment minuscule	Avec ce type d'attaque, un fragment TCP de petite taille force la première en-tête de paquet TCP dans le fragment suivant. Cela peut amener les routeurs filtrant le trafic à ignorer les fragments suivants qui peuvent contenir des données malveillantes.
IGMP fragmenté	Attaque de refus de service qui envoie des paquets IGMP fragmentés à un Endpoint cible, lequel ne peut pas les traiter correctement. Cela peut geler ou ralentir l'Endpoint.
attaque LAND	Type d'attaque qui envoie à l'Endpoint des paquets de synchronisation IP (SYN) dont les adresses source et cible sont identiques. L'Endpoint s'envoie alors en réponse un accusé de réception de synchronisation (SYN/ACK). Cela peut geler ou ralentir l'Endpoint.

Mots-clés

Dans Worry-Free Business Security, les mots-clés incluent les éléments suivants et sont utilisés pour filtrer les messages :

- Mots (pistolets, bombes, etc.)
- Nombres (1, 2, 3, etc.)
- Caractères spéciaux (&, #, +, etc.)
- Locutions (poisson-chat, téléphone rouge, grande maison, etc.)
- Mots ou locutions connectés par des opérateurs logiques (pommes .AND. oranges)

- Mots ou phrases utilisant des expressions rationnelles (.REG. a.*e détecte « armée », « arche » et « archive », mais pas « animal » ou « antivirus »).

Worry-Free Business Security peut importer une liste existante de mots-clés à partir d'un fichier texte (`.txt`). Les mots-clés importés s'affichent dans la liste des mots-clés.

Opérateurs sur mots-clés

Les opérateurs sont des commandes associant plusieurs mots-clés. Ils peuvent élargir ou limiter les résultats d'un critère. Vous devez encadrer les opérateurs par des points (.). Par exemple :

```
pommes .AND. oranges et pommes .NOT. oranges
```

Remarque

un point est placé immédiatement avant et après l'opérateur. Il y a un espace entre le point final et le mot clé.

TABLEAU D-1. Utilisation des opérateurs

OPÉRATEUR	FONCTIONNEMENT	EXEMPLE
N'importe quel mot-clé	Messaging Security Agent recherche le contenu correspondant à ce mot.	Saisissez le mot et ajoutez-le à la liste de mots-clés
OR	Messaging Security Agent recherche chacun des mots-clés séparés par OR. Par exemple, pomme OR orange. L'agent recherche l'un des deux mots. Si un contenu comporte l'un quelconque de ces mots, il y a correspondance.	Saisissez « `.OR.` » entre chacun des mots que vous souhaitez inclure Par exemple, « pomme .OR. orange »

Opérateur	Fonctionnement	Exemple
AND	Messaging Security Agent recherche tous les mots-clés séparés par AND. Par exemple, pomme AND orange. L'agent recherche les deux mots. Si le contenu ne comporte pas les deux mots, il n'y a pas correspondance.	Saisissez « `.AND.` » entre chacun des mots que vous souhaitez inclure Par exemple, « pomme .AND. orange »
NOT	Messaging Security Agent exclut de la recherche les mots-clés suivant l'opérateur NOT. Par exemple, .NOT. jus. L'agent recherche les contenus ne contenant pas le mot jus. Si le message contient « boisson orange », il y a correspondance, mais s'il contient « jus d'orange », il n'y a pas de correspondance.	Saisissez « `.NOT.` » devant tout mot que vous souhaitez exclure Par exemple, « .NOT. jus »
WILD	Le symbole de caractère de substitution remplace une partie du mot manquante. Tous les mots dont l'orthographe comprend le reste du mot correspondent à la recherche. **Remarque** Messaging Security Agent ne prend pas en charge l'utilisation du point d'interrogation « ? » pour la commande de recherche par caractère de substitution « .WILD. ».	Saisissez « `.WILD.` » devant les parties de mots que vous souhaitez inclure Par exemple, si vous souhaitez rechercher tous les mots contenant « valu », saisissez « `.WILD. valu` ». Les mots évaluation, dévaluation et plus-value correspondent.

Opérateur	Fonctionnement	Exemple
REG	Pour définir une expression rationnelle, ajoutez l'opérateur .REG. devant ce modèle (par exemple, .REG. a.*e). Voir *Expressions rationnelles à la page D-10*.	Saisissez « `.REG.` » devant le modèle de mot que vous souhaitez détecter. Par exemple, « .REG. a.*e » correspond à : « approche », « article », « avance », mais pas à « abandon » ni « absent »

Utilisation efficace des mots-clés

Messaging Security Agent offre des fonctions simples et performantes pour créer des filtres très spécifiques. Tenez compte des points suivants lorsque vous créez des règles de filtrage de contenu :

- Par défaut, Messaging Security Agent recherche les correspondances exactes des mots-clés. Utilisez des expressions rationnelles pour rechercher des correspondances partielles de mots-clés. Voir *Expressions rationnelles à la page D-10*.
- Messaging Security Agent analyse les groupes de mots-clés différemment s'ils se trouvent sur une ligne, si chaque mot se trouve sur une ligne distincte et s'ils sont séparés par des virgules, points, traits d'union et autres signes de ponctuation. Consultez le tableau suivant pour obtenir davantage d'informations sur l'utilisation des mots-clés sur plusieurs lignes.
- Vous pouvez également configurer Messaging Security Agent pour qu'il recherche des synonymes des mots-clés concernés.

Tableau D-2. Utilisation des mots-clés

Situation	Exemple	Correspond/ne correspond pas à
Deux mots sur une ligne	pistolets bombes	Correspond à : « Cliquez ici pour acheter pistolets bombes, etc. » Ne correspond pas à : « Cliquez ici pour acheter des pistolets et des bombes. »
Deux mots séparés par une virgule	pistolets, bombes	Correspond à : « Cliquez ici pour acheter pistolets, bombes et autres armes. » Ne correspond pas à : « Cliquez ici pour acheter des pistolets, des bombes et autres armes. »
Mots sur plusieurs lignes	pistolets bombes armes et munitions	Lorsque vous choisissez l'option **Mot-clé spécifié quel qu'il soit** Correspond à : « Pistolets à vendre » Correspond aussi à : « Achetez pistolets, bombes et autres armes » Lorsque vous choisissez l'option **Tous les mots-clés spécifiés** Correspond à : « Achetez des pistolets, bombes, armes et munitions » Ne correspond pas à : « Achetez des pistolets bombes armes munitions. » Ne correspond pas non plus à : « Achetez des pistolets, bombes, armes, et munitions »

Situation	Exemple	Correspond/ne correspond pas à
Plusieurs mots sur une seule ligne	pistolets bombes armes munitions	Correspond à : « Achetez des pistolets bombes armes munitions » Ne correspond pas à : « Achetez des munitions pour vos pistolets et des armes et des bombes »

Correctif

Un patch désigne un groupe de hot fixes et de correctifs de sécurité qui résolvent plusieurs problèmes du programme. Trend Micro publie régulièrement des patchs. Les patchs Windows comprennent un programme d'installation alors que les patchs non issus de Windows disposent en général d'un script d'installation.

Expressions rationnelles

Les expressions rationnelles sont utilisées pour faire correspondre des chaînes de caractères. Les tableaux suivants montrent des exemples courants d'expressions rationnelles. Pour spécifier une expression rationnelle, ajoutez un opérateur « .REG. » devant ce modèle.

Un certain nombre de sites Web et de didacticiels sont disponibles en ligne. Parmi ces sites, vous pouvez consulter le site PerlDoc à l'adresse suivante :

http://www.perl.com/doc/manual/html/pod/perlre.html

AVERTISSEMENT!

Les expressions rationnelles constituent un outil puissant de correspondance de chaînes. C'est pourquoi Trend Micro recommande que les administrateurs qui choisissent d'utiliser les expressions rationnelles soient familiarisés et expérimentés en ce qui concerne la syntaxe de ces expressions. Les expressions rationnelles n'utilisant pas une syntaxe correcte peuvent occasionner des dégâts considérables au niveau des performances. Trend Micro recommande de commencer par des expressions rationnelles simples n'utilisant pas de syntaxe complexe. Pour introduire une nouvelle règle, utilisez l'action d'archivage et étudiez la façon dont Messaging Security Agent gère les messages à l'aide de cette règle. Si vous êtes sûr que la règle ne peut pas avoir de conséquences inattendues, vous pouvez modifier votre action.

Exemples d'expressions rationnelles

Les tableaux suivants montrent des exemples courants d'expressions rationnelles. Pour spécifier une expression rationnelle, ajoutez un opérateur « .REG. » devant ce modèle.

TABLEAU D-3. Dénombrement et groupement

ÉLÉMENT	SIGNIFICATION	EXEMPLE
.	Un point peut représenter n'importe quel caractère excepté les caractères de nouvelle ligne.	ar. correspond à : art, ars, are, arc, ara, etc. a.r correspond à : amer, amour, etc.
*	L'astérisque indique zéro ou une occurrence ou plus de l'élément qui précède.	cre* correspond à : cr, cre, cree, creee, creeee, etc.
+	Le signe plus indique une occurrence ou plus de l'élément qui précède.	cre+ correspond à : cre, cree, creee, creeee, etc. mais ne correspond pas à :cr
?	Le point d'interrogation indique zéro ou une occurrence de l'élément qui précède.	f?l correspond à fl ou fil, mais ne correspond pas à : fiil, fiiil, etc.

Élément	Signification	Exemple
( )	Les parenthèses indiquent que le groupe qu'elles incluent doit être considéré comme une seule entité.	d(ent)+ correspond à dent ou dentent ou dententent, etc. Le signe + s'applique à l'élément entre parenthèses. L'expression rationnelle recherche d suivi d'une ou plusieurs occurrences de « ent. »
[ ]	Les crochets indiquent une série de caractères.	d[aeiouy]+ correspond à : da, de, di, do, du, dy, daa, dae, dai, etc. Le signe + s'applique à la série de caractères entre parenthèses. L'expression rationnelle recherche d suivi d'un ou plusieurs caractères de la série [aeioy]. d[A-Z] correspond à dA, dB, dC, etc. jusqu'à dZ. La série entre crochets représente l'intervalle de lettres majuscules de A à Z.
[^]	Un accent circonflexe compris dans une série entre crochets entraîne la négation de la série ou de l'intervalle spécifié, c'est-à-dire que l'expression rationnelle correspond à n'importe quel caractère n'étant pas inclus dans la série ou l'intervalle.	d[^aeiouy] correspond à : db, dc ou dd, d9, d#--d suivi de n'importe quel caractère n'étant pas une voyelle.
{ }	Les accolades définissent le nombre d'occurrences de l'élément qui précède. Une valeur unique entre accolades indique que le nombre d'occurrences doit correspondre à ce chiffre. Deux chiffres séparés par une virgule représentent une série de nombres d'occurrences valides du caractère qui précède. Un chiffre unique suivi d'une virgule signifie qu'il n'y a pas de limite supérieure.	da{3} correspond à : daaa--d suivi de 3 occurrences de « a », pas plus. da{2,4} correspond à : daa, daaa et daaaa (mais ne correspond pas à daaaaa)--d suivi de 2, 3 ou 4 occurrences de « a ». da{4,} correspond à : daaaa, daaaaa, daaaaaa, etc.--d suivi de 4 occurrences de « a » ou plus.

Tableau D-4. Classes de caractères (sténographie)

Élément	Signification	Exemple
\d	Tout caractère numérique, équivalent de la classe [0-9] ou [[:digit:]]	\d correspond à 1, 12, 123, etc., mais ne correspond pas à 1b7--un ou plusieurs caractères numériques quels qu'ils soient.
\D	Tout caractère non numérique ; équivalent de la classe [^0-9] ou [^[:digit:]]	\D correspond à : a, ab, ab&, mais ne correspond pas à 1--un ou plusieurs caractères quelconques sauf 0, 1, 2, 3, 4, 5, 6, 7, 8, ou 9.
\w	Tout caractère de « mot » --c'est-à-dire tout caractère alphanumérique; équivalent à la classe [_A-Za-z0-9] ou [_[:alnum:]]	\w correspond à a, ab, a1, mais ne correspond pas à !&--une ou plusieurs lettres minuscules ou majuscules ou un ou plusieurs chiffres, mais pas de signes de ponctuation ou autres caractères spéciaux.
\W	Tout caractère non alphanumérique ; équivalent de la classe [^_A-Za-z0-9] ou [^_[:alnum:]]	\W correspond à *, &, mais ne correspond pas à ame ou à a1--un ou plusieurs caractères quelconques sauf lettres en majuscules ou en minuscules et chiffres.
\s	Tout élément marquant un espace : espace, caractère de nouvelle ligne, tabulation, espace insécable, etc. ; équivalent de la classe [[:space]]	légume\s correspond à « légume » suivi d'un élément d'espacement quelconque. Ainsi, la phrase « J'ai un légume dans mon jardin » déclenche l'expression rationnelle, mais pas « J'aime les légumes du jardin ».
\S	Tout élément ne marquant pas un espace ; tout élément autre qu'un espace, caractère de nouvelle ligne, tabulation, espace insécable, etc. ; équivalent à [^[:space]]	légume\s correspond à « légume » suivi d'un élément ne marquant pas un espace. Ainsi, la phrase « J'aime les légumes du jardin » déclenche l'expression rationnelle, mais pas « J'ai un légume dans mon jardin ».

TABLEAU D-5. Classes de caractères

ÉLÉMENT	SIGNIFICATION	EXEMPLE
[:alpha:]	Tout caractère alphabétique	.REG. [[:alpha:]] correspond à abc, def, xxx, mais ne correspond pas à 123 ou à @#$.
[:digit:]	Tout caractère numérique ; équivalent à la classe \d	.REG. [[:digit:]] correspond à 1, 12, 123, etc.
[:alnum:]	Tout « mot » --c'est-à-dire, tout caractère alphanumérique ; équivalent à la classe \w	.REG. [[:alnum:]] correspond à abc, 123, mais ne correspond pas à ~!@.
[:space:]	Tout élément marquant un espace ; espace, caractère de nouvelle ligne, tabulation, espace insécable, etc. ; équivalent à \s	.REG. (légume)[[:space:]] correspond à « légume » suivi d'un élément d'espacement quelconque. Ainsi, la phrase « J'ai un légume dans mon jardin » déclenche l'expression rationnelle, mais pas « J'aime les légumes du jardin ».
[:graph:]	Tout caractère excepté les caractères d'espacement, caractères de contrôle et équivalents	.REG. [[:graph:]] correspond à 123, abc, xxx, ><", mais ne correspond pas à un espace ou un caractère de contrôle.
[:print:]	Tout caractère (de la même façon que [:graph:]) mais inclut les espaces	.REG. [[:print:]] correspond à 123, abc, xxx, ><", et aux espaces.
[:cntrl:]	Tout caractère de contrôle (comme CTRL + C, CTRL + X)	.REG. [[:cntrl:]] correspond à 0x03, 0x08, mais ne correspond pas à abc, 123, !@#.
[:blank:]	Caractères d'espacement et de tabulation	.REG. [[:blank:]] correspond aux caractères d'espacement et de tabulation, mais ne correspond pas à 123, abc, !@#
[:punct:]	Caractères de ponctuation	.REG. [[:punct:]] correspond à ; : ? ! ~ @ # $ % & * ‘ “ , etc., mais ne correspond pas à 123, abc

Élément	Signification	Exemple
[:lower:]	Tout caractère alphabétique en minuscules (remarque : l'option « Résultats sensibles à la casse » doit être activée, sans quoi la fonction fonctionne comme [:alnum:])	.REG. [[:lower:]] correspond à abc, Def, sTress, Do, etc., mais ne correspond pas à ABC, DEF, STRESS, DO, 123, !@#.
[:upper:]	tout caractère alphabétique en majuscules (remarque : l'option « Résultats sensibles à la casse » doit être activée, sans quoi la fonction fonctionne comme [:alnum:])	.REG. [[:upper:]] correspond à ABC, DEF, STRESS, DO, etc., mais ne correspond pas à abc, Def, Stress, Do, 123, !@#.
[:xdigit:]	Chiffres autorisés dans un nombre hexadécimal (0-9a-fA-F)	.REG. [[:xdigit:]] correspond à 0a, 7E, 0f, etc.

Tableau D-6. Motifs d'ancrage

Élément	Signification	Exemple
^	Indique le début d'une chaîne.	^(malgré) correspond à toute section de texte commençant par « malgré ». Ainsi la phrase « malgré le fait que j'aie des légumes dans mon jardin » déclenche l'expression rationnelle, mais pas « Le fait que j'aie des légumes dans mon jardin malgré tout ».
$	Indique la fin d'une chaîne.	(malgré)$ correspond à toute section de texte finissant par « malgré ». Ainsi la phrase « malgré le fait que j'aie des légumes dans mon jardin » ne déclenche pas l'expression rationnelle, mais « Le fait que j'aie des légumes dans mon jardin malgré tout ».

TABLEAU D-7. Séquences d'échappement et chaînes littérales

ÉLÉMENT	SIGNIFICATION	EXEMPLE
\	Pour correspondre à des caractères ayant une signification particulière dans une expression rationnelle (par exemple, « + »).	(1) .REG. C\\C\+\+ correspond à 'C\C++'. (2) .REG. * correspond à *. (3) .REG. \? correspond à ?.
\t	Indique une tabulation.	(stress)\t correspond à toute section de texte contenant l'élément « stress » suivi immédiatement d'une tabulation (ASCII 0x09).
\n	Indique un caractère de nouvelle ligne. **Remarque** le caractère de nouvelle ligne peut être représenté différemment suivant les plates-formes. Sous Windows, un caractère de nouvelle ligne est représenté par une série de deux caractères, un retour chariot suivi d'un saut de ligne. Sous Unix et Linux, une nouvelle ligne correspond juste à un saut de ligne, et sous Macintosh à un retour chariot.	(stress)\n\n correspond à toute section de texte contenant l'élément « stress » suivi immédiatement de deux caractères de nouvelle ligne (ASCII 0x0A).
\r	Indique un caractère de retour chariot.	(stress)\r correspond à toute section de texte contenant l'élément « stress » suivi immédiatement d'un caractère de retour chariot (ASCII 0x0D).

Élément	Signification	Exemple
\b	Indique un espacement arrière. OR Indique les limites	(stress)\b correspond à toute section de texte contenant l'élément « stress » suivi immédiatement d'un espacement arrière (ASCII 0x08). Une limite de mot (\b) est définie comme un point entre deux caractères avec un \w d'un côté et un \W de l'autre côté (dans l'un ou l'autre ordre), comptant les caractères imaginaires du début jusqu'à la fin de la chaîne correspondant à \W. (Dans les classes de caractères, \b représente un espacement arrière plutôt qu'une limite de mot.) Par exemple, l'expression rationnelle suivante peut correspondre à un numéro de sécurité sociale : .REG. \b\d{3}-\d{2}-\d{4}\b
\xhh	Indique un caractère ASCII avec un code hexadécimal donné (où hh représente une valeur hex à deux chiffres quelconque).	\x7E(\w){6} correspond à toute section de texte contenant un « mot » d'exactement six caractères alphanumériques précédé d'un ~ (tilde). Ainsi, les mots '~ab12cd', '~Pa3499' correspondent, mais '~oops' ne correspond pas.

Générateur d'expressions rationnelles

Lorsque vous choisissez le mode de configuration des règles pour la prévention de la perte de données, tenez compte du fait que le générateur d'expressions rationnelles ne peut créer que des expressions simples, conformément aux règles et restrictions suivantes :

- Seuls des caractères alphanumériques peuvent former des variables.

- Tous les autres caractères, tels que [-], [/], etc., ne peuvent être que des constantes.
- Les plages de variables ne peuvent être comprises qu'entre A et Z et 0 à 9 ; vous ne pouvez pas les limiter, par exemple, à A-D.
- Les expressions rationnelles générées par cet outil respectent la casse.
- Les expressions rationnelles générées par cet outil ne gèrent que les correspondances positives, pas les correspondances négatives (« si ne correspond pas à »).
- Les expressions fondées sur votre échantillon ne peuvent correspondre qu'au nombre exact de caractères et d'espaces de ce dernier ; l'outil ne peut pas générer de modèles correspondant à « un ou plusieurs » pour un caractère ou une chaîne donnée.

Syntaxe d'expression complexe

Une expression de mot-clé est composée de jetons, qui sont l'unité la plus petite utilisée pour faire correspondre l'expression et le contenu. Un jeton peut être un opérateur, un symbole logique ou l'opérande, c'est-à-dire la valeur ou l'argument sur lequel agit l'opérateur.

Les opérateurs comprennent : .AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., ".(." et " .)." L'opérande et l'opérateur doivent être séparés par un espace. Un opérande peut aussi contenir plusieurs jetons. Voir *Mots-clés à la page D-5*.

Fonctionnement des expressions rationnelles

L'exemple suivant décrit comment fonctionne le filtre de contenu de la Sécurité Sociale (l'un des filtres par défaut) :

[Format] .REG. \b\d{3}-\d{2}-\d{4}\b

L'expression ci-dessus utilise \b, un caractère d'espacement arrière, suivi de \d, n'importe quel chiffre, puis de {x}, indiquant le nombre de chiffres, et enfin, -, signalant un tiret. Cette expression correspond au numéro de sécurité sociale. Le tableau suivant décrit les chaînes de caractères qui correspondent à l'exemple de l'expression rationnelle :

TABLEAU D-8. Numéros correspondant à l'expression rationnelle de la Sécurité Sociale

.REG. \b\d{3}-\d{2}-\d{4}\b	
333-22-4444	Correspond
333224444	Ne correspond pas
333 22 4444	Ne correspond pas
3333-22-4444	Ne correspond pas
333-22-44444	Ne correspond pas

Si vous modifiez l'expression de la façon suivante

[Format] .REG. \b\d{3}\x20\d{2}\x20\d{4}\b

la nouvelle expression correspond à la séquence suivante :

333 22 4444

Listes des exclusions de scan

Liste des exclusions de scan pour les agents Security Agent

Cette liste d'exclusion contient tous les produits Trend Micro exclus par défaut des opérations de scan.

TABLEAU D-9. Liste des exclusions des agents Security Agent

NOM DU PRODUIT	EMPLACEMENT DU CHEMIN D'INSTALLATION

InterScan eManager 3.5x	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\VersionActuelle`
	
	`ProgramDirectory=`

ScanMail eManager (ScanMail for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\VersionActuelle`
	
	`ProgramDirectory=`

Nom du produit	Emplacement du chemin d'installation
ScanMail for Lotus Notes (SMLN) eManager NT	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\VersionActuelle AppDir= DataDir= IniDir=
InterScan Web Security Suite (IWSS)	HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite Programmes= C:\Program Files\Trend Micro\IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\VersionActuelle ProgramDirectory=
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\VersionActuelle ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\VersionActuelle ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\VersionActuelle ProgramDirectory={Lecteur d'installation}:\INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\VersionActuelle ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \VersionActuelle ProgramDirectory=

Nom du produit	Emplacement du chemin d'installation
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \VersionActuelle HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=

NOM DU PRODUIT	EMPLACEMENT DU CHEMIN D'INSTALLATION
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\VersionActuelle TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption \Advance QuarantineFolder=

NOM DU PRODUIT	EMPLACEMENT DU CHEMIN D'INSTALLATION
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager QMDir= Rechercher le fichier exclusion.txt dans le répertoire HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir Accédez au répertoire HomeDir (par ex. C:\Program Files\Trend Micro\Messaging Security Agent\) Ouvrez le fichier exclusion.txt C:\Program Files\Trend Micro\Messaging Security Agent\Temp\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\ C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool

Listes des exclusions de scan pour l'agent Messaging Security Agent (Advanced uniquement)

Par défaut, lorsque Messaging Security Agent est installé sur un serveur Microsoft Exchange (2000 ou version ultérieure), il ne scanne pas les bases

de données Microsoft Exchange, les fichiers journaux Microsoft Exchange, les dossiers de serveur virtuel ou le lecteur M:\. La liste d'exclusions est enregistrée dans le répertoire :

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp
\VersionActuelle\Misc.

ExcludeExchangeStoreFiles=C:\Program Files\Exchsrvr\mdbdata\

priv1.stm|C:\Program Files\Exchsrvr\mdbdata\

priv1.edb|C:\Program Files\Exchsrvr\mdbdata\

pub1.stm|C:\Program Files\Exchsrvr\mdbdata\pub1.edb

ExcludeExchangeStoreFolders=C:\Program Files\Exchsrvr\mdbdata\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\Queue\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\PickUp\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\BadMail\
```

Pour tous les autres dossiers Microsoft Exchange recommandés, veuillez les ajouter manuellement à la liste des exclusions de scan. Voir http://support.microsoft.com/kb/245822/.

Exclusions SBS 2003

Pour SBS 2003, ajoutez manuellement les éléments suivants :

Exclusions Microsoft Exchange	
Base de données Microsoft Exchange Server	`C:\Program Files\Exchsrvr\MDBDATA`
Fichiers MTA Microsoft Exchange	`C:\Program Files\Exchsrvr\Mtadata`
Fichiers journaux de suivi des messages Microsoft Exchange	`C:\Program Files\Exchsrvr\server_name.log`
Mailroot SMTP Microsoft Exchange	`C:\Program Files\Exchsrvr\Mailroot`

Fichiers de fonctionnement Microsoft Exchange	`C:\Program Files\Exchsrvr\MDBDATA`
Service de réplication de sites	`C:\Program Files\Exchsrvr\srsdata` `C:\Program Files\Exchsrvr\conndata`
Exclusions IIS	
Fichiers système IIS	`C:\WINDOWS\system32\inetsrv`
Dossier de compression IIS	`Fichiers temporaires compressés` `C:\WINDOWS\IIS`
Exclusions du contrôleur de domaine	
Fichiers de base de données Active Directory	`C:\WINDOWS\NTDS`
SYSVOL	`C:\WINDOWS\SYSVOL`
Fichiers de base de données NTFRS	`C:\WINDOWS\ntfrs`
Exclusions de services Windows SharePoint	
Dossier temporaire SharePoint	`C:\windows\temp\FrontPageTempDir`
Exclusions de dossiers du poste de travail client	
Magasin Windows Update	`C:\WINDOWS\SoftwareDistribution\DataStore`
Exclusions supplémentaires	
Base de données de stockage amovible (utilisée par SBS Backup)	`C:\Windows\system32\NtmsData`

Échecs de messages du connecteur POP3 SBS	`C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail`
Messages entrants du connecteur POP3 SBS	`C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail`
Magasin Windows Update	`C:\WINDOWS\SoftwareDistribution\DataStore`
Magasin de données DHCP	`C:\WINDOWS\system32\dhcp`
Magasin de données WINS	`C:\WINDOWS\system32\wins`

Service Pack

Un Service Pack désigne un regroupement de hot fixes, de correctifs et d'améliorations de fonctions suffisamment significatives pour être considérées comme une mise à niveau du produit. Les service packs Windows et non-Windows contiennent un programme et un script d'installation.

Ports des chevaux de Troie

Les ports de chevaux de Troie sont couramment utilisés par les programmes de type cheval de Troie pour se connecter à des clients. Lors d'une épidémie, Worry-Free Business Security bloque les numéros de port suivants, susceptibles d'être utilisés par les chevaux de Troie :

TABLEAU D-10. Ports des chevaux de Troie

NUMÉRO DE PORT	CHEVAL DE TROIE	NUMÉRO DE PORT	CHEVAL DE TROIE
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker

Numéro de port	Cheval de Troie	Numéro de port	Cheval de Troie
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Fichiers non nettoyables

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

TABLEAU D-11. Solutions aux fichiers non nettoyables

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
Fichiers infectés par des chevaux de Troie	Les chevaux de Troie sont des programmes qui exécutent des actions inattendues, non autorisées et généralement malveillantes, telles que l'affichage de messages, l'écrasement de fichiers ou le formatage de disques. Il est inutile de nettoyer les fichiers puisque les chevaux de Troie ne les infectent pas. Solution : le moteur Damage Cleanup et le modèle Damage Cleanup suppriment les chevaux de Troie.
Fichiers infectés par des vers	Un ver 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 de client. 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 permettre le nettoyage du fichier.
Fichiers protégés par mot de passe	Les fichiers protégés par mot de passe incluent les fichiers compressés protégés par mot de passe et les fichiers Microsoft Office protégés par mot de passe. Solution : supprimez la protection par mot de passe pour permettre le nettoyage du fichier.
Fichiers de sauvegarde	Les fichiers possédant une extension RB0~RB9 sont des copies de sauvegarde des fichiers infectés. Le processus de nettoyage crée une sauvegarde du fichier infecté au cas où le virus/programme malveillant l'endommagerait au cours du processus de nettoyage. Solution : si le nettoyage réussit, vous n'avez pas besoin de conserver la copie de sauvegarde du fichier infecté. Si le client fonctionne correctement, vous pouvez supprimer le fichier de sauvegarde.
Fichiers infectés dans la corbeille	Il peut arriver que le système n'autorise pas la suppression des fichiers infectés présents dans la corbeille, car le système est en cours d'exécution. Solution :

Fichier non nettoyable	Explication et solution

	1. Redémarrez le client en mode MS-DOS.
	2. Ouvrez l'invite de commande.
	3. Saisissez ce qui suit pour effacer les fichiers :
	`cd \`
	`cd recycled`
	`del *.* /S`
	La dernière commande supprime tous les fichiers de la corbeille.

Fichiers infectés dans le dossier Temp de Windows ou dans un dossier temporaire d'Internet Explorer	Il peut arriver que le système n'autorise pas le nettoyage des fichiers infectés présents dans le dossier Temp de Windows ou dans le dossier temporaire d'Internet Explorer, car le client les utilise. Les fichiers à nettoyer sont peut-être des fichiers temporaires nécessaires au fonctionnement de Windows.
	Solution :
	1. Redémarrez le client en mode MS-DOS.
	2. Si le fichier infecté se trouve dans le dossier Temp de Windows:
	a. Ouvrez l'invite de commande et accédez au dossier Temp de Windows (situé sous `C:\Windows\Temp` par défaut).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd temp`
	`attrib -h`
	`del *.* /S`
	La dernière commande supprime tous les fichiers du dossier Temp de Windows.
	c. Redémarrez le client en mode normal.
	3. Si le fichier infecté se trouve dans le dossier temporaire d'Internet Explorer:
	a. Ouvrez une invite de commande et accédez au dossier Temp d'Internet Explorer (situé sous `C:\Users\<votre nom`

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION

	`d'utilisateur>\AppData\Local\Microsoft\Windows \Temporary Internet Files` par défaut).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	La dernière commande supprime tous les fichiers du dossier temporaire d'Internet Explorer.
	c. Redémarrez le client en mode normal.

Fichiers compressés à l'aide d'un format de compression non pris en charge	Solution : décompressez les fichiers.
Fichiers verrouillés ou en cours d'exécution	Solution : déverrouillez les fichiers ou attendez qu'ils aient été exécutés.
Fichiers corrompus	Solution : supprimez les fichiers.

Index

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

www.trendmicro.com

Item Code: WFFM108701/190701