



TREND MICRO™ Remote Manager

Guide de l'utilisateur



Protection en ligne

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

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

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

© 2014 Trend Micro Incorporated. Tous droits réservés.

Référence du document : APFM36398/140410

Date de publication : avril 2014

Protégé par le brevet américain n° : Brevets en attente.

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

Vous trouverez des informations détaillées sur l'utilisation des fonctionnalités spécifiques du produit/service dans le centre d'aide en ligne Trend Micro et/ou la base de connaissances Trend Micro.

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

Évaluez cette documentation sur le site Web suivant :

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

Table des matières

Préface

Préface	vii
À propos de Trend Micro	viii
Public	viii
Conventions typographiques du document	viii

Chapitre 1: Introduction

Trend Micro Remote Manager	1-2
Fonctions	1-4
Plate-forme intégrée	1-4
Widgets Tableau de bord	1-5
Paramètres personnalisables des nouveaux comptes	1-5
État des menaces	1-5
État du système	1-6
État de la licence	1-7
Gestion du réseau	1-7
Génération de rapports	1-7
Intégration avec les outils tiers	1-8
Envoi de commentaires	1-8
Produits pris en charge	1-8
Worry-Free Business Security Suite	1-9
Hosted Email Security	1-10
Les outils tiers	1-10
Nouveautés	1-15
Infrastructure générale	1-17
Terminologie clé	1-19

Chapitre 2: Démarrage

Configuration requise du navigateur	2-2
Ajout de l'URL de la console Web Trend Micro Remote Manager aux sites de confiance	2-2
Utilisation d'Internet Explorer 9 pour obtenir le certificat SSL	2-3
Accès à la plate-forme	2-3
Coordination avec le client	2-4

Chapitre 3: Présentation de la console Web

La bannière de la console Web	3-2
Menu principal	3-3
Explication du tableau de bord	3-4
Écrans du tableau de bord État	3-4
Onglets et widgets	3-5
Informations sur le produit/service	3-18

Chapitre 4: Préparation de l'infrastructure

Présentation de l'installation de l'infrastructure	4-2
Worry-Free Business Security Standard et Advanced	4-2
Hosted Email Security et Worry-Free Business Security Services ..	4-2
ConnectWise	4-2
Kaseya	4-3
Autotask	4-3
Ajout de produits	4-3
Ajout de clients	4-3
Enregistrement des produits Trend Micro dans Trend Micro Remote Manager	4-8
Intégration de produits tiers à Trend Micro Remote Manager	4-15

Chapitre 5: Gestion des clients

Clients	5-2
Ajout de nouveaux clients	5-2
Association de comptes	5-7

Vérification de la licence du produit	5-9
Ajout de produits/services	5-9
Contacts	5-10
Suppression de clients	5-13
Filtrage de la liste des clients	5-13

Chapitre 6: Gestion des agents

Gestion des agents à partir de la console Web Remote Manager	6-2
Vérification de la connexion entre l'agent et le serveur	6-2
État de l'agent	6-2
Envoi des commandes d'agents	6-4
Affichage des détails relatifs à l'agent	6-5
Gestion des agents à partir du serveur géré	6-6
Messages d'état de l'agent	6-6
Modification du GUID de l'agent sur le serveur géré	6-6
Utilisation de l'outil de configuration de l'agent	6-7
Configuration de l'agent	6-8
Sauvegarde et restauration des paramètres de l'agent	6-11
Sauvegarde des paramètres	6-11
Restauration des paramètres	6-12
Recherche du numéro de compilation de l'agent	6-13
À partir de la console Web Remote Manager	6-13
Sur l'agent	6-13
Emplacement des journaux de l'agent et des fichiers de configuration	6-14
Activation du journal de débogage de l'agent	6-14
Suppression d'agents	6-14
Suppression des agents localement	6-15

Chapitre 7: Gestion des licences

Ajout de sièges affectés	7-2
Renouvellement de licences	7-2

Chapitre 8: Gestion des paramètres

Configuration des notifications	8-2
---------------------------------------	-----

Configuration des paramètres de console	8-3
Configuration de modèles de paramètres par défaut	8-4

Chapitre 9: Gestion des événements

Gestion des événements	9-2
Affichage des événements	9-4
Types d'événement	9-5
Détails sur l'état de défense anti-épidémies	9-5
Détails sur l'état antivirus	9-7
Détails sur l'état anti-spyware	9-9
Détails sur l'état anti-spam	9-11
Détails sur l'état des virus de réseau	9-11
Détails sur l'état de réputation de sites Web	9-12
Détails sur l'état de surveillance des comportements	9-13
Détails sur l'état du filtrage d'URL	9-13
Détails sur l'état du contrôle des périphériques	9-14
Smart Scan	9-14
Mise à jour des composants	9-15
Espace disque utilisé	9-16

Chapitre 10: Rapports

Présentation des rapports	10-2
Création de rapports	10-3
Création de modèles de rapport	10-3
Affichage des rapports	10-7
Modification des rapports	10-7
Téléchargement et envoi de rapports	10-8
Abonnement aux rapports	10-8

Chapitre 11: Dépannage et problèmes connus

Dépannage de la console Web Trend Micro Remote Manager	11-2
Problèmes d'accès	11-2

Arborescence des domaines invisible après l'installation de l'agent	11-2
Un nœud de l'arborescence ne se développe pas	11-3
Impossible d'afficher la page	11-4
Informations incorrectes sur le tableau de bord	11-4
Impossible de déployer des commandes	11-5
État de l'agent anormal	11-5
L'agent fonctionne de façon anormale en utilisant un GUID existant après... ..	11-6
Dépannage de l'agent	11-6
Problèmes d'agent	11-6
Connexion au serveur impossible	11-8
Enregistrement avec le serveur distant impossible	11-9
Problèmes de connexion avec Hosted Email Security	11-10
Problèmes de serveur connus	11-11
Icônes d'état incohérentes	11-11
Données de spam incohérentes avec Worry-Free Business Security Standard ou Advanced	11-11
Nom d'utilisateur incorrect sur la console Worry-Free Business Security Services	11-12
Infos sur la licence incohérentes sur la console Worry-Free Business Security Services	11-12
Les connexions simultanées à partir de deux onglets/fenêtres du même navigateur ne sont pas autorisées	11-12
Les rapports historiques sont automatiquement supprimés	11-13
Un compte Worry-Free Business Security Services arrivé à expiration ne peut pas être géré	11-13
Connexion ConnectWise interrompue	11-13
Problèmes d'agent connus	11-14
Les agents réinstallés fournissent des données se chevauchant ..	11-14
Les résultats de la commande de scan ne peuvent pas être vérifiés	11-14
L'outil de configuration de l'agent n'est pas visible après la mise à niveau de ce dernier	11-14
FAQ	11-15
Foire aux questions de la console Web	11-15
Foire aux questions Hosted Email Security	11-17

Foire aux questions sur les rapports 11-18

Chapitre 12: Obtenir de l'aide

Comment contacter Trend Micro 12-2
Optimisation de la demande d'assistance 12-2
Utilisation du portail d'assistance 12-3
Encyclopédie des menaces 12-3
À propos de Trend Micro 12-4
TrendLabs 12-5

Index

Index IN-1

Préface

Préface

Le manuel de l'utilisateur Remote Manager™ fournit des détails sur la façon d'utiliser la plate-forme et d'effectuer les tâches de base.

Les rubriques comprennent :

- *À propos de Trend Micro à la page viii*
- *Public à la page viii*
- *Conventions typographiques du document à la page viii*

À propos de Trend Micro

En tant que leader mondial de la sécurité cloud, Trend Micro développe des solutions de sécurité de contenu Internet et de gestion des menaces pour que les entreprises et les consommateurs puissent échanger des informations numériques dans un environnement sécurisé. Avec plus de 20 ans d'expérience, Trend Micro fournit des solutions client, serveur et cloud de premier plan qui arrêtent les menaces plus rapidement et qui protègent les données des environnements physiques, virtuels et cloud.

À mesure de l'apparition de nouvelles menaces et failles, Trend Micro s'engage à aider les clients à sécuriser les données, à assurer la conformité, à réduire les coûts et à protéger l'intégrité de l'entreprise. Pour plus d'informations, rendez-vous sur :

<http://www.trendmicro.com>

Trend Micro et le logo t-ball de Trend Micro sont des marques commerciales de Trend Micro Incorporated et sont enregistrées dans certains pays. Toutes les autres marques sont des marques commerciales ou déposées de leurs propriétaires respectifs.

Public

Le manuel de l'utilisateur Trend Micro Remote Manager est destiné aux partenaires et fournisseurs de services gérés (MSP) qui utilisent la plate-forme pour surveiller et gérer à tout moment l'intégralité du portefeuille de produits Trend Micro SMB d'un partenaire, pour tous ses clients, en tout lieu et à tout moment.

Conventions typographiques du document

Le manuel de l'utilisateur Remote Manager™ utilise les conventions suivantes.

TABEAU 1. Conventions typographiques du document

CONVENTION	DESCRIPTION
TOUT EN MAJUSCULES	Acronymes, abréviations, noms de certaines commandes et touches du clavier

CONVENTION	DESCRIPTION
Gras	Menus et commandes de menus, boutons de commande, onglets et options
Chemin de > navigation	Le chemin de navigation permettant d'atteindre un écran spécifique Par exemple, Fichier > Enregistrer signifie que vous devez cliquer sur Fichier , puis Enregistrer sur l'interface
 Remarque	Remarques de configuration
 Conseil	Recommandations ou suggestions
 AVERTISSEMENT!	Actions critiques et options de configuration

Chapitre 1

Introduction

Cette section contient les rubriques suivantes :

- *Trend Micro™ Remote Manager™ à la page 1-2*
- *Fonctions à la page 1-4*
- *Produits pris en charge à la page 1-8*
- *Nouveautés à la page 1-15*
- *Infrastructure générale à la page 1-17*
- *Terminologie clé à la page 1-19*

Trend Micro™ Remote Manager™

Trend Micro™ Remote Manager™ est une console fiable qui fonctionne en parallèle avec Trend Micro Licensing Management Platform™ pour fournir des services de sécurité gérés aux petites et moyennes entreprises.

Remote Manager vous permet de surveiller l'intégrité de plusieurs réseaux gérés grâce à de multiples produits et services gérés. Trend Micro Remote Manager permet aux administrateurs revendeurs de générer des commandes pour gérer les aspects critiques de la sécurité réseau.

Remote Manager est hébergé sur les serveurs des centres de données régionaux Trend Micro pour lesquels les revendeurs peuvent obtenir un compte. Les revendeurs peuvent utiliser Remote Manager pour créer des comptes client, surveiller les réseaux client et gérer la sécurité à l'aide de la console Web Remote Manager.

Remote Manager surveille les produits suivants :

- Worry-Free Business Security™ Standard (anciennement Client Server Suite) versions 6.x, 7.x, 8.0 et 9.0
- Worry-Free Business Security Advanced (anciennement Client Server Messaging Suite) versions 6.x, 7.x, 8.0 et 9.0
- Worry-Free Business Security Services versions 5.0, 5.1, 5.2, 5.3, 5.3 SP1



Remarque

Worry-Free Business Security Standard et Advanced, et Worry-Free Business Security Services sont collectivement appelés Worry-Free Business Security (tous), le cas échéant.

- Trend Micro Hosted Email Security™ version 1.x



Remarque

Worry-Free Business Security Standard et Advanced, Worry-Free Business Security Services, et Hosted Email Security sont collectivement désignés par l'expression « produits gérés » et/ou « services gérés » dans ce document.

Remote Manager inclut un tableau de bord de surveillance qui permet aux revendeurs de surveiller les aspects suivants de la sécurité réseau :

- Worry-Free Business Security (tous) :
 - Incidents liés aux virus, virus de réseau et spywares/graywares
 - Incidents liés au spam et au phishing
 - Modifications non autorisées apportées aux ordinateurs
 - Situations d'épidémie
 - État des licences et des mises à jour des produits de sécurité
 - Espace disque utilisé sur les postes de travail, les serveurs et les serveurs Exchange (Worry-Free Business Security Standard et Advanced uniquement)
 - Principaux indicateurs de sécurité
- Hosted Email Security :
 - Trafic de messagerie électronique
 - Taille du message électronique accepté
 - Résumé des menaces
 - Principaux destinataires de spam
 - Principaux destinataires de virus

**Remarque**

Pour plus d'informations sur Hosted Email Security et Worry-Free Business Security (tous), consultez la documentation relative à ces produits à l'adresse : <http://docs.trendmicro.com/fr-fr/home.aspx>.

Remote Manager offre une vue structurée des réseaux client et permet aux revendeurs de générer des commandes et de gérer les aspects critiques suivants de la sécurité réseau :

- Mises à jour des composants et mises à jour du serveur géré.

- Évaluation des failles
- Damage Cleanup
- Réponse automatique aux épidémies
- Paramètres de pare-feu et de scan en temps réel
- Scans manuels

Remote Manager prend également en charge des fonctions de rapport complètes et permet aux revendeurs d'abonner des individus aux rapports générés automatiquement.

Fonctions

Trend Micro Remote Manager offre les fonctions suivantes.

Plate-forme intégrée

Remote Manager fonctionne en parallèle avec Trend Micro™ Licensing Management Platform, mais avec une interface plus fiable. Vous pouvez effectuer les actions suivantes à partir du portail Remote Manager :

- Créer de nouveaux comptes
- Renouveler les licences pour les comptes individuels
- Ajouter davantage de sièges

Par ailleurs, Remote Manager surveille et gère de multiples réseaux protégés à partir d'une seule console en communiquant avec un agent Remote Manager exécuté sur les serveurs gérés. De plus, Remote Manager permet de surveiller les événements d'après des indicateurs de sécurité clés.

Widgets Tableau de bord

Personnalisez les widgets de la page du tableau de bord. Ces widgets peuvent vous permettre de savoir si vous devez renouveler des licences, ajouter davantage de sièges affectés ou même de savoir qui sont les clients les plus exposés aux menaces.

Paramètres personnalisables des nouveaux comptes

Lors de la création de comptes, vous pouvez personnaliser les paramètres de base par défaut que les nouveaux comptes utiliseront par défaut ou sélectionner les paramètres des modèles que vous avez configurés et enregistrés.

État des menaces

L'écran Événements Remote Manager indique l'état des aspects suivants de la sécurité réseau :

- Worry-Free Business Security Standard et Advanced
 - Défense anti-épidémies
 - Antivirus
 - Anti-spyware
 - Réputation de sites Web
 - Surveillance des comportements
 - Virus de réseau
 - Anti-spam
 - Filtrage de URL (versions 6.x et ultérieures uniquement)
 - Contrôle des dispositifs (versions 7.x, 8.x et 9.0 uniquement)
- Worry-Free Business Security Services
 - Défense anti-épidémies

- Antivirus
- Anti-spyware
- Réputation de sites Web
- Surveillance des comportements
- Virus de réseau
- Filtrage des URL
- Hosted Email Security
 - Ensemble du trafic de messagerie électronique
 - Taille du message électronique accepté
 - Résumé des menaces
 - Principaux destinataires de spam
 - Principaux destinataires de virus

Remote Manager fournit des détails sur ces aspects, notamment des données statistiques telles que le nombre d'ordinateurs infectés et d'incidents liés à des virus/programmes malveillants. Les administrateurs revendeurs peuvent également vérifier des informations détaillées, notamment les noms des ordinateurs concernés ou les menaces.

État du système

Les administrateurs revendeurs peuvent vérifier les aspects système suivants de la sécurité réseau via l'écran Événements Remote Manager :

- Smart Protection Services
- Mises à jour des composants
- Espace disque insuffisant
- Appareil/agent hors ligne
- Appareil/agent hors ligne (dernières 24 heures)

- Défaillance de l'appareil
- Défaillance de l'appareil (dernières 24 heures)

État de la licence

Les administrateurs des revendeurs peuvent afficher les détails suivants concernant les licences :

- Total des licences achetées
- Nombre de licences utilisées
- Licences arrivées à expiration, y compris la date d'expiration
- Licences arrivant à expiration, y compris le nombre jours avant l'expiration

Gestion du réseau

Remote Manager offre une vue structurée des réseaux gérés et permet aux administrateurs revendeurs de générer des commandes et de gérer les aspects critiques suivants de la sécurité du réseau :

- Mises à jour des composants et mises à jour du serveur géré.
- Évaluation des failles
- Réponse automatique aux épidémies
- Damage Cleanup
- Paramètres de pare-feu et de scan en temps réel
- Scans manuels

Génération de rapports

Outre les notifications liées aux événements de sécurité, Remote Manager peut automatiquement générer et envoyer des rapports, à intervalles réguliers. Vous pouvez

créer des rapports en fonction du client, du produit, de la fréquence et du contenu, et les enregistrer sous différents formats.

Intégration avec les outils tiers

Activez la surveillance des journaux à l'aide des outils tiers, y compris Autotask™, Kaseya™, ou ConnectWise™, pour standardiser les tâches et les processus que vous surveillez.

Envoi de commentaires

Trend Micro a pour ambition d'offrir aux utilisateurs la meilleure plate-forme qui soit, mais également la plus utile. Cependant, Trend Micro ne sait pas quels services ou quelles fonctionnalités vous importent. À cette fin, Remote Manager aimerait que vous partagiez vos commentaires et suggestions en cliquant sur le bouton **Envoyer les commentaires**, accessible dans la bannière. Trend Micro pourra ainsi traiter vos suggestions et identifier les fonctionnalités qui seront utiles au plus grand nombre d'utilisateurs.

Produits pris en charge

- Worry-Free Business Security Standard
- Worry-Free Business Security Advanced
- Worry-Free Business Security Services
- Hosted Email Security
- Cloud Edge



Remarque

Worry-Free Business Security Standard et Advanced, et Worry-Free Business Security Services sont collectivement appelés Worry-Free Business Security (tous), le cas échéant.

- Les outils tiers

- Autotask™
- Kaseya™
- ConnectWise™

Worry-Free Business Security Suite

Trend Micro™ Worry-Free Business Security Standard, Worry-Free Business Security Advanced et Worry-Free Business Security Services représentent une solution complète, à gestion centralisée, pour les petites et moyennes entreprises.

Worry-Free Business Security Standard fournit un antivirus côté client et une protection de pare-feu pour les postes de travail et les serveurs. Worry-Free Business Security Advanced inclut les mêmes fonctions que Worry-Free Business Security Standard, mais fournit aussi une solution anti-spam et anti-menaces de messagerie pour les serveurs de messagerie exécutant Microsoft™ Exchange Server. Worry-Free Business Security Standard et Advanced incluent tous deux un composant côté serveur pour la surveillance et la gestion de la protection client, à partir d'un emplacement central.

Worry-Free Business Security Services offre la plupart des avantages proposés par Worry-Free Business Security Standard. En outre, étant donné que Worry-Free Business Security Services est un service hébergé, vous pouvez gérer la sécurité de façon centralisée depuis n'importe où sans devoir ajouter, installer, configurer ou gérer un serveur. Les experts de la sécurité de Trend Micro hébergent ce service et le mettent à jour en permanence.



Remarque

Pour plus d'informations sur Worry-Free Business Security Standard et Advanced et Worry-Free Business Security Services, consultez la documentation à l'adresse :

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

Trend Micro Remote Manager surveille et gère les réseaux protégés par Worry-Free Business Security Standard et Advanced en communiquant avec un agent exécuté sur les serveurs Worry-Free Business Security Standard et Advanced situé dans les centres de données Trend Micro.

Hosted Email Security

Trend Micro™ Hosted Email Security bloque les spams, les virus, les attaques de phishing et autres menaces de messagerie avant qu'elles n'atteignent votre réseau. Comme il s'agit d'une solution hébergée, elle ne nécessite aucune installation ni maintenance matérielle et logicielle, ce qui vous permet de soulager l'équipe informatique et d'améliorer la productivité de l'utilisateur, la qualité de la bande passante, la capacité de stockage du serveur de messagerie, sans oublier les performances du processeur.

De plus, l'équipe internationale d'experts Trend Micro s'occupe des correctifs de type hotfix, des patches, des mises à jour et réglages d'applications pour optimiser en permanence les performances de la solution.



Remarque

Pour plus d'informations sur Hosted Email Security, consultez la documentation à l'adresse :

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

Trend Micro Remote Manager surveille et gère les réseaux protégés par Hosted Email Security en communiquant avec le serveur Hosted Email Security situé dans les centres de données Trend Micro.

Les outils tiers

Trend Micro Remote Manager s'intègre à des outils tiers afin d'assurer un environnement réseau plus sécurisé. Ces outils sont les suivants :

Autotask™

Remote Manager peut envoyer les notifications d'événements suivantes au système Autotask :

- Worry-Free Business Security Standard et Advanced
 - Agent anormal
 - Défense anti-épidémies

- Antivirus
- Anti-spyware
- Réputation de sites Web
- Surveillance des comportements
- Virus de réseau
- Anti-spam
- Serveurs gérés obsolètes
- Événements système exceptionnels
- Expiration de la licence
- Filtrage des URL
- Contrôle des périphériques
- Arrêt du serveur Worry-Free Business Security Standard et Advanced
- Arrêt du serveur Exchange
- Worry-Free Business Security Services
 - Agent anormal
 - Défense anti-épidémies
 - Antivirus
 - Anti-spyware
 - Réputation de sites Web
 - Surveillance des comportements
 - Virus de réseau
 - Serveurs gérés obsolètes
 - Événements système exceptionnels
 - Expiration de la licence

- Filtrage des URL
- Arrêt du serveur Exchange

Ces événements sont envoyés à Autotask sous la forme de messages électroniques transformés en ticket Autotask. Pour que cela soit possible, vous devez ajouter les destinataires des notifications à la console Web Remote Manager et plusieurs champs dans le système de tickets d'Autotask. Pour plus d'informations, consultez [Intégration d'Autotask™ à la page 4-15](#).

Kaseya™

Remote Manager et Worry-Free Business Security Services peuvent envoyer des notifications d'événements au système Kaseya. Les événements suivants peuvent être envoyés à Kaseya :

- Worry-Free Business Security Standard et Advanced
 - Agent anormal
 - Défense anti-épidémies
 - Antivirus
 - Anti-spyware
 - Réputation de sites Web
 - Surveillance des comportements
 - Virus de réseau
 - Anti-spam
 - Serveurs gérés obsolètes
 - Événements système exceptionnels
 - Expiration de la licence
 - Filtrage des URL
 - Contrôle des périphériques

- Arrêt du serveur Client Server Messaging/Worry-Free Business Security Standard et Advanced
- Arrêt du serveur Exchange
- Worry-Free Business Security Services
 - Agent anormal
 - Défense anti-épidémies
 - Antivirus
 - Anti-spyware
 - Réputation de sites Web
 - Surveillance des comportements
 - Virus de réseau
 - Serveurs gérés obsolètes
 - Événements système exceptionnels
 - Expiration de la licence
 - Filtrage des URL
 - Arrêt du serveur Exchange

Ces événements sont envoyés à Kaseya sous la forme de messages électroniques transformés en ticket Kaseya. Pour que cela soit possible, les destinataires des notifications doivent être ajoutés à la console Web Remote Manager et plusieurs champs doivent être créés dans le système de tickets de Kaseya. Pour plus d'informations, consultez *Intégration de Kaseya™ à la page 4-23*.

ConnectWise™

Remote Manager et Worry-Free Business Security Services peuvent envoyer des notifications d'événements au système ConnectWise. Les événements suivants peuvent être envoyés à ConnectWise :

- Worry-Free Business Security Standard et Advanced

- Agent anormal
- Défense anti-épidémies
- Antivirus
- Anti-spyware
- Réputation de sites Web
- Surveillance des comportements
- Virus de réseau
- Anti-spam
- Serveurs gérés obsolètes
- Événements système exceptionnels
- Expiration de la licence
- Filtrage des URL
- Contrôle des périphériques
- Arrêt du serveur Client Server Messaging/Worry-Free Business Security Standard et Advanced
- Arrêt du serveur Exchange
- Worry-Free Business Security Services
 - Agent anormal
 - Défense anti-épidémies
 - Antivirus
 - Anti-spyware
 - Réputation de sites Web
 - Surveillance des comportements
 - Virus de réseau

- Serveurs gérés obsolètes
- Événements système exceptionnels
- Expiration de la licence
- Filtrage des URL
- Arrêt du serveur Exchange

Ces événements sont envoyés à ConnectWise sous la forme de messages électroniques enregistrés dans ConnectWise. Pour que cela soit possible, les destinataires des notifications doivent être ajoutés à la console Web Remote Manager et plusieurs champs doivent être créés dans le système de tickets de ConnectWise. Pour plus d'informations, consultez *Intégration de ConnectWise™ à la page 4-30*.

Nouveautés

Trend Micro™ Remote Manager inclut les nouvelles fonctions et améliorations suivantes :

FONCTION/AMÉLIORATION	DÉTAILS
Notification pouvant donner lieu à une action	<p>Cliquez sur les liens des widgets ou de la notification électronique pour afficher les licences nécessitant une action immédiatement ou prochainement et prendre les mesures nécessaires.</p> <p>Vous pouvez également ouvrir la console Web de certains produits en cliquant sur les événements. Reportez-vous à Authentification unique.</p>
Personnalisez vos rapports	<p>Les partenaires et les clients ont des besoins différents en matière de rapports. Vous pouvez utiliser le nouveau contenu et les nouveaux modèles pour vous assurer qu'ils obtiennent les informations adéquates.</p>

FONCTION/AMÉLIORATION	DÉTAILS
<p>Configurez de nouveaux clients en 3 étapes simples</p> <hr/> <p> Remarque Cette fonction est destinée uniquement aux utilisateurs de Trend Micro Licensing Management Platform. Contactez votre fournisseur de services gérés ou votre représentant Trend Micro pour plus d'informations.</p>	<p>Configurez de nouvelles stratégies par défaut et déployez-les sur les nouveaux clients en trois (3) étapes. Une fois le déploiement terminé, ces clients bénéficieront du même niveau de protection et de surveillance fourni par Trend Micro Remote Manager.</p>
<p>Personnaliser les modèles de paramètres par défaut</p> <hr/> <p> Remarque Cette fonction est destinée uniquement aux utilisateurs de Trend Micro Licensing Management Platform. Contactez votre fournisseur de services gérés ou votre représentant Trend Micro pour plus d'informations.</p>	<p>Préconfigurez différents modèles de paramètres Worry-Free Business Security Services afin de disposer d'une variété de modèles de service pour vos clients.</p>
<p>Authentification unique</p>	<p>Cliquez sur le lien Ouvrir la console à la page Client pour ouvrir la console Web des services suivants :</p> <ul style="list-style-type: none"> • Worry-Free Business Security Services • Hosted Email Security • Cloud Edge

FONCTION/AMÉLIORATION	DÉTAILS
Aide supplémentaire	<p>Trend Micro Remote Manager vous permet d'accéder facilement à de la documentation à l'aide du bouton Aide, mais aussi à des didacticiels vidéo que vous pouvez regarder directement depuis la console.</p> <p>Trend Micro Remote Manager vous procure également un lien rapide vers le guide de bonnes pratiques Trend Micro Remote Manager.</p>

Infrastructure générale

Trend Micro Remote Manager est constitué de trois parties principales :

- Le revendeur
- Le centre de données de Trend Micro
- Le réseau client

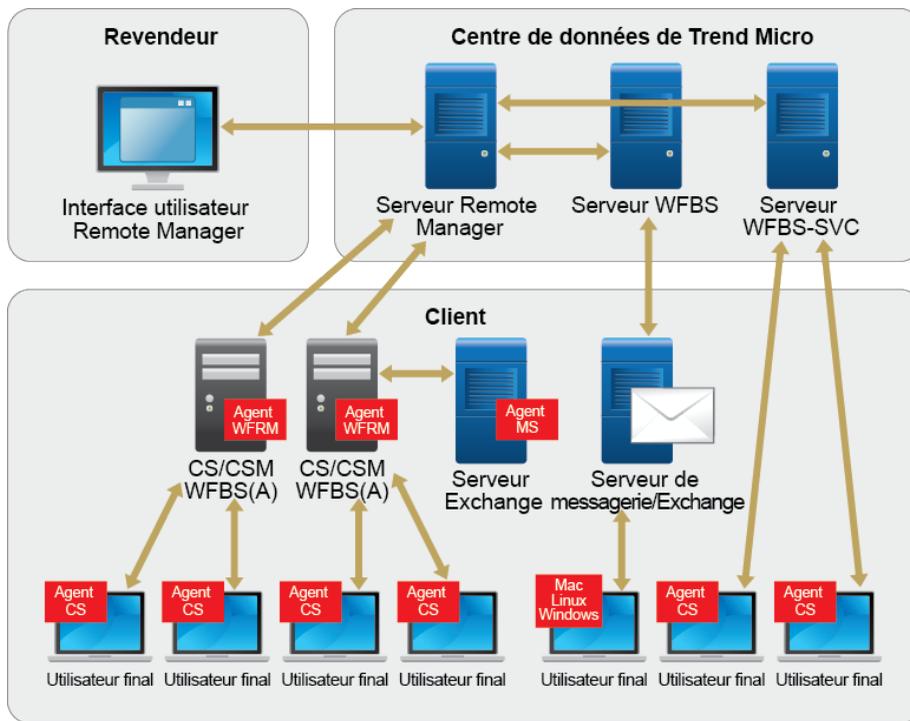


FIGURE 1-1. Architecture générale de Remote Manager

Le revendeur accède à un centre de données de Trend Micro (actuellement sur différents continents) par le biais de la console Web Remote Manager, via Internet. Le revendeur ne doit rien installer pour pouvoir utiliser le produit. Le revendeur doit ajouter et configurer chaque client sur la console Web Remote Manager avant de pouvoir gérer les comptes client.

Chaque serveur géré Worry-Free Business Security Standard et Advanced possède un agent Remote Manager qui permet de communiquer avec les serveurs Remote Manager. Comme Worry-Free Business Security Services est hébergé au centre de données Trend Micro, aucun agent ne doit être installé. En revanche, Worry-Free Business Security Services doit être enregistré sur la console Web Remote Manager pour chaque client.

L'agent Remote Manager, qui peut être installé depuis la console Web Remote Manager, est exécuté sur le serveur géré Worry-Free Business Security Standard et Advanced au sein du réseau client. L'agent Remote Manager envoie des informations au serveur Remote Manager, sur lequel vous pouvez accéder aux données à partir de votre console, 24 h/24 et 7 j/7, grâce à une connexion Internet.

Terminologie clé

Le fait de connaître les termes suivants pourra vous aider à travailler avec Remote Manager plus efficacement :

TERME	DÉFINITION
Agent	Installé sur les serveurs Worry-Free Business Security Standard et Advanced, ce programme permet à Remote Manager de surveiller et de gérer Worry-Free Business Security Standard et Advanced.
Évaluation	Vérifications régulières faites sur les données collectées auprès des réseaux client pour déterminer l'intégrité des réseaux surveillés. Ces vérifications utilisent des indicateurs clés appelés index d'évaluation.
Index d'évaluation	Représentent la base des évaluations de sécurité ; les administrateurs revendeurs peuvent personnaliser ces index individuellement pour contrôler les intervalles, les pages et les notifications d'évaluation.
Client Security Agent (CSA)	Agent qui communique avec le serveur Worry-Free Business Security. L'agent CSA envoie des informations en temps réel sur l'état des événements. Les agents rapportent les événements tels que la détection d'une menace, leur démarrage ou leur arrêt, le lancement d'un scan et la réalisation d'une mise à jour. L'agent CSA met à votre disposition trois méthodes de scan : le scan en temps réel, le scan programmé et le scan manuel. Vous pouvez configurer les paramètres de scan sur les agents à partir de la console Web.
Tableau de bord	Le tableau de bord dans Remote Manager est l'écran principal (onglet Accueil) qui affiche la console Web et les widgets.

TERME	DÉFINITION
Détection	Découverte d'une menace ; une détection ne représente pas une infection système, mais indique simplement qu'un programme malveillant a atteint l'ordinateur. La détection de la même menace sur différents ordinateurs peut représenter une épidémie.
Événement	Occurrence d'une condition dans un domaine surveillé.
Identificateur global unique (GUID) ou clé d'enregistrement	Numéro de référence unique utilisé comme identifiant dans un logiciel informatique.
Infection	La condition qui permet à une menace d'exécuter ses charges sur un ordinateur ;Remote Manager considère qu'une infection est survenue lorsque le scan antivirus détecte un virus/ programme malveillant et ne peut pas le nettoyer, le supprimer ou mettre la menace en quarantaine. Une infection par spyware/ grayware se produit lorsque l'ordinateur ne peut pas être complètement nettoyé sans être redémarré.
Messaging Security Agent (MSA)	Agent situé sur les serveurs Microsoft Exchange et communiquant avec les serveurs Client Server Messaging et Worry-Free Business Security Advanced. Cet agent assure une protection contre les virus/programmes malveillants, chevaux de Troie, vers et autres menaces de messagerie. Il offre également des fonctions de blocage de spams et de pièces jointes, ainsi que des filtres de contenu.
Revendeur	Terme générique faisant référence aux organisations qui fournissent directement des services de surveillance et de gestion de la sécurité aux clients de Remote Manager.
Administrateurs revendeurs	Administrateurs du côté revendeur qui effectuent des tâches s'apparentant à un service à l'aide de Remote Manager.
Centre de données de Trend Micro	Centre de surveillance et de gestion Trend Micro hébergeant les serveurs Remote Manager (et Hosted Email Security) et fournissant une assistance aux administrateurs revendeurs.
Security Server	Ordinateur serveur Worry-Free Business Security Standard et Advanced.

TERME	DÉFINITION
Alerte virale	État de vigilance déclaré par TrendLabs SM pour préparer les réseaux client à une épidémie virale ; TrendLabs alerte différents produits Trend Micro et fournit des solutions préventives que les administrateurs informatiques peuvent mettre en œuvre pour servir de première ligne de défense en attendant qu'une signature soit disponible.
Épidémie virale	Propagation rapide d'une menace virale sur différents ordinateurs et réseaux ; selon l'étendue de la menace, une épidémie peut être interne, régionale ou mondiale.

Chapitre 2

Démarrage

Cette section contient les rubriques suivantes :

- *Configuration requise du navigateur à la page 2-2*
- *Accès à la plate-forme à la page 2-3*
- *Coordination avec le client à la page 2-4*

Configuration requise du navigateur

- Connexion Internet
- Informations du compte Remote Manager de Trend Micro
- Navigateurs pris en charge :
 - Version la plus récente de Firefox™ (recommandé)
 - Version la plus récente de Google™ Chrome™ (recommandé)
 - Internet Explorer™ 9.0

Ajout de l'URL de la console Web Trend Micro Remote Manager aux sites de confiance

Ajoutez l'URL de la console Web Remote Manager à votre liste de sites de confiance dans Internet Explorer pour être certain de pouvoir accéder à tous les écrans et à toutes les fonctionnalités de la console de façon appropriée.

Procédure

1. Ouvrez Internet Explorer.
 2. Cliquez sur **Outils > Options Internet > Sécurité (onglet)**.
 3. Sélectionnez la zone **Sites de confiance**.
 4. Cliquez sur **Sites**.
 5. Dans **Ajouter ce site Web à la zone**, saisissez l'URL de la console.
 6. Cliquez sur **Ajouter**.
 7. Cliquez sur **OK**.
-

Utilisation d'Internet Explorer 9 pour obtenir le certificat SSL

Pour utiliser l'agent, ajoutez le certificat SSL de Trend Micro au navigateur sur le serveur géré.

Procédure

1. Ouvrez Internet Explorer et accédez au site Trend Micro Remote Manager en fonction de votre région.
 2. Double-cliquez sur l'icône de cadenas à la droite de la barre d'adresses.
Le menu d'identification du site Web s'ouvre.
 3. Cliquez sur **Afficher les certificats**.
La fenêtre **Certificat** s'ouvre, affichant le certificat émis pour *.trendmicro.com.
 4. Accédez à **Chemin d'accès de certification (onglet) > Geotrust ou Equifax Secure Certificate Authority > Afficher le certificat**.
 5. Lorsque la fenêtre **Certificat** affichant l'autorité des informations de sécurité s'ouvre, cliquez sur l'onglet **Détails**.
 6. Accédez à **Copier dans un fichier > Suivant**, puis sélectionnez **Binaire codé DER X.509 (.cer)**.
 7. Cliquez sur **Suivant**, puis saisissez le chemin et le nom de fichier de certificat.
Par exemple, wfrmcert.cer.
 8. Cliquez sur **Suivant > Terminer**.
-

Accès à la plate-forme

Tout le monde, quels que soient le type et les autorisations du compte, se connecte à partir de la même page. Saisissez simplement vos informations d'identification de

connexion et cliquez sur **Connexion**. L'URL de connexion, ainsi que vos informations d'identification de connexion venant de l'utilisateur possédant le compte parent devraient apparaître.

Les utilisateurs ne pourront pas voir les paramètres et options qu'ils souhaitent s'ils ne disposent pas des privilèges adéquats pour les voir.

Coordination avec le client

La surveillance et la gestion du réseau de votre client au moyen de Trend Micro Remote Manager apporte de nombreux avantages à ce dernier. Toutefois, tout comme d'autres activités de gestion à distance, les actions effectuées sur la console peuvent considérablement affecter le réseau géré.

Avant de commencer à fournir des services, assurez-vous que vous disposez du consentement de votre client pour effectuer les activités suivantes de surveillance et de gestion :

- Consulter la liste des ordinateurs de son réseau
- Renouveler ou ajouter des sièges à vos licences
- Consulter les informations de sécurité suivantes :
 - Détections de virus/programmes malveillants, spyware/grayware et virus de réseau
 - Noms et nombre d'ordinateurs infectés
 - Noms des fichiers infectés
 - Adresses électroniques ayant reçu les fichiers infectés
 - Informations de patch pour les failles connues
 - Informations de licence et de système sur Worry-Free Business Security (tous) et Hosted Email Security
- Envoyer des notifications aux personnes de l'organisation cliente
- Exécuter les actions suivantes :

- Déploiement de composants de sécurité
- Démarrer des scans d'évaluation des failles
- Démarrer Damage Cleanup Services
- Démarrage ou arrêt d'un scan manuel
- Mettre à jour le serveur Worry-Free Business Security Standard et Advanced
- Démarrage ou arrêt de la défense anti-épidémies
- Configurer les paramètres suivants :
 - Déploiement automatique de la défense anti-épidémies
 - Paramètres de scan en temps réel
 - Paramètres du pare-feu
 - Détection d'emplacement
 - Surveillance des comportements
 - Réputation de sites Web
 - Filtrage des URL
 - Contrôle des dispositifs (Worry-Free Business Security 7.0 et versions ultérieures)

Chapitre 3

Présentation de la console Web

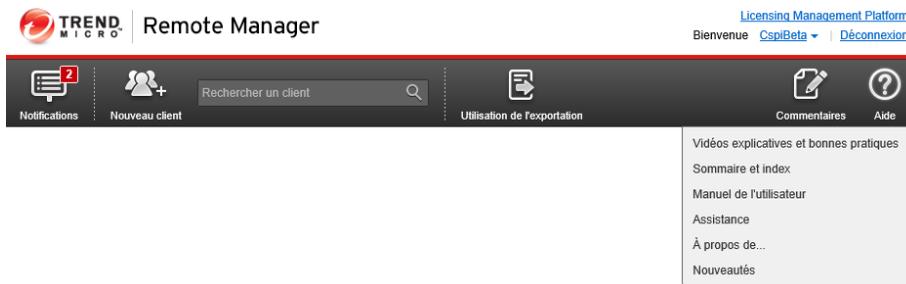
La console Web est le point central permettant de surveiller et gérer les produits et les clients.

Cette section contient les rubriques suivantes :

- *La bannière de la console Web à la page 3-2*
- *Menu principal à la page 3-3*
- *Explication du tableau de bord à la page 3-4*

La bannière de la console Web

La zone de la bannière fournit les options suivantes :

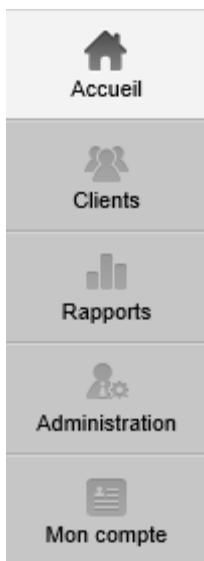


- **<nom de compte>** : affiche le compte connecté actuellement.
- **Déconnexion** : vous déconnecte de la console Web.
- **Licensing Management Platform** : ce lien n'apparaîtra que si vous avez intégré cette console par le biais du site License Management Platform.
- **Notifications** : indique combien d'événements nécessite une action.
- **Nouveau client** : cliquez sur ce bouton pour ajouter un nouveau client.
- **Barre de recherche** : spécifiez les informations client pour trouver rapidement un client spécifique..
- **Utilisation de l'exportation** : cliquez sur ce bouton pour exporter un document montrant l'utilisation de votre licence.
- **Commentaires** : cliquez sur ce bouton pour envoyer de précieux commentaires à Trend Micro concernant votre façon d'utiliser le produit, les fonctionnalités qu'on pourrait y ajouter ou comment rendre les fonctionnalités actuelles plus utiles.
- **Aide** :
 - **Vidéos explicatives et bonnes pratiques** : ouvre la page sur laquelle vous pouvez visionner des vidéos explicatives et fournit un lien vers le manuel des bonnes pratiques.

- **Sommaire et index** : ouvre l'aide en ligne Trend Micro Remote Manager.
- **Manuel de l'utilisateur** : télécharge et affiche le manuel de l'utilisateur au format PDF.
- **Assistance** : affiche la page Web d'assistance de Trend Micro sur laquelle vous pouvez poser des questions et trouver des réponses aux questions les plus fréquentes concernant les produits Trend Micro.
- **À propos de...** : fournit un aperçu du produit et des instructions pour vérifier les détails de la version du composant.
- **Nouveautés** : redirige vers la page présentant les nouvelles fonctionnalités.

Menu principal

Le menu principal affiche les boutons que vous pouvez utiliser pour naviguer vers les différentes fonctionnalités et options. Vous pouvez utiliser la barre de navigation pour cliquer sur les options suivantes :



- **Accueil** : cette option vous redirigera vers la page d'accueil, qui présente le tableau de bord et les widgets sur le panneau de droite.
- **Clients** : cette option présente la liste des clients, à laquelle vous pouvez ajouter des clients ou effectuer des changements dans les paramètres client ou les configurations client..
- **Rapports** : cette option affiche les rapports et les nouveaux rapports pouvant être ajoutés.
- **Administration** : cette page vous permet de modifier les paramètres de notification ou de la console Web ou les modèles de paramètres par défaut, ainsi que de configurer l'intégration à des outils tiers.
- **Mon compte** : cette option s'affichera uniquement si vous n'avez pas intégré votre compte à Licensing Management Platform.

Explication du tableau de bord

Cette section contient des informations sur les onglets, les widgets et le tableau de bord.

Écrans du tableau de bord État

Le tableau de bord est l'écran central permettant de vérifier l'état des réseaux surveillés. Le tableau de bord répertorie uniquement les produits présentant un état anormal. Par exemple, si la licence Worry-Free Business Security Services d'un client arrive à expiration ou si un client a trop de menaces, ce client est répertorié dans ce tableau.

Pour accéder au tableau de bord, ouvrez un navigateur compatible et connectez-vous au site Trend Micro Remote Manager de votre région.

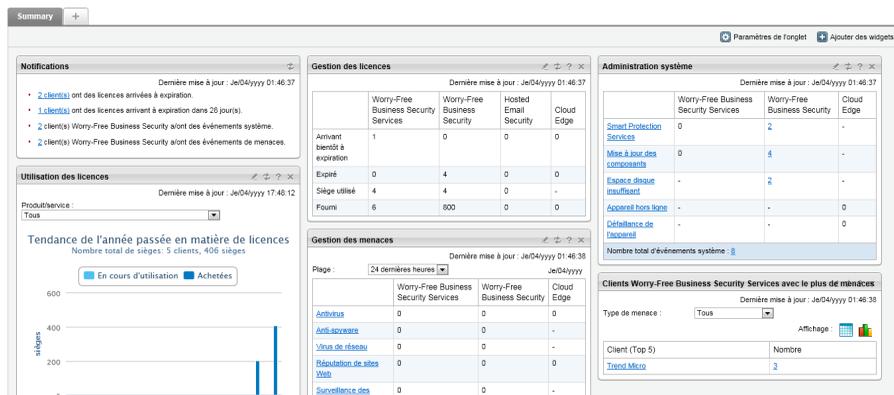


FIGURE 3-1. Onglet État des menaces du tableau de bord

La plupart des éléments du tableau de bord sont liés pour vous aider à résoudre un problème. Cliquez sur un élément (graphique, lien, numéro) pour résoudre le problème. Pour plus d'informations sur ce que vous pouvez faire, voir [Informations sur le produit/service à la page 3-18](#).

Onglets et widgets

Les onglets fournissent un recueil pour les widgets. Chaque onglet de l'écran **Résumé** peut contenir jusqu'à 20 widgets. L'écran **Résumé** prend en charge jusqu'à 30 onglets.

Les widgets sont des composants essentiels du tableau de bord. Les widgets apportent des informations spécifiques concernant différents événements de menaces ou de licence. Certains widgets vous permettent d'exécuter certaines tâches.

Les informations affichées par un widget figurent dans :

- le serveur et les clients Worry-Free Business Security ;
- le serveur Worry-Free Business Security Services ;
- les services Hosted Email Security ;

- les serveurs et les clients Cloud Edge.

Onglet Tâches

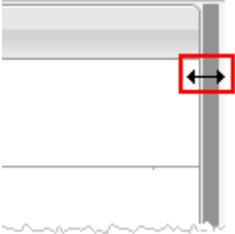
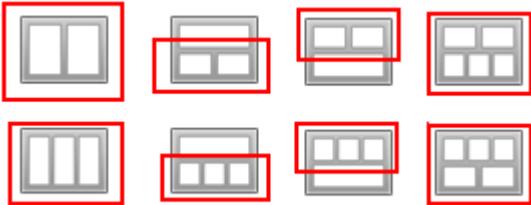
Le tableau suivant répertorie toutes les tâches relatives à cet onglet :

TÂCHE	ÉTAPES
Ajouter un onglet	Cliquez sur l'icône plus (+) en haut de l'écran Résumé . La fenêtre Nouvel onglet apparaît.
Modifier les paramètres de l'onglet	Cliquez sur Paramètres de l'onglet . Une fenêtre similaire à la fenêtre Nouvel onglet apparaît, dans laquelle vous pouvez modifier les paramètres.
Déplacer l'onglet	Utilisez la fonction glisser-déplacer pour modifier la position d'un onglet.
Supprimer un onglet	Cliquez sur l'icône de suppression (X) qui se trouve à côté du titre de l'onglet. La suppression d'un onglet implique également la suppression de tous les widgets se trouvant dans cet onglet.

Tâches de widget

Le tableau suivant répertorie les tâches relatives au widget :

TÂCHE	ÉTAPES
Ajouter un widget	Ouvrez un onglet puis cliquez sur Ajouter des widgets dans l'angle supérieur droit de l'onglet. L'écran Ajouter des widgets s'affiche.
Actualiser les données de widget	Cliquez sur l'icône Actualiser (↻).
Afficher l'aide	Cliquez sur Aide (?).

TÂCHE	ÉTAPES
Supprimer un widget	Cliquez sur Fermer le widget (X). Cette action supprime le widget de l'onglet qui le contient, mais pas des autres onglets qui le contiennent ou de la liste de widgets de l'écran Ajouter des widgets .
Déplacer un widget	Utilisez la fonction glisser-déplacer pour déplacer un widget vers emplacement différent dans l'onglet.
Redimensionner un widget	<p>Pour redimensionner un widget, positionnez le curseur sur le bord droit du widget. Lorsqu'une ligne pleine verticale et une flèche s'affichent (comme illustré sur l'image suivante), maintenez puis déplacez le curseur vers la gauche ou vers la droite.</p>  <p>Seuls les widgets des onglets multicolonne peuvent être redimensionnés. Ces onglets ont l'une des mises en page suivantes et les sections en surbrillance contiennent des widgets qui peuvent être redimensionnés.</p> 

Widgets disponibles

Le tableau de bord présente les widgets suivants.

Widget Notifications

Indique les événements nécessitant une action. Il peut s'agir d'événements de menaces ou de licence.



Remarque

Il s'agit d'un widget permanent qui ne peut être ni ajouté, ni supprimé.

Widget Clients requérant la plus grande attention

Indique le nombre de clients le plus récent avec le plus grand nombre d'événements et requérant une action ou une réponse immédiate. Les données s'affichent dans un tableau et dans un graphique circulaire. Vous pouvez passer du tableau au graphique circulaire en cliquant sur les icônes d'affichage ( .

Clients requérant la plus grande attention			
Dernière mise à jour : 15/avr./2014 04:35:15			
Affichage :  			
Client (Top 5)	Action requise	Avertissement	Total
 Trend Micro	9	17	26
 Trend Micro RM	4	10	14

- Si le nombre de clients pour un état particulier est 1 ou plus, vous pouvez cliquer sur le nombre pour afficher les événements dans l'arborescence des produits.
- Cliquez sur le nom du client pour afficher tous les événements pour ce client ou développez le nom du client pour afficher les événements de certaines catégories.

- Le nombre d'événements sous **Action requise** représente des événements qui doivent être traités dès que possible.
- Le nombre d'événements sous **Avertissement** représente des événements qui ne sont pas aussi urgents que les événements dans Action requise, mais qui doivent également être traités assez rapidement.

Widget Gestion des menaces

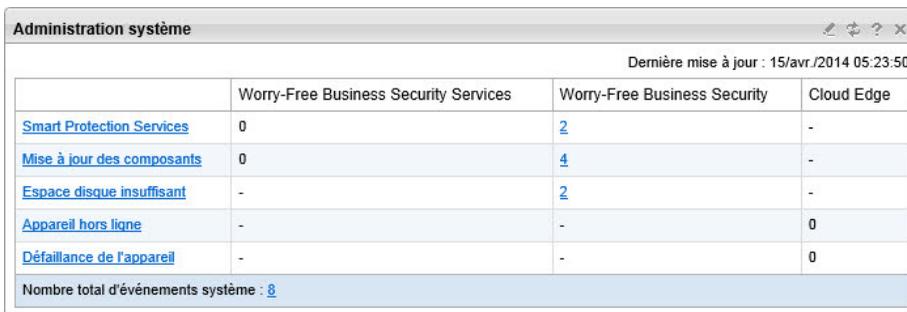
Indique le nombre d'événements de menaces pour tous les produits enregistrés.

Gestion des menaces			
Plage :		Dernière mise à jour : 15/avr./2014 05:23:50	
24 dernières heures		De 08/avr./2014 à 15/avr./2014	
	Worry-Free Business Security Services	Worry-Free Business Security	Cloud Edge
Antivirus	0	0	0
Anti-spyware	0	0	-
Virus de réseau	0	0	-
Réputation de sites Web	0	97	0
Surveillance des comportements	0	0	-
Filtrage des URL	3	408	-
Contrôle des périphériques	0	0	-
Botnet	-	-	0
IPS	-	-	0
Nombre total d'événements de menaces : 508			

- Vous pouvez modifier l'intervalle de temps pour les données affichées en sélectionnant :
 - 24 dernières heures (par défaut)
 - 7 derniers jours
 - 30 derniers jours
- Si le nombre d'événements pour une catégorie particulière est 1 ou plus, vous pouvez cliquer sur le nombre pour afficher les journaux des événements.

Widget Administration du système

Indique le nombre actuel d'événements système pour les produits enregistrés. Vous pouvez l'utiliser pour déterminer les problèmes de matériel ou les événements pour le serveur ou l'agent.



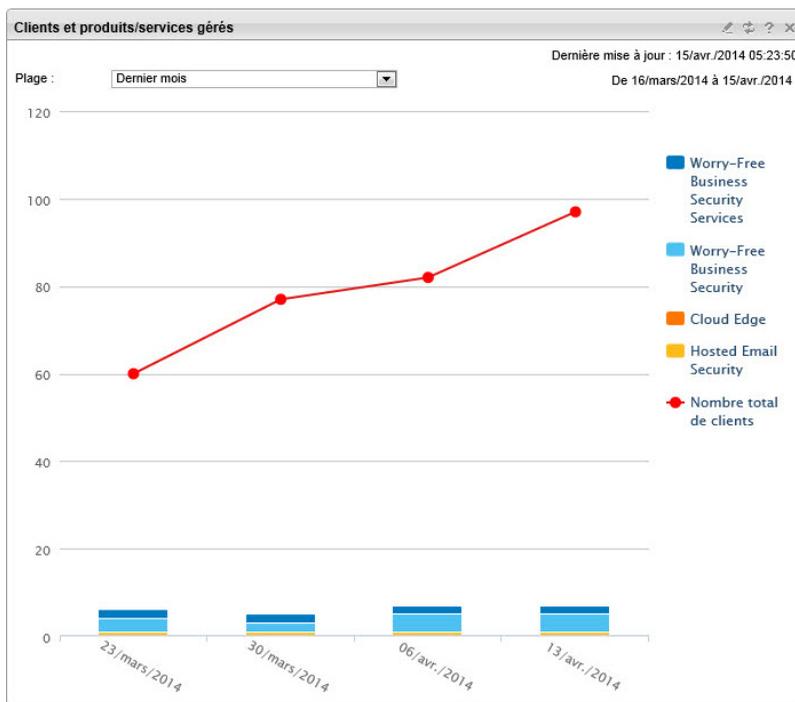
The screenshot shows a window titled 'Administration système' with a table of system events. The table has four columns: an empty column for the event name, and three columns for 'Worry-Free Business Security Services', 'Worry-Free Business Security', and 'Cloud Edge'. The rows list events like 'Smart Protection Services', 'Mise à jour des composants', 'Espace disque insuffisant', 'Appareil hors ligne', and 'Défaillance de l'appareil'. A footer row shows the total number of system events as 8.

	Worry-Free Business Security Services	Worry-Free Business Security	Cloud Edge
Smart Protection Services	0	2	-
Mise à jour des composants	0	4	-
Espace disque insuffisant	-	2	-
Appareil hors ligne	-	-	0
Défaillance de l'appareil	-	-	0
Nombre total d'événements système : 8			

Si le nombre d'événements pour une catégorie particulière est 1 ou plus, vous pouvez cliquer sur le nombre pour afficher les journaux des événements.

Widget Clients et produits/services gérés

Indique le nombre de clients gérés pour chaque produit sur une période définie.

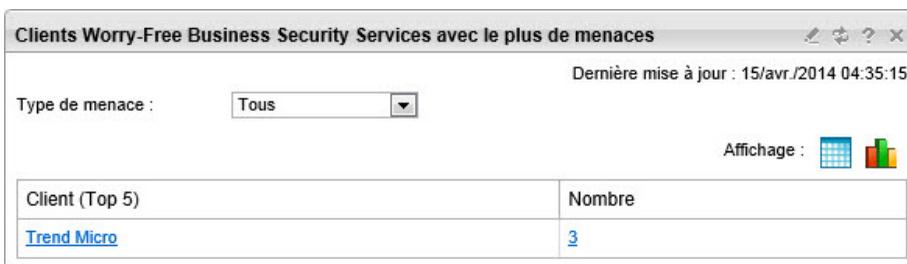


- Vous pouvez modifier l'intervalle de temps pour les données affichées en sélectionnant :
 - Dernier mois (par défaut)
 - 3 derniers mois
 - 6 derniers mois
 - An dernier
- Vous pouvez cliquer sur les noms des produits enregistrés à droite pour ajouter ou supprimer les données du graphique.

- Chaque graphique à barres représente une semaine ou un mois.
- Le graphique à barres indique le nombre total de produits/services.

Widget Clients Worry-Free Business Security Services avec le plus de menaces

Indique les clients Worry-Free Business Security Services avec le plus grand nombre d'événements de menaces. Les données s'affichent dans un tableau et dans un graphique circulaire. Vous pouvez passer du tableau au graphique circulaire en cliquant sur les icônes d'affichage ( ).



Client (Top 5)	Nombre
Trend Micro	3

- Vous pouvez modifier le type de menace pour les données affichées en sélectionnant :
 - Antivirus
 - Anti-spyware
 - Réputation de sites Web
 - Filtrage des URL
 - Surveillance des comportements
 - Virus de réseau
 - Contrôle des périphériques
- Cliquez sur le nom du client pour afficher les informations du client.

- Si le nombre de menaces est 1 ou plus, vous pouvez cliquer sur le nombre pour afficher les journaux des événements.

Widget Clients Cloud Edge avec le plus de menaces

Indique les clients Cloud Edge avec le plus grand nombre d'événements de menaces. Les données s'affichent dans un tableau et dans un graphique circulaire. Vous pouvez passer du tableau au graphique circulaire en cliquant sur les icônes d'affichage ( ).

Clients Cloud Edge avec le plus de menaces ✎ ↺ ? ✕

Dernière mise à jour : 29/04/2014 08:39:59

Plage : De 30/03/2014 à 29/04/2014

Type de menace :

Affichage :  

Client (Top 5)	Nombre de menaces
 [redacted]	31
abcdefghijklmnpqrstuvwxyzabcdefghijkl	31
 [redacted]	12
ce189	1
ce188	11

- Vous pouvez modifier l'intervalle de temps pour les données affichées en sélectionnant :
 - Dernière heure
 - 24 dernières heures (par défaut)
 - 7 derniers jours

- 30 derniers jours
- Vous pouvez modifier le type de menace pour les données affichées en sélectionnant :
 - Tous
 - Botnet
 - Système de prévention des intrusions
 - Réputation de sites Web
 - Virus
- Cliquez sur le nom du client pour afficher les informations du client.
- Cliquez sur le nombre de menaces pour ouvrir les informations relatives aux menaces depuis la console Cloud Edge.

Widget Appareils Cloud Edge avec le plus de menaces

Indique les appareils Cloud Edge avec le plus grand nombre d'événements de menaces.

Appareils Cloud Edge avec le plus de menaces ✎ ↺ ? ✕

Dernière mise à jour : 29/04/2014 08:39:59

Plage : De 30/03/2014 à 29/04/2014

Type de menace :

Appareil (Top 5)	Client	Nombre de menaces
abcdefghijklmnopqrstuvwxyzabcdefghijklmnop...	Client_1234567890	31
ce188	Client_123456789	11
ce189	Client_123456789	1

- Vous pouvez modifier l'intervalle de temps pour les données affichées en sélectionnant :
 - Dernière heure
 - 24 dernières heures (par défaut)
 - 7 derniers jours
 - 30 derniers jours
- Vous pouvez modifier le type de menace pour les données affichées en sélectionnant :
 - Tous
 - Botnet
 - Système de prévention des intrusions
 - Réputation de sites Web
 - Virus
- Cliquez sur le nom du client pour afficher les informations du client.
- Cliquez sur le nombre de menaces pour ouvrir les informations relatives aux menaces depuis la console Cloud Edge.

Widget Gestion des licences

Affiche l'état actuel des licences en cours d'utilisation par les clients.

Gestion des licences				
Dernière mise à jour : 15/avr./2014 05:23:49				
	Worry-Free Business Security Services	Worry-Free Business Security	Hosted Email Security	Cloud Edge
Arrivant bientôt à expiration	1	0	0	0
Expiré	0	4	0	0
Siège utilisé	4	4	0	-
Fourni	6	800	0	0

Indique les détails suivants concernant les licences pour les clients et les produits :

- **Arrivant bientôt à expiration** : IL s'agit du nombre de licences qui n'ont pas encore expiré mais qui expireront bientôt.
- **Expiré** : Il s'agit des licences qui ont déjà expiré.



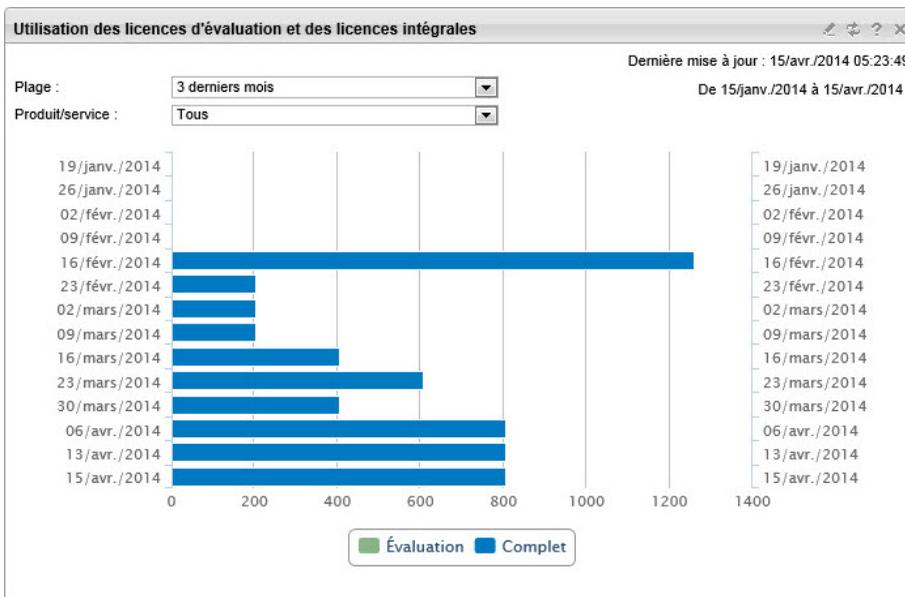
Remarque

Trend Micro conseille de renouveler ces licences dès que possible.

- **Sièges utilisés** : Il s'agit du nombre de sièges en cours d'utilisation.
- **Fourni** : Il s'agit du nombre de sièges que le client a fourni.

Widget Utilisation des licences d'évaluation et des licences intégrales

Indique combien de licences intégrales ou d'évaluation ont été utilisées pour les produits enregistrés.



Vous pouvez modifier l'intervalle de temps pour les données affichées en sélectionnant :

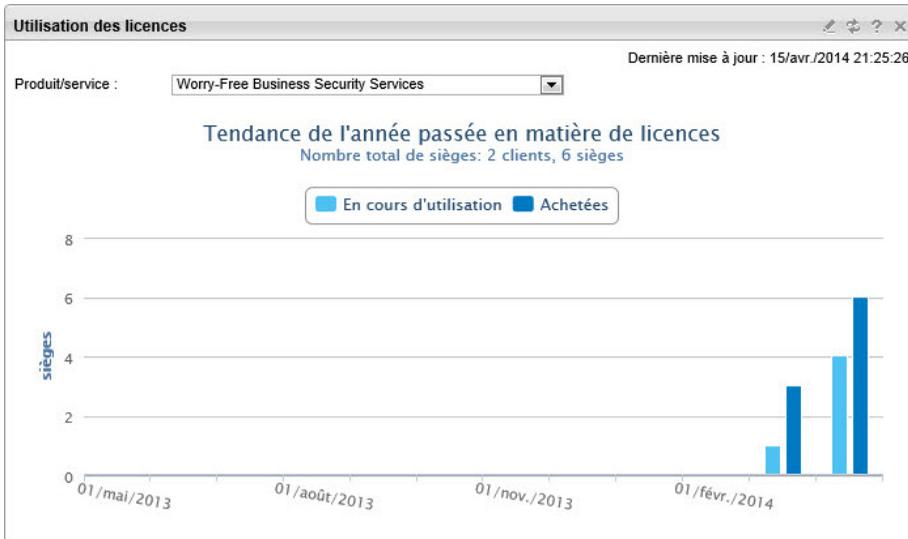
- Dernier mois (par défaut)
- 3 derniers mois
- 6 derniers mois
- An dernier

Vous pouvez modifier le produit/service en sélectionnant :

- Tous
- Hosted Email Security
- Worry-Free Business Security
- Worry-Free Business Security Services
- Cloud Edge

Widget Utilisation des licences

Affiche une analyse graphique des sièges qui ont été affectés et de ceux qui ont effectivement été achetés pour l'année. Cela permet de déterminer si vous devez augmenter ou réduire le nombre de sièges affectés.



Vous pouvez modifier le produit/service en sélectionnant :

- Tous
- Hosted Email Security
- Worry-Free Business Security
- Worry-Free Business Security Services

Informations sur le produit/service

Le tableau de bord répertorie uniquement les clients nécessitant une attention. Pour obtenir les détails d'un produit, y compris ceux qui ne sont pas répertoriés dans le

tableau de bord, accédez à l'onglet **Clients**, puis au produit souhaité dans l'arborescence des clients.

Cliquez sur **Clients > {client} > {produit}** pour afficher des informations supplémentaires.

**Remarque**

Les options affichées diffèrent pour chaque produit ou service.

- Worry-Free Business Security Services
 - **Groupes** : répertorie les groupes et les types configurés.
 - **Infos sur la licence** : affiche tous les détails de la licence.
 - **Terminaux** : répertorie le nom, l'adresse IP, l'état En ligne/Hors ligne et les détails du moteur de scan, du fichier de signatures et de la plate-forme.
 - **Paramètres de sécurité** : configurez les paramètres de sécurité de Worry-Free Business Security Services. Consultez la documentation sur [Trend Micro Worry-Free Business Security Services](#) pour plus d'informations.

**Remarque**

Pour apporter des modifications plus détaillées, accédez à la console Worry-Free Business Security Services.

- Worry-Free Business Security
 - **Groupes** : répertorie les différents groupes configurés sur le serveur. Vous pouvez demander le démarrage ou l'arrêt d'un scan dans cet onglet.
 - **Terminaux** : répertorie le nom, l'adresse IP, l'état En ligne/Hors ligne et les détails du moteur de scan, du fichier de signatures et de la plate-forme.
 - **Infos sur la licence** : affiche tous les détails de la licence.
 - **Paramètres de domaine** : configurez les paramètres de l'ensemble du domaine. Consultez la documentation sur [Trend Micro Worry-Free Business Security](#) pour plus d'informations.



Remarque

Il est impossible de configurer les paramètres de sécurité de groupes individuels dans cet onglet. Vous devrez accéder à la console Worry-Free Business Security pour apporter ces modifications.

- **Serveur géré** : affiche tous les détails du serveur. Vous pouvez demander la mise à jour du serveur et des agents dans cet onglet.
- **Agent TMRM** : Contient des informations générales sur l'agent Trend Micro Remote Manager, y compris la disponibilité, le GUID ou la clé d'enregistrement et l'adresse IP.
- **Paramètres de sécurité** : configurez les paramètres de sécurité d'un groupe spécifique (applicable uniquement à Worry-Free Business Security 6.0 et versions ultérieures). Consultez la documentation sur [Trend Micro Worry-Free Business Security](#) pour plus d'informations.
- Hosted Email Security
 - **État actuel** : affiche les dernières informations Hosted Email Security
 - **Paramètres de stratégie** : répertorie toutes les stratégies disponibles.
 - **Expéditeurs approuvés** : répertorie tous les expéditeurs approuvés.
 - **Infos sur la licence** : affiche tous les détails de la licence.



Remarque

Pour apporter des modifications plus détaillées, accédez à la console Hosted Email Security.

Affichage des produits gérés

Pour afficher les produits gérés, cliquez sur **Clients** > {nom du client} > **Produits (onglet)**. Cet onglet affiche une arborescence des produits gérés des clients sur le panneau de droite, ainsi que des informations détaillées, des paramètres et des possibilités de contrôle.

Pour plus d'informations sur Hosted Email Security et Worry-Free Business Security (tous), consultez la documentation relative à ces produits.

Clients

La page **Clients** donne une représentation des clients et de leurs produits que vous gérez. Par défaut, l'onglet affiche un tableau de tous les clients. Cliquez sur le nom de la société pour afficher une arborescence de ses produits sur le panneau de gauche et des informations détaillées, les paramètres et les possibilités de contrôle sur le panneau de droite.



Remarque

Pour plus d'informations sur Hosted Email Security et Worry-Free Business Security (tous), consultez la documentation relative à ces produits.

Pour afficher un produit dans la liste des clients, cliquez sur **Clients** > **{nom du client}** > **{produit}**. Vous pouvez effectuer les actions suivantes :

- Saisir le nom d'un client ou d'un compte
- Filtrer la liste affichée par client, produits, menaces, systèmes ou événements de licences



Remarque

Lorsque vous filtrez des événements, vous pouvez choisir un ou deux événements ou produits, ou tous simultanément.

- Parcourez tous les clients en utilisant les flèches de pagination.

D'autres tâches sont possibles :

- *Ajouter de nouveaux clients à la page 5-2*
- *Renouveler les licences arrivant à expiration ou expirées des clients à la page 7-2*
- *Exporter des rapports pour des clients spécifiques à la page 10-8*

Vous pouvez également ajouter ici de nouveaux clients et cliquer avec le bouton droit de la souris sur la plupart des nœuds de l'arborescence pour exécuter des commandes spécifiques.

Société	Personne à contacter	Téléphone	Produits	Événements système et de menaces	Événements de licence	Dernière transaction
Nouveau client						
Jaclyn T O	Jaclyn Ong	0800-092 pos le 000	WFBS-SVC	2 2	0 0	12/évr./2014 09:15:31
Theresa	Theresa Tu	0800-000 pos lw 092	WFBS-SVC.CE	2 0	1 0	13/mars/2014 15:16:21
WFBS_demo	WFBS demo	-	WFBS	0 0	1 0	-
PSA_noti	ktboy 123	-	WFBS-SVC	0 4	0 1	10/avr./2014 14:34:06
neil_lmo	neil beta	-	WFBS-SVC	0 0	0 0	15/nov./2013 14:40:59
abc	denise chen	-	WFBS-SVC	0 0	0 0	20/évr./2014 01:02:34
20140205_09000	ss ss	-	WFBS-SVC	0 0	0 0	05/évr./2014 16:43:34
cyn_test	cynthia lee	-	WFBS-SVC	0 0	0 0	27/janv./2014 11:52:18
utic-7	utic-7	-	WFBS-SVC	0 0	0 0	06/évr./2014 09:31:34
0109CE	0109 CE	-	CE	0 0	0 0	09/janv./2014 11:26:19

FIGURE 3-2. Liste de clients

Clients > XYZ

Produits Licences Profil de la société Contact Notification ConnectWise

Ajouter

Afficher par : Action requise et avertissement Menace et système Tous

- Tous les produits (3)
 - HES_HES
 - WFBS_abc
 - WFBS-SVC_abc

Action requise (0) Avertissement (0) Nombre total d'événements : 0

FIGURE 3-3. Arborescence clients

Arborescence des réseaux

Sur le côté gauche de l'onglet **Clients**, l'écran affiche une représentation en arborescence des réseaux de vos clients. Vous pouvez rechercher un client, afficher tous les produits simultanément, ou uniquement Worry-Free Business Security (tous), Hosted Email Security ou Cloud Edge dans la liste déroulante **Afficher par**, ou parcourir tous les clients à l'aide des flèches de pagination. Vous pouvez également ajouter un client et cliquer avec le bouton droit de la souris sur la plupart des nœuds de l'arborescence pour

exécuter des commandes spécifiques. Le tableau ci-dessous décrit les objets de l'arborescence.

TABEAU 3-1. Objets de l'arborescence des réseaux

ICÔNE	OBJET DE RÉSEAU	DESCRIPTION
	Produit/service	Ce produit/service n'est pas connecté à Remote Manager.
	Produit/service	Ce produit/service est connecté à Remote Manager.
	Groupe	Groupe de serveurs : ce groupe gère plusieurs agents Client Security Agent (CSA).
	Groupe	Groupes de postes de travail
	Serveur	Un ordinateur serveur : cet ordinateur exécute l'agent Client Security Agent (CSA).
	Serveur Exchange	Un ordinateur serveur Exchange : cet ordinateur exécute l'agent Messaging Security Agent (MSA).
	Poste de travail	Un ordinateur poste de travail : cet ordinateur exécute l'agent Client Security Agent (CSA)

Panneau de droite

Ce panneau de droite affiche les éléments suivants :

Produits

L'onglet **Produits** (Produits) sur le panneau de droite répertorie tous les produits d'un client et vous permet de les supprimer. Pour afficher **Produits**, cliquez sur **Clients > {nom du client} > Produits (onglet)**. Pour supprimer un produit, cochez l'icône située à la gauche du produit, puis cliquez sur **Supprimer**. L'onglet **Produits** contient les éléments d'interface suivants :

- Nom du produit
- Type de produit
- Catégorie

- Incidents
- Détails
- État



Remarque

La mise à jour des données Hosted Email Security sur la console Web Remote Manager peut nécessiter jusqu'à trois heures. Les informations client Hosted Email Security sont mises à jour de manière quotidienne. Voir *Paramètres et mises à jour de données Hosted Email Security à la page 3-32*.

Licences

L'onglet **Licences** d'un client répertorie toutes les licences associées à un client. L'onglet **Licences** contient les éléments d'interface suivants :

- Nom du produit
- Plan de service/Version
- Licences utilisées
- Sièges fournis
- Date d'expiration
- État de renouvellement automatique

État des paramètres de sécurité

Pour afficher l'état des paramètres de sécurité en temps réel, cliquez sur **Clients** > {nom du client} > {produit} dans l'arborescence des réseaux > {groupe} > Paramètres de sécurité (panneau de droite).

Clients > Trend Micro_RM

The screenshot shows the 'Clients > Trend Micro_RM' interface. At the top, there are tabs for 'Produits' (3 9), 'Licences' (1 1), 'Profil de la société', 'Contact', 'Notification', and 'ConnectWise'. Below the tabs is a navigation tree on the left with 'Ajouter' and 'Tous les produits (3)'. The tree includes 'HES_HES', 'WFBS-A_BS_WIN-PCGBA...' (with sub-items 'Servers (default)' and 'Desktops (default)'), and 'WFBS-SVC_ttt'. The main panel on the right is titled 'Paramètres de sécurité' and shows the following information:

- Méthode de scan actuelle : Scan traditionnel
- Dernière mise à jour le : 10/févr./2014 08:13:45
- Paramètres de domaine:
 - Scan antivirus/anti-spyware en temps réel (✓)
 - Surveillance des comportements (✗)
 - Scan en temps réel du courrier POP3 (✗)
 - Filtrage des URL (✓)
 - Pare-feu (au bureau) (✗)
 - Pare-feu (hors bureau) (✗)
 - Réputation de sites Web (au bureau) (✓)
 - Réputation de sites Web (hors bureau) (✓)
 - Contrôle des périphériques (✗)
 - Stratégie de prévention des épidémies (OPP) (✓)

FIGURE 3-4. État des paramètres de sécurité en temps réel

Les paramètres Au bureau et Hors bureau sont consultables (s'applique exclusivement à Worry-Free Business Security Standard et Advanced). Les paramètres sont contrôlés au moyen du menu déroulant Paramètres. Les paramètres Hors Bureau ne sont pertinents que lorsque la détection d'emplacement est activée.

Pour plus d'informations, consultez *Barre de menu* à la page 3-26 et *Commandes Worry-Free Business Security* à la page 3-28.

Détection d'emplacement

La détection d'emplacement (s'applique exclusivement à Worry-Free Business Security Standard et Advanced) permet aux administrateurs de contrôler les paramètres de

sécurité en fonction du mode de connexion du client au réseau. Worry-Free Business Security Standard et Advanced identifie automatiquement l'emplacement du client et contrôle les sites Web auxquels les utilisateurs peuvent accéder. Les restrictions varient selon l'emplacement de l'utilisateur. Worry-Free Business Security classe les clients comme :

- **Clients normaux** : les ordinateurs stationnaires qui établissent une connexion réseau permanente avec le serveur Security Server.
- **Clients itinérants** : les ordinateurs qui n'établissent pas une connexion réseau permanente avec le serveur Security Server, par exemple les ordinateurs portables. Ces agents Client/Server Security Agent des clients participent à la protection antivirus du réseau mais communiquent leur état au serveur Security Server avec un certain retard.



Remarque

La détection d'emplacement contrôle les paramètres de connexion Au bureau/Hors bureau.

Barre de menus

La barre de menus sur le panneau de droite s'affiche uniquement lorsque Worry-Free ou Hosted Email Security est sélectionné dans l'arborescence des réseaux. Ces commandes vous permettent de gérer les aspects critiques de la sécurité, notamment les paramètres de scan en temps réel et le déploiement des mises à jour des composants. Pour obtenir

une liste des commandes de réseau faisant partie de la barre de menus, ainsi que des instructions sur leur utilisation, voir *Commandes Worry-Free Business Security à la page 3-28*.

Clients > **Trend Micro** ?

Produits **6** **16** Licences **3** Profil de la société Contact Notification ConnectWise

Ajouter

Tous les produits (6)

- ▶ WFBS-A_BS_20140313_W ●●
- ▶ WFBS-A_KKVM_KKVM-PC ●●
- ▶ WFBS-A_BS_WIN-PCGBA ●●
- ▶ WFBS_bs ●●
- ▶ WFBS-SVC_BSS_20140314 ●●
- ▶ WFBS-SVC_aaa ●●

Événements Groupes Paramètres de domaine Serveur géré Agent TMRM

Afficher par : Action requise et avertissement Menace et système Non résolu

Type	Catégorie	Occurrences	Détails	État
Aucun événement				

FIGURE 3-5. Barre de menus



Remarque

Les éléments de la barre de menus sont désactivés et ne répondent pas aux clics de souris si l'objet réseau sélectionné ne peut pas recevoir les commandes.

Terminaux

Si vous sélectionnez un serveur ou un poste de travail dans l'arborescence des réseaux, Trend Micro Remote Manager affiche des informations relatives au terminal. Les informations affichées varient selon que le terminal est un serveur/poste de travail ou un serveur Exchange. Pour afficher ces informations, cliquez sur l'onglet **Clients** > **{nom}**

du client} > {produit} > {groupe} > **Appareils (panneau de droite)**. Remote Manager™ affiche les informations suivantes :

Clients > Trend Micro_RM

Produits 3 0 Licences 1 1 Profil de la société Contact Notification ConnectWise

Ajouter

Tous les produits (3)

- HES_HES
- WFBS-A_BS_WIN-PCGBA
 - Servers (default) 0
 - Desktops (default) 3
- WFBS-SVC_ttt

Appareil Paramètres de sécurité

Nom	Adresse IP	État	Moteur de scan antivirus	Fichier de signatures de virus	Version
WFBS-A_BS_WIN-PCGBA	192.168.1.100	En ligne	AVP	2014-08-15	Window
WFBS-A_BS_WIN-PCGBA	192.168.1.101	En ligne	AVP	2014-08-15	Window
WFBS-A_BS_WIN-PCGBA	192.168.1.102	En ligne	AVP	2014-08-15	Window

Enregistrements : 1 - 3 / 3 Page 1 / 1 25 par page

FIGURE 3-6. État du terminal

- Nom
- Adresse IP
- État
- Moteur de scan antivirus
- Signatures de virus
- Version de plate-forme

Commandes Worry-Free Business Security

Les commandes Worry-Free Business Security (Standard et Advanced) vous permettent de gérer les aspects critiques de la sécurité, y compris le déploiement de composants de sécurité, le scan des ordinateurs pour détecter des virus et des failles connues, ainsi que la mise à niveau des serveurs gérés.



Remarque

Les commandes de cette section sont disponibles uniquement pour Worry-Free Business Security (Standard et Advanced). Pour Worry-Free Business Security Services et Hosted Email Security, vous devez vous connecter à la console Web de ces produits.

Le tableau ci-dessous répertorie les commandes du menu Paramètres de Worry-Free Business Security (Standard et Advanced).

TABEAU 3-2. Commandes du menu Paramètres

COMMANDE	ACTION	EFFETS
Scan manuel	Démarrer ou arrêter un scan pour un domaine ou un groupe entier.	Permet un scan manuel à la demande.
Mise à jour immédiate	Déployer les derniers composants de sécurité, y compris le moteur de scan et les fichiers de signatures.	Autorise les mises à jour de composants à la demande.
Scan antivirus/anti-spyware en temps réel	Activer/désactiver les scanners antivirus et anti-spyware en temps réel sur tous les ordinateurs du domaine.	Le scan en temps réel scanne automatiquement les fichiers faisant l'objet d'un accès. La désactivation du scan en temps réel rend le domaine vulnérable.
Scan en temps réel du courrier POP3	Activer/désactiver le scan en temps réel de la messagerie POP3 pour tout le domaine.	Le scan de la messagerie POP3 (utilisant le plug-in de barre d'outils anti-spam de Trend Micro) protège les ordinateurs en temps réel contre les risques de sécurité et les spams transmis via les e-mails POP3.
Activer la surveillance des comportements	Activer/désactiver la surveillance des comportements pour tout le domaine.	La surveillance des comportements protège les ordinateurs des modifications non autorisées qui pourraient être apportées au système d'exploitation, aux entrées de registre, aux autres logiciels, aux fichiers et aux dossiers.

COMMANDE	ACTION	EFFETS
Détection d'emplacement	Activer/désactiver la détection d'emplacement pour tout le domaine.	<p>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.</p> <p>Cette fonction affecte les paramètres « Au bureau/Hors bureau » du pare-feu, de la réputation des sites Web et des barres d'outils TrendSecure : anti-enregistreurs de frappe, chiffrement de frappe, évaluation des pages.</p> <p>Les paramètres Au bureau fonctionnent comme les paramètres par défaut si la détection d'emplacement est désactivée.</p> <p>Les paramètres Hors bureau ne sont disponibles que si la détection d'emplacement est activée.</p>
Pare-feu	Activer/désactiver le pare-feu personnel pour tout le domaine.	En fonction des règles de pare-feu existantes, l'activation du pare-feu peut limiter la capacité des ordinateurs à communiquer avec le réseau. La désactivation, quant à elle, peut exposer les ordinateurs à du trafic réseau indésirable.
Réputation de sites Web	Configurer la réputation de sites Web pour tout le domaine.	La réputation de sites Web contribue à empêcher l'accès aux URL représentant un risque de sécurité potentiel par le biais de la vérification de toute URL demandée dans la base de données de sécurité Web de Trend Micro.

COMMANDE	ACTION	EFFETS
Filtrage des URL	Activer/désactiver le filtrage des URL pour tout le domaine.	L'activation du filtrage des URL surveillera les tentatives d'accès aux sites Web non autorisés. Cela est disponible uniquement pour Worry-Free Business Security Services et Worry-Free Business Security Advanced 6.0 et versions ultérieures.
Contrôle des périphériques	Activer/désactiver le contrôle de périphériques pour tout le domaine.	L'activation du contrôle des périphériques surveillera les tentatives non autorisées d'accès aux périphériques. Cela est disponible uniquement pour Worry-Free Business Security Advanced 7.x et 8.0.
Démarrer l'évaluation des failles	Lancer l'évaluation des failles pour scanner les ordinateurs dans le domaine et détecter les failles connues.	Consomme quelques ressources sur les ordinateurs et accroît légèrement le trafic entre le serveur géré et les ordinateurs.
Démarrer Damage Cleanup Service	Déployer Damage Cleanup Services (DCS) pour nettoyer les ordinateurs infectés.	Consomme quelques ressources sur les ordinateurs et accroît légèrement le trafic entre le serveur géré et les ordinateurs.
Mise à jour du serveur géré	Déployer les derniers composants de sécurité, notamment le moteur de scan et les fichiers de signatures, sur le serveur géré.	Vérifie que les ordinateurs exécutent les derniers composants de sécurité. Le déploiement peut accroître le trafic entre les ordinateurs et le serveur géré.

COMMANDE	ACTION	EFFETS
Mise à jour de Client Server Security Agent	Déployer les derniers composants de sécurité, notamment le moteur de scan et les fichiers de signatures, sur tous les agents Client Server Security Agent du domaine.	Vérifie que les ordinateurs exécutent les derniers composants de sécurité. Le déploiement peut accroître le trafic entre les ordinateurs et le serveur géré.

Paramètres et mises à jour de données Hosted Email Security

Pour afficher les paramètres et les données HES, y compris l'état actuel, les paramètres généraux et la rubrique À propos de..., cliquez sur l'onglet **Clients** > **{client}** > **Hosted Email Security**.

Les détails suivants sont répertoriés pour tous les domaines et mis à jour une fois par jour :

- Toutes les informations sous l'onglet **État actuel**.
- **Paramètres de stratégie**
- **Expéditeurs approuvés**
- Toutes les informations sous l'onglet **Infos sur la licence**.



Remarque

La mise à jour des données Hosted Email Security sur la console Web Remote Manager peut nécessiter jusqu'à trois heures.

Notifications

Les notifications client peuvent être envoyées par e-mail ou vues depuis le widget **Notifications** ou un logiciel tiers.

L'écran **Configurer les notifications** apparaîtra. Sur cette page, vous pouvez définir les fonctionnalités suivantes :

- Les événements qui déclencheront les notifications :
 - Les événements liés à la licence :
 - **Arrivant bientôt à expiration** : envoie une notification s'il y a des licences qui arrivent bientôt à expiration. Vous pouvez également régler la fréquence à laquelle le système va envoyer une notification.
 - **Une fois par mois** : le système enverra une notification par e-mail tous les 30 jours, 60 jours avant l'expiration.
 - **Bi-hebdomadaire** : le système enverra une notification par e-mail tous les 14 jours, 28 jours avant l'expiration.
 - **Hebdomadaire** : le système enverra une notification par e-mail tous les 7 jours, 14 jours avant l'expiration.

**Remarque**

Bien que vous ayez réglé les notifications afin de recevoir un e-mail par semaine uniquement, toutes les deux semaines ou un par mois, il est possible que vous receviez une notification par e-mail tous les jours car la notification par e-mail dépend de la date d'expiration de chaque société. Cependant, afin de garantir que vous ne recevez pas plusieurs e-mails de notification le même jour, Trend Micro inclut également les noms des sociétés, ainsi que les dates des autres produits arrivant bientôt à expiration dans le même e-mail.

-
- **Expiré** : envoie une notification s'il y a des licences qui ont déjà expiré.
 - **Dépassement du nombre affecté** : envoie une notification si le pourcentage de sièges utilisés dépasse le nombre de sièges fournis. Vous pouvez spécifier le pourcentage de sièges utilisés dépassant le nombre de sièges fournis au client. Cette valeur peut être comprise entre 100 et 120.
 - Les événements liés au produit :
 - Les événements Worry-Free Business Security et Worry-Free Business Security Services :
 - **Menaces** : envoie une notification si le nombre d'événements de menaces dépasse le seuil spécifié.

- **Système** : envoie une notification si le nombre d'événements système ou périphérique dépasse le seuil spécifié.
- Événements Cloud Edge :
 - **Le nombre de menaces Web détectées dépasse** : envoie une notification si le nombre d'événements de menaces Web détectées dépasse le seuil spécifié.
- Destinataires de la notification :
 - **Kaseya** (événements Worry-Free Business Security et Worry-Free Business Security Services uniquement)
 - **Autotask** (événements Worry-Free Business Security et Worry-Free Business Security Services uniquement)
 - **ConnectWise**
 - **Moi** : il s'agit de l'adresse e-mail qui recevra la notification par e-mail.



Remarque

Si l'adresse e-mail est incorrecte, cliquez sur le lien de **Licensing Management Platform** ou le bouton **Mon compte** pour accéder à la page des paramètres du profil et modifier les paramètres du profil.

- **Destinataires supplémentaires** : vous pouvez spécifier des destinataires d'e-mails supplémentaires pour des événements spécifiques à certains clients.

Pour plus d'informations sur comment configurer une notification, consultez [Configuration des notifications à la page 8-2](#).

Mises à jour de l'état et des données de Worry-Free Business Security Services

Pour afficher les paramètres et les données Worry-Free Business Security Services, y compris l'état, cliquez sur **Clients** > **{nom du client}** > **{produit}** > **WFBS-SVC**.

Les informations relatives à Worry-Free Business Security Services sont mises à jour une fois par jour. Ces informations comprennent :

- toutes les informations sous **Paramètres de sécurité**.
- La **date d'expiration** qui figure dans l'onglet **Infos sur la licence** (la date d'expiration est celle du code d'activation de Worry-Free Business Security Services).



Remarque

La mise à jour des données Worry-Free Business Security Services sur la console Web Remote Manager peut nécessiter jusqu'à trois heures.

En fonction de votre mécanisme de licence, les options affichées peuvent différer.

Chapitre 4

Préparation de l'infrastructure

Cette section contient les rubriques suivantes :

- *Présentation de l'installation de l'infrastructure à la page 4-2*
- *Ajout de produits à la page 4-3*

Présentation de l'installation de l'infrastructure

En règle générale, la préparation de l'infrastructure de service passe par les étapes suivantes pour chaque type de produit/service.

Worry-Free Business Security Standard et Advanced

1. Ajoutez un nouveau client à la console Web Remote Manager.
2. Ajoutez le contact du client principal.
3. Ajoutez au moins un produit pour ce client.
4. Installez l'agent sur le serveur du client.
5. Saisissez le GUID ou la clé d'enregistrement sur l'agent.

Hosted Email Security et Worry-Free Business Security Services

1. Ajoutez un nouveau client à la console Web Remote Manager.
2. Ajoutez le contact du client principal.
3. Ajoutez au moins un service pour ce client.
4. Saisissez la clé d'autorisation sur la console du service du client.

ConnectWise

1. Liez ConnectWise et ajoutez les informations d'identification ConnectWise sous **Administration > Configurer l'intégration de tiers (écran)** de la console Web Remote Manager.
2. Spécifiez les paramètres généraux de notification ConnectWise.
3. Ajoutez le destinataire de la notification à la liste des destinataires sous **Clients > {client} > Notification (onglet)** de la console Web Remote Manager.

4. Ajoutez les champs obligatoires à la console ConnectWise.
5. (Facultatif) Configurez les paramètres et la notification ConnectWise de chaque client.

Kaseya

1. Liez Kaseya et ajoutez les informations d'identification Kaseya sous **Administration > Configurer l'intégration de tiers (écran)** de la console Web Remote Manager.
2. Ajoutez le destinataire de la notification à la liste des destinataires sous **Clients > {client} > Notification (onglet)** de la console Web Remote Manager.
3. Ajoutez les champs obligatoires à la console Kaseya.

Autotask

1. Liez Autotask et ajoutez les informations d'identification Autotask sous **Administration > Configurer l'intégration de tiers (écran)** de la console Web Remote Manager.
2. Ajoutez le destinataire de la notification à la liste des destinataires sous **Clients > {client} > Notification (onglet)** de la console Web Remote Manager.
3. Ajoutez les champs obligatoires à la console Autotask.

Ajout de produits

Ajout de clients

Vous devez identifier les informations client de base avant de créer le compte client. Parmi les champs notables figurent **Prénom et nom** (tels qu'ils s'afficheront dans les rapports et les notifications), **Fuseau horaire** (du client) et **Langue** (dans laquelle le client recevra les rapports et les notifications). Avant d'ajouter un client et d'installer

l'agent sur le serveur géré, vérifiez que vous disposez de l'approbation écrite pour effectuer les tâches visant à accéder aux ressources du client, à les surveiller et à les gérer.

Procédure

1. À partir de la bannière de la console Web Remote Manager, cliquez sur **Nouveau Client**.



Remarque

Vous pouvez cliquer sur **Nouveau Client** à partir de la bannière ou à partir de l'onglet **Clients**.

2. Renseignez les informations client.

Nouveau client

Saisir les informations client

Profil de la société

Nom de la société :*

Adresse :

Ville :*

État/Région :*

Code postal :

Pays : Chine

Compte utilisateur

ID du compte :*

Personne à contacter :*

Prénom

Nom

Numéro du contact :

Indicatif régional - Numéro de téléphone - Poste

Adresse électronique :*

Fuseau horaire : (UTC-08:00) Fuseau horaire du Pacifique (États-Unis et Canada)

Langue : Anglais (États-Unis)

Suivant > Annuler

FIGURE 4-1. Écran Infos client

3. Cliquez sur **Suivant >**.
4. Affectez un plan de service, la date d'entrée en vigueur de la licence et le nombre d'unités par licence.

Nouveau client

Affecter le plan de service à testrmx

Plan de service : BSS_Monthly_noautorenew_RM_FULL
Full CE
trial CE

Date de début :* 16/04/2014

Unités par licence :* 50 sièges

< Précédent Suivant > Terminé Annuler

5. Configurez les paramètres par défaut du produit pour ce compte. Il s'agit des paramètres suivants :



Remarque

Cette fonction est prévue uniquement pour Worry-Free Business Security Services.

- **Paramètres de base du produit** : configurez uniquement les paramètres apparaissant sur cet écran que les nouveaux comptes client utiliseront.

FIGURE 4-2. Paramètres de base du produit

- **Modèles** : utilisez cette option pour sélectionner un modèle de paramètre par défaut. Configurez les paramètres à partir de **Admin > Configurer les modèles de paramètres par défaut**.
6. Vérifiez toutes les informations et cliquez sur **Terminé**.



Remarque

Une fois le client ajouté, les profils ne peuvent être modifiés qu'à partir de Trend Micro Licensing Management Platform.

Enregistrement des produits Trend Micro dans Trend Micro Remote Manager

Vous pouvez enregistrer les produits Trend Micro dans Trend Micro Remote Manager. Pour les produits tiers, consultez *Intégration de produits tiers à Trend Micro Remote Manager à la page 4-15*.

Enregistrement de Worry-Free Business Security

Cette section vous explique comment connecter ou déconnecter Worry-Free Business Security dans Trend Micro Remote Manager.

GUID ou clé d'enregistrement de l'agent

Pour distinguer les différents produits et services, Remote Manager attribue un identificateur global unique (GUID) ou une clé d'enregistrement à chacun d'eux. À chaque ajout de produit ou de service à la console Web Remote Manager, Remote Manager génère un nouveau GUID ou une nouvelle clé d'enregistrement. La personne installant l'agent sur le serveur géré ou ajoutant le service à la console Web Remote Manager doit saisir le GUID ou la clé d'enregistrement au cours de l'installation pour que le produit ou service soit enregistré auprès de Remote Manager.

Les GUID ou clés d'enregistrement des produits ou services d'un client sont toujours disponibles à l'endroit suivant : **Clients** > **Tous les clients (dans l'arborescence)** > **{client}** > **Agent TMRM (onglet)**.

Clients > Trend Micro

The screenshot shows the Trend Micro Remote Manager interface. At the top, there are tabs for 'Produits' (6, 16), 'Licences' (3), 'Profil de la société', 'Contact', 'Notification', and 'ConnectWise'. Below this is a sidebar with a tree view under 'Ajouter' and 'Tous les produits (6)'. The selected product is 'WFBS-A_KKVM_KKVM-PC'. The main panel has tabs for 'Événements', 'Groupes', 'Paramètres de domaine', 'Serveur géré', and 'Agent TMRM'. The 'Agent TMRM' tab is active, displaying the following information:

État :	En ligne
Nom de la société :	KKVM-PC
GUID :	1A2B3C4567D8-E1FGHI23-J456-78K9-1L23
Adresse IP :	192.168.1.10
Enregistré le :	02/avr./2014 02:12:48
Dernière mise à jour :	15/avr./2014 09:07:25
Version de l'agent :	3.5.0.1033
Produit géré :	Worry-Free Business Security Advanced 9.0
Version du produit géré :	9.0

FIGURE 4-3. Le GUID ou la clé d'autorisation de l'agent est toujours disponible (Worry-Free Business Security Standard et Advanced)

Remote ManagerGUID de l'agent

```
1A2B3C4567D8-E1FGHI23-J456-78K9-1L23
```

Installation de l'agent pour Worry-Free Business Security 6,0 et versions ultérieures

Il existe plusieurs façons d'installer l'agent Trend Micro Remote Manager sur le serveur Worry-Free Business Security Standard or Advanced 6.0 et versions ultérieures. Les procédures d'installation changent selon que le client est nouveau ou qu'il a déjà un compte sur la console Web Remote Manager.

Informations préalables

- Remote ManagerGUID de l'agent
- Programme d'installation de l'agent (WFRMAgentforWFBS.exe)
- Connexion Internet active

- 50 Mo d'espace disque disponible

Clients sans compte Remote Manager

Procédure

- Option 1 : À partir de la console Web Remote Manager
 1. À partir de la console Web Remote Manager, ajoutez le client et saisissez une description facultative.
 2. Ajoutez Worry-Free Business Security Standard ou Advanced à la console Web Remote Manager, en générant un GUID durant ce processus.
 3. Installez l'agent Remote Manager sur le serveur Worry-Free Business Security Standard ou Advanced en utilisant le GUID généré par la console.
 - Option 2 : Installez l'agent sur le serveur Worry-Free Business Security
Utilisez le programme d'installation de l'agent Remote Manager du serveur Worry-Free Business Security (sans d'abord ajouter le client à la console Web Remote Manager) pour installer l'agent.
-

Clients avec des comptes Remote Manager

Procédure

1. Ajoutez Worry-Free Business Security Standard ou Advanced à la console Web Remote Manager, en générant un GUID durant ce processus.
 2. Installez l'agent Remote Manager sur le serveur Worry-Free Business Security Standard ou Advanced en utilisant le GUID généré par la console.
-

Vérification de l'installation de l'agent Trend Micro Remote Manager

Vérifiez que l'agent a été correctement installé.

Vérification de l'état du service d'agent

Sur l'ordinateur où est installé l'agent Remote Manager, vérifiez si Centre d'informations Trend Micro pour CSM est démarré.

Procédure

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Outils administrateurs > Services**.
 2. Recherchez l'agent **Trend Micro Remote Manager Agent**.
 3. Vérifiez si l'état est **Démarré**.
-

Vérification des raccourcis du menu Démarrer

Sur l'ordinateur où l'agent Trend Micro Remote Manager est installé, vérifiez le groupe de programmes dans le menu Démarrer.

Procédure

1. Cliquez sur **Démarrer > Programmes > Trend Micro Remote Manager Agent**.
 2. Vérifiez que le groupe de programmes contient les éléments suivants :
 - Outil de configuration de l'agent
 - Lisez-moi
-

Vérification des icônes de la barre d'état système

Sur l'ordinateur sur lequel l'agent Trend Micro Remote Manager est installé, vérifiez que l'icône de l'agent Trend Micro Remote Manager est présente dans la barre d'état système. Si, pour une quelconque raison, l'icône ne s'y trouve pas, vous pouvez la faire apparaître en cliquant sur **Démarrer > Programmes > Trend Micro Remote Manager Agent > Outil de configuration de l'agent**.

Le fait de quitter l'outil n'arrête pas le service Trend Micro 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.

Placez la souris au-dessus de l'icône pour obtenir les informations d'état.

TABLEAU 4-1. Icônes de la barre d'état système

ICÔNE	DESCRIPTION
	Une icône verte indique que l'agent est connecté au serveur de communication Trend Micro Remote Manager. L'agent fonctionne normalement.
	Une icône rouge indique que l'agent n'est pas connecté au serveur de communication Trend Micro Remote Manager ou que sa version 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 Trend Micro Remote Manager.
	Une icône avec un « X » rouge signifie que l'agent a été désactivé.

Vérification de la connexion entre l'agent et le serveur

Pour vérifier que le service Trend Micro Remote Manager s'exécute correctement, assurez-vous que les agents s'affichent à l'état « Connecté » ou « En ligne » sur la console Web Remote Manager.

Accédez à **Clients** > {client} > **Produits (onglet)**.

L'arborescence répertorie l'état de chaque agent dans la colonne **État**. Pour obtenir des détails sur chaque état, voir [État de l'agent à la page 6-2](#)

En plus de la section en cours, consultez [Dépannage et problèmes connus à la page 11-1](#) pour d'autres problèmes de connectivité serveur/agent.

Affichage des erreurs d'installation

Les journaux d'installation des agents couvrent les activités d'installation des agents. Si vous rencontrez des problèmes au cours de l'installation, rassemblez ces journaux et envoyez-les à votre service d'assistance. Les journaux d'installation des agents sont accessibles à l'emplacement suivant sur le serveur géré :

C:\WFRMAgentForCSM_Install.log

Enregistrement de Worry-Free Business Security Services

Cette section vous explique comment connecter ou déconnecter Worry-Free Business Security Services dans Trend Micro Remote Manager.

Connexion d'un client Worry-Free Business Security Services à la console Web Remote Manager

Afin de gérer Worry-Free Business Security Services depuis la console Web Trend Micro Remote Manager, vous devez enregistrer le compte Worry-Free Business Security Services d'un client auprès de Remote Manager en suivant la procédure ci-après :



Remarque

Si le revendeur a ajouté le produit à votre compte à partir de Licensing Management Platform, vous n'avez pas besoin de suivre cette procédure.

Procédure

1. Ajoutez le produit à la console Web Remote Manager et enregistrez le GUID ou la clé d'enregistrement.

Pour plus d'informations, consultez *Ajout de produits/services à la page 5-9*.
 2. Connectez-vous au compte Worry-Free Business Security Services du client.
 3. Accédez à **Administration** > **Trend Micro Remote Manager**.
 4. Saisissez la clé d'autorisation et cliquez sur **Se connecter**.
-

Déconnexion d'un client Worry-Free Business Security Services de la console Web Remote Manager

Pour déconnecter un client Worry-Free Business Security Services de la console Web Remote Manager :

- Si le compte a été intégré à Licensing Management Platform, le revendeur peut supprimer le plan de service à partir de la console Web Licensing Management Platform. Une fois le plan de service supprimé, le client est déconnecté de la console Web Remote Manager.
- Pour les autres comptes, le client peut ouvrir l'écran Remote Manager sur la console Web Worry-Free Business Security Services, puis cliquer sur **Déconnexion**.

Le client reçoit ensuite une notification sur la console Worry-Free Business Security Services.

Enregistrement de Hosted Email Security

Cette section vous explique comment connecter ou déconnecter Hosted Email Security dans Trend Micro Remote Manager.

Connexion d'un client Hosted Email Security à la console Web Remote Manager

Pour gérer Hosted Email Security à partir de la console Web Trend Micro Remote Manager, le compte Hosted Email Security d'un client doit être enregistré auprès de Remote Manager.



Remarque

Si le revendeur a ajouté le produit à votre compte à partir de Licensing Management Platform, vous n'avez pas besoin de suivre cette procédure.

Procédure

1. Ajoutez le produit à la console Web Remote Manager et enregistrez le GUID ou la clé d'enregistrement.
2. Connectez-vous au compte Hosted Email Security du client.
3. Accédez à **Administration > Remote Manager**.
4. Saisissez le GUID ou la clé d'enregistrement, puis cliquez sur **Se connecter**.

Une fois que vous avez saisi le GUID ou la clé d'enregistrement et cliqué sur **Se connecter**, la connexion de Hosted Email Security à la console Web Remote Manager peut prendre jusqu'à dix minutes.

5. Examinez l'état de la connexion.

La mise à jour des données Hosted Email Security sur la console Web Remote Manager peut nécessiter jusqu'à trois heures. Les informations client Hosted Email Security sont mises à jour de manière quotidienne. Voir *Paramètres et mises à jour de données Hosted Email Security à la page 3-32*.

Déconnexion d'un client Hosted Email Security de la console Web Remote Manager

Pour déconnecter un client Hosted Email Security de la console Web Remote Manager :

- Si le compte a été intégré à Licensing Management Platform, le revendeur peut supprimer le plan de service à partir de la console Web Licensing Management Platform. Une fois le plan de service supprimé, le client est déconnecté de la console Web Remote Manager.
- Pour les autres comptes, le client peut ouvrir l'écran Remote Manager sur la console Web Hosted Email Security, puis cliquer sur **Se désinscrire**.

Le client reçoit ensuite une notification sur la console Hosted Email Security et doit cliquer sur **OK**.

Intégration de produits tiers à Trend Micro Remote Manager

Vous pouvez enregistrer des produits tiers dans Trend Micro Remote Manager. Pour les produits Trend Micro, consultez *Enregistrement des produits Trend Micro dans Trend Micro Remote Manager à la page 4-8*.

Intégration d'Autotask™

Configurez les paramètres suivants pour intégrer Autotask™ à Remote Manager :

Configuration des paramètres Autotask dans Remote Manager

Procédure

1. Cliquez sur **Administration > Configurer l'intégration de tiers**.

La fenêtre **Intégration de tiers** s'ouvre.

Autotask

Activer l'intégration

ID de connexion :

Mot de passe de connexion :

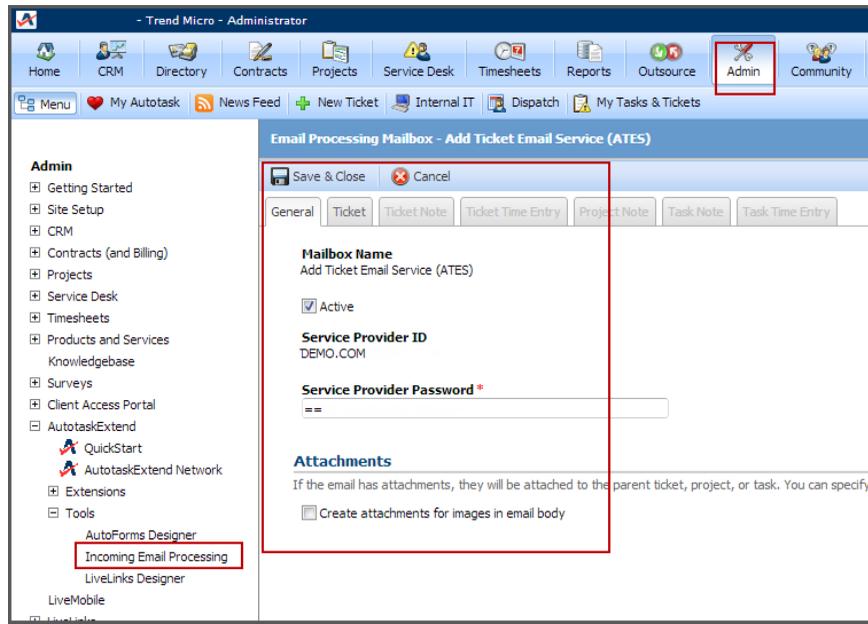
Langue :

Anglais



FIGURE 4-4. Zone du groupe des notifications des informations sur le compte

2. Cliquez sur **Activer l'intégration**.
3. Spécifiez les informations d'identification. Vous pouvez vérifier les informations d'identification Autotask dans **Admin > AutotaskExtend > Outils > Traitement des messages entrants > Ajouter un service de messagerie de ticket > Modifier > Général**.



4. Sélectionnez la langue préférée.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Clients > Tous les clients (dans l'arborescence) > (client) > Notifications (onglet)**.

Clients > Trend Micro



Produits **6** **16** Licences **3** Profil de la société Contact **Notification** ConnectWise

Événements

Utiliser les [paramètres de notification en temps réel](#) par défaut
 Utiliser les paramètres personnalisés

Tous les événements de licence

Événement	E-mail	Fréquence des messages	Seuil d'alerte
Arrivant bientôt à expiration	<input checked="" type="checkbox"/>	Toutes les deux semaines	Licence arrivant à expiration dans 28 jours
Expiré	<input checked="" type="checkbox"/>	Par événement	
Dépassement du nombre affecté	<input checked="" type="checkbox"/>	Par événement	La quantité attribuée dépasse (%) : 100

Worry-Free Business Security Services

Événement	E-mail
Menace	<input checked="" type="checkbox"/>
Système	<input checked="" type="checkbox"/>

Worry-Free Business Security

Événement	E-mail
Menace	<input checked="" type="checkbox"/>
Système	<input checked="" type="checkbox"/>

Cloud Edge

Événement	E-mail	Seuil d'alerte
Seuil de menaces Web détectées dépassé	<input checked="" type="checkbox"/>	Le nombre de menaces Web dépasse : 1 (1-300)

Destinataires

Remarque : Activez l'intégration avec les outils tiers pour pouvoir recevoir des notifications. Pour cela, sélectionnez [Administration > Configurer l'intégration de tiers](#). Pour ConnectWise, vous devez également activer le paramètre de clients spécifiques en cliquant sur l'onglet ConnectWise à la page client.

ConnectWise
 Kaseya (événements Worry-Free Business Security et Worry-Free Business Security Services uniquement)
 Autotask (événements Worry-Free Business Security et Worry-Free Business Security Services uniquement)

Destinataires supplémentaires :

Si vous saisissez plusieurs entrées, séparez-les par un point-virgule.

FIGURE 4-5. Sélection des notifications obligatoires

7. Sélectionnez les notifications à envoyer à Autotask pour Worry-Free Business Security Services.
 8. Dans les destinataires, sélectionnez Autotask.
 9. Répétez les étapes 5, 6 et 7 pour chaque client.
-

Configuration des paramètres dans Autotask

Procédure

1. Dans Autotask, pour ajouter les champs suivants au système de tickets, accédez à **Admin > Bureau de service > Types de problèmes et de sous-problèmes > Alerte des services gérés**. Cela active l'affichage des notifications Trend Micro Remote Manager dans Autotask. Sélectionnez l'une des alertes de service géré suivantes :
 - Événements de menaces Trend Micro
 - Événements système Trend Micro
 - Événements de licence Trend Micro

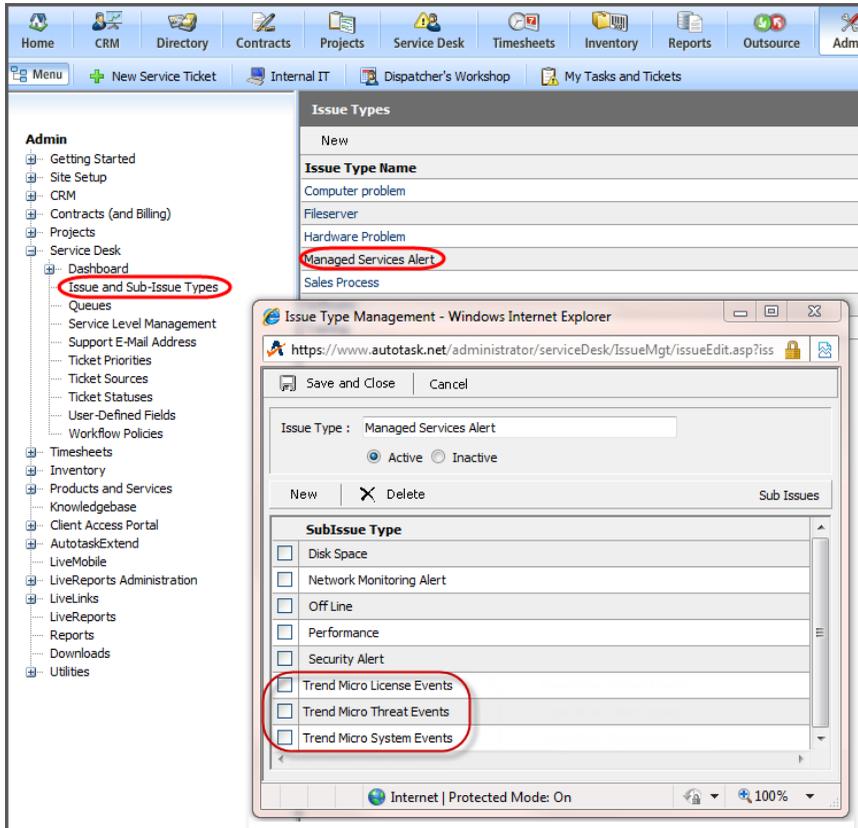


FIGURE 4-6. Types de sous-problèmes Trend Micro

2. Accédez à **Admin > AutotaskExtend > Outils > Traitement des messages entrants > Ajouter un service de messagerie de ticket > Modifier > Ticket**, puis vérifiez que la configuration des e-mails est correcte :

The screenshot displays the configuration page for the 'Email Processing Mailbox - Add Ticket Email Service (ATES)'. The interface includes a top navigation bar with icons for Home, CRM, Directory, Contracts, Projects, Service Desk, Timesheets, Reports, Outsource, Admin, Community, and Help. Below this is a secondary navigation bar with 'Menu', 'My Autotask', 'News Feed', 'New Ticket', 'Internal IT', 'Dispatch', and 'My Tasks & Tickets'. The main content area is titled 'Email Processing Mailbox - Add Ticket Email Service (ATES)' and contains several sections:

- Save & Close** and **Cancel** buttons.
- Tabbed interface with 'General', 'Ticket', 'Ticket Note', 'Ticket Time Entry', 'Project Note', 'Task Note', and 'Task Time Entry' tabs. The 'Ticket' tab is active.
- Enabled**
- Defaults** section:
 - Status ***: New
 - Priority ***: High
 - Queue ***: Managed Services Alerts
 - Source ***: Monitoring Alert
 - Due Date Offset ***: 1 Days
 - Due Time**:
 - Use Default Due Time from Workflow Policy
 - Offset from Create Time by:
 - 0 hours
 - 0 minutes
- Issue Type**: Managed Services Alert
- Sub-Issue Type**: Trend Micro Threat Events (with a dropdown menu showing options like Disk Space, Network Monitoring Alert, Off Line, Performance, Security Alert, Trend Micro License Events, Trend Micro Other Events, Trend Micro Site ID, Trend Micro System Events, Trend Micro Threat Events, and Virus Alert).
- Failure Notification (to email originator)**:
 - When a ticket cannot be successfully created, an email will be sent to the email sender that initiated the ticket creation. Specify the notification template.
 - Notification Template**: (dropdown menu)
 - Send XML Notifications

3. Accédez à **Admin > Configuration du site > Zones définies par l'utilisateur**, puis créez le champ de l'identifiant du site Trend Micro :

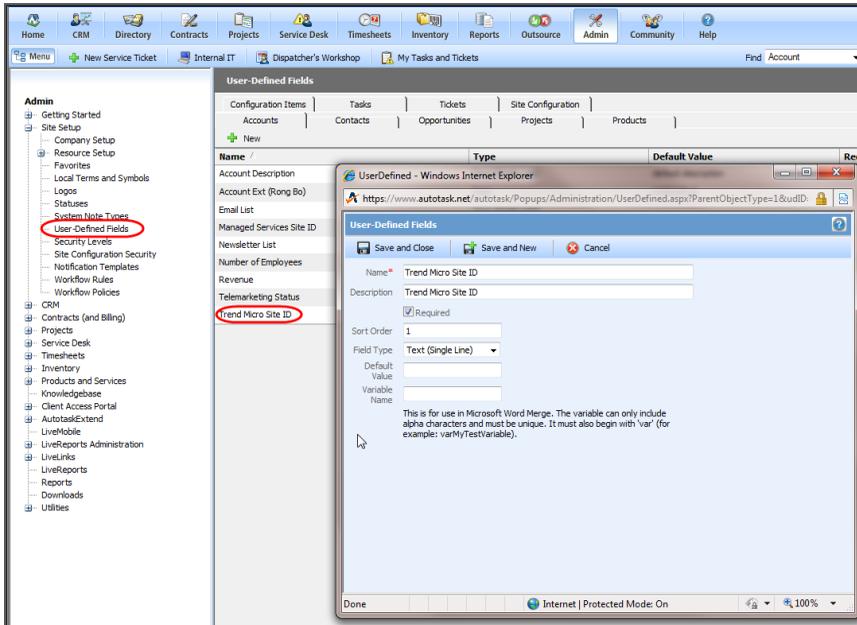
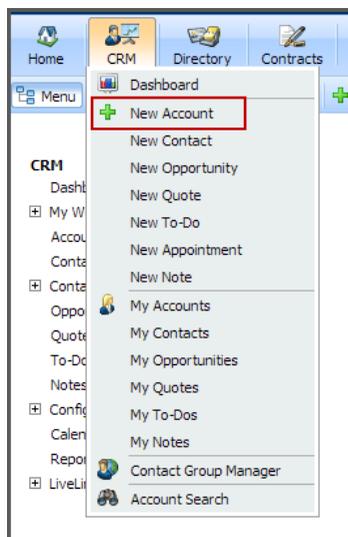


FIGURE 4-7. Définition de l'identifiant du site Trend Micro

4. Accédez à **CRM > Nouveau compte**, puis saisissez l'ID unique Remote Manager dans le nouveau champ Identification du site Trend Micro.

Il s'agit de l'identifiant unique exporté depuis Remote Manager.



Intégration de Kaseya™

Configurez les paramètres suivants pour intégrer Kaseya™ à Remote Manager :

Configuration des paramètres Kaseya dans Remote Manager

Procédure

1. Cliquez sur **Administration** > **Configurer l'intégration de tiers**.

La fenêtre **Intégration de tiers** s'ouvre.

Kaseya

Activer l'intégration

Adresse électronique Kaseya :

FIGURE 4-8. Zone du groupe des notifications des informations sur le compte

2. Cliquez sur **Activer l'intégration**.
3. Ajoutez l'adresse électronique Kaseya.
4. Cliquez sur **Enregistrer**.
5. Accédez à **Clients > Tous les clients (dans l'arborescence) > {client} > Notifications (onglet)**.

Clients > Trend Micro



Produits **6** **16** Licences **3** Profil de la société Contact **Notification** ConnectWise

Événements

Utiliser les [paramètres de notification en temps réel](#) par défaut

Utiliser les paramètres personnalisés

Tous les événements de licence

Événement	E-mail	Fréquence des messages	Seuil d'alerte
Arrivant bientôt à expiration	<input checked="" type="checkbox"/>	Toutes les deux semaines	Licence arrivant à expiration dans 28 jours
Expiré	<input checked="" type="checkbox"/>	Par événement	
Dépassement du nombre affecté	<input checked="" type="checkbox"/>	Par événement	La quantité attribuée dépasse (%) : 100

Worry-Free Business Security Services

Événement	E-mail
Menace	<input checked="" type="checkbox"/>
Système	<input checked="" type="checkbox"/>

Worry-Free Business Security

Événement	E-mail
Menace	<input checked="" type="checkbox"/>
Système	<input checked="" type="checkbox"/>

Cloud Edge

Événement	E-mail	Seuil d'alerte
Seuil de menaces Web détectées dépassé	<input checked="" type="checkbox"/>	Le nombre de menaces Web dépasse : 1 (1-300)

Destinataires

Remarque : Activez l'intégration avec les outils tiers pour pouvoir recevoir des notifications. Pour cela, sélectionnez [Administration > Configurer l'intégration de tiers](#). Pour ConnectWise, vous devez également activer le paramètre de clients spécifiques en cliquant sur l'onglet ConnectWise à la page client.

ConnectWise

Kaseya (événements Worry-Free Business Security et Worry-Free Business Security Services uniquement)

Autotask (événements Worry-Free Business Security et Worry-Free Business Security Services uniquement)

Destinataires supplémentaires :

Si vous saisissez plusieurs entrées, séparez-les par un point-virgule.

FIGURE 4-9. Sélection des notifications obligatoires

6. Sélectionnez les paramètres de notification de produit devant être envoyés à Kaseya.



Remarque

Sélectionnez les paramètres de notification en temps réel par défaut qui s'appliquent à tous les produits et clients, ou spécifiez les paramètres pour ce client.

7. Dans les destinataires, sélectionnez Kaseya.
8. Répétez les étapes 5, 6 et 7 pour chaque client.

Configuration des paramètres dans Kaseya

Procédure

1. Dans Kaseya, ajoutez les champs suivants au système de tickets pour afficher les notifications Trend Micro Remote Manager.
 - Worry-Free Business Security

NOM DU CHAMP	FONCTION
TM_CreateTime	Heure de génération de l'événement
TM_ProductName	Nom du produit
TM_AgentGUID	GUID de l'agent Remote Manager
TM_CustomerName	Client/Nom de la société
TM_EventName	Nom de l'événement
TM_ServerName	Nom du serveur Client Server Messaging/Worry-Free Business Security
TM_MASClientName (facultatif)	Nom du serveur Exchange (ne concerne que l'événement Arrêt du serveur Exchange)

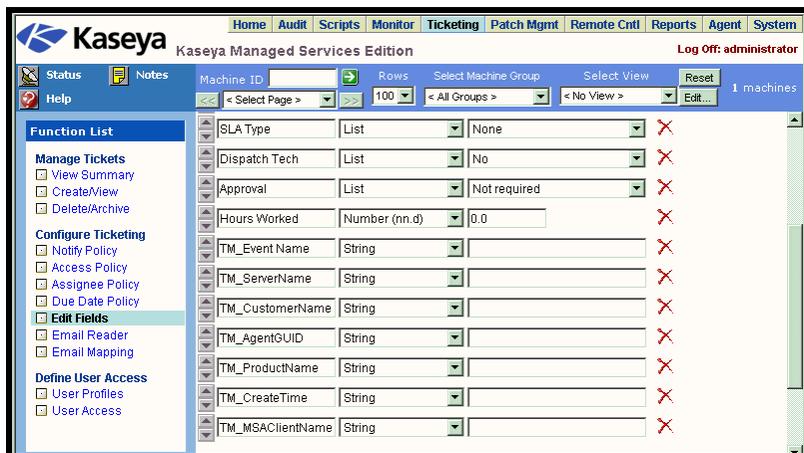


FIGURE 4-10. Champs de tickets Kaseya

- Worry-Free Business Security Services

NOM DU CHAMP	FONCTION
TM_CreateTime	Heure de génération de l'événement
TM_ProductName	Nom du produit
TM_CustomerName	Client/Nom de la société
TM_EventName	Nom de l'événement

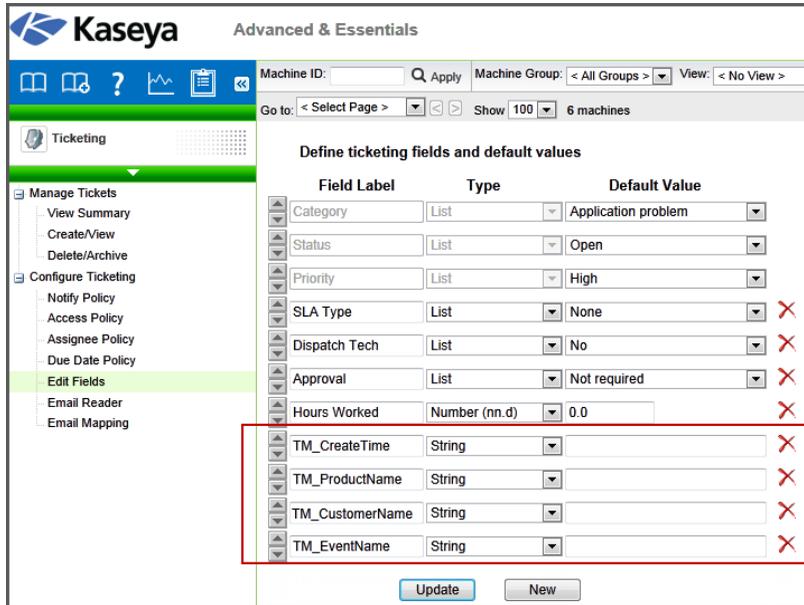


FIGURE 4-11. Champs de tickets Kaseya

2. Vérifiez que le paramètre d'e-mail est correct comme sur l'écran suivant :

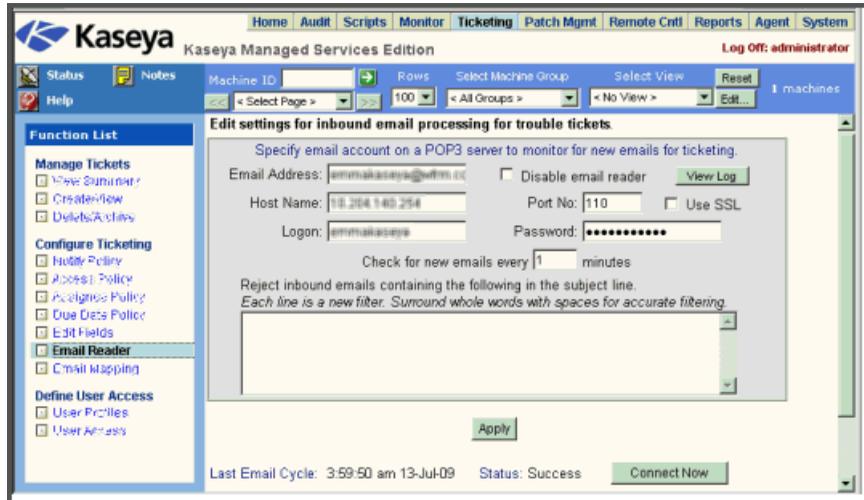


FIGURE 4-12. Paramètres d'e-mail Kaseya

Lorsqu'un événement est déclenché, Kaseya reçoit le ticket :

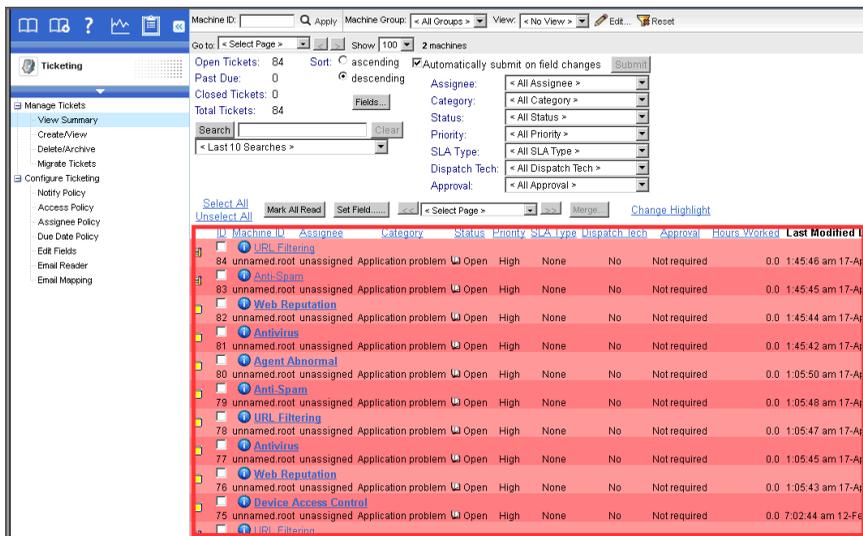


FIGURE 4-13. Ticket d'événement Kaseya

Intégration de ConnectWise™

Configurez les paramètres suivants pour intégrer ConnectWise™ à Remote Manager :

Configuration des paramètres généraux de ConnectWise dans Remote Manager

Procédure

1. Accédez à **Administration > Configurer l'intégration de tiers.**

La fenêtre **Intégration de tiers** s'ouvre.

ConnectWise

Activer l'intégration

URL ConnectWise :

ID de la société :

ID de connexion :

Mot de passe de connexion :

Envoyer les informations de facturation relatives à tous les produits à ConnectWise chaque mois le

Envoyer les informations HES (Hosted Email Security) sur la détection de messages de spam/d'e-mails infectés par un virus à ConnectWise chaque

FIGURE 4-14. Zone du groupe des notifications des informations sur le compte

2. Mettez à jour les options suivantes :
 - **Activer l'intégration ConnectWise** : Cochez la case pour activer l'intégration de Trend Micro Remote Manager et de ConnectWise.
 - **URL ConnectWise** : saisissez l'URL du service.
 - **ID de la société**
 - **ID de connexion** : compte utilisé pour se connecter à ConnectWise.
 - **Mot de passe de connexion** : mot de passe associé au compte.
 - Sélectionnez la fréquence à laquelle Remote Manager doit envoyer les informations de facturation.
 - Sélectionnez la fréquence à laquelle Remote Manager doit envoyer des statistiques de spam.
3. Cliquez sur **Enregistrer**.

Configuration des paramètres ConnectWise spécifiques au client dans Remote Manager

Configurez les paramètres ConnectWise de chaque client. Ces paramètres sont facultatifs. Toutefois, si vous souhaitez recevoir les notifications spécifiques à certains clients, vous devez activer cette fonction.

Procédure

1. Accédez à **Clients (onglet) > {client} > ConnectWise (onglet, panneau de droite)**.

2. Sélectionnez **Activer l'intégration**.
3. Spécifiez un **ID de société** valide qui existe dans ConnectWise.



Remarque

Vous pouvez cliquer sur **Tester la validité** pour vérifier l'ID de la société si vous n'êtes pas sûr de l'orthographe.

4. Sélectionnez les paramètres d'intégration.

- Utilisez les paramètres par défaut sous **Administration**.
 - Spécifiez vos propres options de facturation et de récapitulatif d'exécution.
5. Cliquez sur **Enregistrer**.
 6. Accédez à **Clients (onglet) > {client} > Notification (onglet, panneau de droite)**.
 7. Configurez les paramètres de notification de ce client.
 8. Dans les destinataires, sélectionnez **ConnectWise**.
 9. Cliquez sur **Enregistrer**.

Configuration des paramètres de ConnectWise

Procédure

1. Connectez-vous à ConnectWise à l'aide de l'outil PSA (Professional services automation).
2. Générez une nouvelle carte de service.

Cette étape est facultative. Cependant, elle vous permettra de filtrer plus efficacement les résultats renvoyés par Trend Micro Remote Manager.

- a. Accédez à **Setup (Configuration) > Setup Table (Table de configuration) > Rechercher**, puis saisissez **Service Board**.



- b. Cliquez sur **Service Board (Carte de service)**.
Une liste des cartes de service apparaît.
- c. Cliquez sur l'icône Nouveau pour créer une nouvelle carte de service.

L'écran New service board (Nouvelle carte de service) s'affiche.

- d. Mettez à jour les champs **Board Name (Nom de carte)**, **Emplacement**, **Business Unit (Unité commerciale)** et **Sign Off Template (Modèle de validation)**. Tous les autres champs sont facultatifs.

The screenshot displays the 'Service Board' configuration page. At the top, there are navigation tabs: 'Board', 'Statuses', 'Types', 'Sub Types', 'Items', 'Auto Templates', 'Teams', 'Codes', and 'Auto Assign'. Below the tabs, there's a status bar indicating the last update: 'Updated: 2012/5/15 10:10:41 by admin1'. The main configuration area is divided into several sections:

- Board Information:** Includes fields for 'Board Name' (RM event notification), 'Location' (Tampa Office), 'Business Unit' (Admin), 'Inactive' checkbox, 'Board Icon' (with a 'Browse' button), and 'Signoff Template' (Default Signoff Template).
- Ticket Finance Defaults and Billing Override Options:** Contains dropdowns for 'Work Role', 'Work Type', 'Bill Time?' (No Default), 'Bill Expenses?' (No Default), and 'Bill Products?' (Do Not Bill). It also has a 'Billing Override Options' section with checkboxes for 'Override Billing Setup for Board Location?', 'Bill each service ticket separately.', 'Bill service tickets only after they have been closed.', and 'Bill unapproved time and expense records.'
- Time Entry and Closed Loop / Automatic Email Options:** Includes 'Time Entry Options' (checkboxes for 'Ticket Detail Description', 'Ticket Internal Analysis', 'Ticket Resolution'), 'Automatic Email Options' (fields for 'Sent From', 'Display Name', and 'Send To'), and 'Closed Loop Options' (checkboxes for 'Time Entry option cannot be changed', 'Detail Description cannot be updated directly', and 'Turn on Closed Loop features for the following:' with sub-options for 'Updates to Detail Description', 'Updates to Internal Analysis', and 'Updates to Resolution').

- e. Cliquez sur **Enregistrer**.
 - f. Cliquez sur l'onglet **Statuses (États)**.
 - g. Cliquez sur l'icône Nouveau pour créer un nouveau service d'état.
 - h. Mettez à jour les champs **État à Description**, **Ordre de tri**, puis cochez la case **Display on Board (Afficher sur la carte)**.
 - i. Cliquez sur **Enregistrer**.
3. Affectez des droits à l'utilisateur.

- a. Accédez à **Setup (Configuration) > Setup Table (Table de configuration) > Rechercher**, puis saisissez **Integrator Login**.
 - b. Cliquez sur **Integrator Login (Connexion à l'intégrateur)** puis cliquez sur l'icône Nouveau pour créer un nouveau compte de connexion.

L'écran **Général** s'affiche.
 - c. Dans **Access Levels (Niveaux d'accès)**, cliquez sur **All records (Tous les enregistrements)**.
 - d. Vérifiez les options suivantes : **Service Ticket API (API de ticket de service)**, **Management Services API (API des services de gestion)**, **Company API (API de la société)**, **System API (API système)** et **Configuration API (API de configuration)**.
 - e. Sélectionnez la carte de service que vous avez créée, mettez à jour le champ **URL de rappel de ticket** sur **www.example.com** ou toute autre URL arbitraire, puis cliquez sur **Enregistrer**.
 - f. Cliquez sur **Enregistrer**.
4. Générez une nouvelle solution de gestion.
- a. Accédez à **Setup (Configuration) > Setup Table (Table de configuration) > Rechercher**, puis saisissez **Management IT**.
 - b. Cliquez sur **Management IT (Informatique de gestion)**.
 - c. Cliquez sur l'icône Nouveau pour créer une nouvelle solution de gestion.
 - d. Mettez à jour **Nom** sur **TMRM Management Setup, Solution informatique de gestion** sur **Custom** et **Nom de la solution personnalisée** sur **TMRM Management Solution**.

L'utilisation d'autres valeurs peut interrompre la connexion.
 - e. Cliquez sur **Enregistrer**.
5. Modifiez l'état par défaut de la société sur **Actif**.
- a. Accédez à **Setup (Configuration) > Setup Table (Table de configuration) > Rechercher**, puis saisissez **Company Status**.

- b. Cliquez sur **Company Status (État de la société)**.
 - c. Cliquez sur **Actif**.
 - d. Sélectionnez **Default Flag (Indicateur par défaut)**.
 - e. Cliquez sur **Enregistrer**.
6. Générez un nouveau service pour chaque produit ou service Remote Manager géré.
- a. Accédez à **Configuration > Produits > Nouveau**.
 - b. Mettez à jour l'**ID de produit** sur un produit ou un service géré. Choisissez parmi **HES/WFBS-SVC/WFBS-S/WFBS-A**.
 - c. Si besoin, mettez à jour les prix.
 - d. Cliquez sur **Enregistrer**.
- Répétez ces étapes pour chaque produit ou service géré.
7. Générez des références croisées pour chaque produit ou service Remote Manager géré.
- a. Accédez à **Configuration > Table de configuration > Rechercher**, puis saisissez **Managed Devices Integration**.
 - b. Cliquez sur **Managed Devices Integration (Intégration au périphérique géré)**.
 - c. Sélectionnez la solution de gestion appelée « **Solution de gestion Remote Manager** ».
 - d. Cliquez sur l'onglet **Référence croisée > Nouveau**.
 - e. Si nécessaire, mettez à jour les champs.
- Paramètres des produits ou services Remote Manager gérés.

PRODUIT/SERVICE	PARAMÈTRES
Worry-Free Business Security Standard	<ul style="list-style-type: none"> • Type : T-WFBS-S • Niveau : Standard • Agreement Type (Type de contrat) : Managed Service • Produit : WFBS-S • Configuration Type (Type de configuration) : Spam Stats
Worry-Free Business Security Advanced	<ul style="list-style-type: none"> • Type : T-WFBS-A • Niveau : Advanced • Agreement Type (Type de contrat) : Managed Service • Produit : WFBS-A • Configuration Type (Type de configuration) : Spam Stats
Worry-Free Business Security Services	<ul style="list-style-type: none"> • Type : T-WFBSS • Niveau : Standard • Agreement Type (Type de contrat) : Managed Service • Produit : WFBSS • Configuration Type (Type de configuration) : Spam Stats
Hosted Email Security	<ul style="list-style-type: none"> • Type : T-HES • Niveau : Standard • Agreement Type (Type de contrat) : Managed Service • Produit : HES • Configuration Type (Type de configuration) : Spam Stats

- f. Cliquez sur **Enregistrer**.
8. Générez une nouvelle société pour chaque client à intégrer à ConnectWise.
 - a. Accédez à **Contacts > Société > Nouveau**.
 - b. Mettez à jour l'**ID de la société**.

Trend Micro recommande d'utiliser le nom de client Remote Manager en tant qu'ID de société ConnectWise.
 - c. Cliquez sur **Enregistrer**.

Répétez ces étapes pour générer une société pour chaque client.
9. Générez une nouvelle solution de gestion pour chaque société
 - a. Cliquez sur l'onglet **Gestion**.
 - b. Cliquez sur **Enregistrer**.
 - c. Cliquez sur **Nouvel élément**.
 - d. Mettez à jour **Solution** sur **Remote Manager Management Solution**.
 - e. Mettez le champ **ID géré** à jour en sélectionnant l'ID de la société précisée à l'étape précédente.
 - f. Cliquez sur **Enregistrer**.
10. Générez des configurations pour chaque société.
 - a. Cliquez sur l'onglet **Configuration**.
 - b. Générez une nouvelle configuration avec **Type de configuration** défini sur **Spam Stats** et **Nom** défini pour utiliser l'ID de la société.
 - c. Cliquez sur **Enregistrer**.
11. Générez un nouveau contrat pour chaque client à intégrer à ConnectWise.
 - a. Accédez à **Contrats (onglet) > Nouveau**.
 - b. Sélectionnez **Service géré** comme **Type de contrat** et mettez à jour les autres informations requises.

Company Search ► Company ► Agreement Maintenance

RM agreement

Agreement | Additions | Adjustments | Agreements | Work Roles | Work Types | Sites | Invoice | Service | Time | Expense | Product | Co

Updated: 2012/5/17 1:33:49 by admin1

Agreement Type: Managed Service
 Agreement Name: RM agreement
 Company: RM trendmicro
 Contact: trendmicroRM
 Purchase Order:
 Location: Tampa Office Restrict:
 Business Unit: Sales Restrict:
 Start Date: 14/05/2012
 End Date: or No Ending Date
 Cancelled:
 Date Cancelled:
 Reason:
 SLA: Standard SLA

Application Recap		Invoicing Recap	
Starting:	0.00	Last Inv Date:	
Adjustments:	0.00	Last Inv #:	
Used:	0.00	Last Inv Amt:	
Remaining:	0.00	Next Inv Date:	2012/3/1
Overrun:	0.00	Next Inv Amt:	0.00
Available:	0.00	Unbilled Overage	0.00

Opportunity:
 Sub-contractor Information
 Company: RM trendmicro
 Contact: trendmicro RM
 Work Order:

Internal Notes

c. Cliquez sur **Enregistrer**.

12. Incluez des compléments à introduire dans le contrat.

a. Accédez à **Agreements (Contrats) > Additions (Compléments)**.

b. Si nécessaire, mettez à jour les champs.

Par exemple, mettez à jour le prix et le numéro de série.



Important

Le numéro de série doit respecter le format `SerialNumber` :
`Serial_Company ID`.

The screenshot shows the 'WFRM' Agreement Maintenance interface. The breadcrumb trail is 'Company Search > Company > Agreement Maintenance'. The main title is 'WFRM'. Below the title are tabs for 'Agreement', 'Additions', 'Adjustments', 'Agreements', 'Work Roles', 'Work Types', 'Sites', 'Invoice', and 'Service'. A status bar indicates 'Updated: 2012/3/28 10:49:12 by admin1'. The main form contains the following fields:

Product:	WFBSS
Description:	Worry-Free Business Security Services
Total Quantity:	500
Less Included:	400
Quantity to Bill:	100
Unit Price:	7.70
Unit Cost:	7.00
Effective Date:	03/04/21
Cancelled Date:	30/08/21
Bill Customer?	<input checked="" type="checkbox"/>
Taxable?	<input type="checkbox"/>
UOM:	User-based
Ext. Price:	770.00
Ext. Cost:	3500.00
Margin:	-2730.00
SerialNumber:	Serial_RM trendmi

Invoice Description: Customers

c. Cliquez sur **Enregistrer**.

Répétez ces étapes pour chaque produit ou service géré.

Chapitre 5

Gestion des clients

Cette section contient la rubrique suivante :

- *Clients à la page 5-2*

Clients

La page **Clients** vous permet de vérifier les informations sur vos clients et sur les licences. Vous pouvez également effectuer les actions suivantes :

- Cliquer sur le nom de chaque client afin d'obtenir des informations plus détaillées sur ce client
- Filtrer la liste des clients
- Exporter les informations sur les clients dans un fichier `csv`
- Ajouter de nouveaux clients
- Renouveler des licences
- Gérer des produits

Ajout de nouveaux clients

Procédure

- Pour les comptes Licensing Management Platform :
 1. Accédez à **Clients** > {nom du client} > **Produits (onglet)** > **Ajouter**.

Nouveau client

Affecter le plan de service à testrmx

Plan de service : BSS_Monthly_noautorenew_RM_FULL
Full CE
trial CE

Date de début :* 16/04/2014

Unités par licence :* 50 sièges

< Précédent Suivant > Terminé Annuler

2. Sélectionnez le plan de service, la date de début et le nombre d'unités par licence.
3. Cliquez sur **Suivant**.
4. Configurez les paramètres par défaut pour le produit. Vous pouvez choisir l'une des options suivantes :

**Remarque**

Cette fonction ne s'affiche que si vous avez sélectionné Worry-Free Business Security Services.

Affecter le plan de service [X]

Configurer les paramètres par défaut du produit

De base Modèles

Liste Approuvé pour la réputation de sites Web et le filtrage des URL ⓘ

Incluez HTTP:// ou HTTPS:// lors de l'ajout d'URL. [Ajouter]

http://www.trendmicro.com/* [Supprimer]
 http://wustat.windows.com/*
 http://windowsupdate.microsoft.com/*
 http://uk.trendmicro-europe.com/*

Liste Bloqué pour le filtrage des URL ⓘ

Incluez HTTP:// ou HTTPS:// lors de l'ajout d'URL. [Ajouter]

[Supprimer]

Activer le scan programmé pour le serveur

Quotidien
 Hebdomadaire
 Mensuel

Chaque : Lundi [v]
 Heure de début : 12 : 30
 hh mm

Activer le scan programmé pour l'appareil

Utiliser les paramètres du serveur
 Utiliser ces paramètres :

Quotidien
 Hebdomadaire
 Mensuel

Chaque : Lundi [v]
 Heure de début : 12 : 30
 hh mm

[< Précédent] Terminé Annuler

- **De base** : configurez uniquement les paramètres affichés.
- Liste Approuvé pour la réputation de sites Web et le filtrage des URL



Remarque

Si vous ajoutez une URL à la liste Approuvé, vérifiez qu'elle n'a pas été ajoutée à la liste Bloqué et inversement.

- Liste Bloqué pour le filtrage des URL
 - Scan programmé pour le serveur et dispositif
 - **Modèles** : Accédez à **Administration** > **Configurer les modèles de paramètres par défaut**, afin de configurer plus de paramètres en utilisant une console similaire à Worry-Free Business Security.
5. Cliquez sur **Terminé**.

Le produit/service est ajouté et les détails de l'ajout s'affichent.



Remarque

Notez le GUID ou la clé d'enregistrement.

6. Cliquez sur **Se connecter** pour obtenir des informations sur la méthode de connexion du produit ou du service à la console.
- Pour les autres comptes :
 1. Cliquez sur **Nouveau client** sur la bannière ou sélectionnez **Clients** > **Nouveau client**. Une page Nouveau client s'affiche.

2. Saisissez les informations demandées.
3. Cliquez sur **Suivant >**.
4. Sélectionnez le type de produit et saisissez une description de produit.

5. Cliquez sur **Terminé**.

Association de comptes

Si vous gérez d'autres comptes Trend Micro Remote Manager qui n'ont pas migré vers la nouvelle version de Licensing Management Platform, vous pouvez fusionner ces comptes avec le compte actuel.

Procédure

1. Connectez-vous à un compte Remote Manager qui a été migré vers Licensing Management Platform.

L'écran **Tableau de bord** s'ouvre.



2. Cliquez sur la flèche qui se trouve à côté du nom de connexion et cliquez sur **Fusionner un autre compte > Continuer**.

**AVERTISSEMENT!**

Si vous fusionnez un compte avec le compte actuel, toutes les données enregistrées sur l'autre compte seront transférées vers le compte actuel. Par exemple, si vous êtes actuellement connecté en tant que `admin1` et que vous fusionnez les comptes `admin2` et `admin1`, toutes les données du compte `admin2` seront supprimées du compte `admin2`. Ces données ont été fusionnées avec le compte `admin1`. Vous pourrez toujours ouvrir le compte `admin2` mais toutes les données concernant ce compte se trouveront dans le compte `admin1`.

3. Entrez le nom d'utilisateur et le mot de passe du compte que vous voulez fusionner avec le compte actuel.
4. Cliquez sur **Fusionner**.

Attendez quelques minutes afin que les données puissent fusionner.

Que faire ensuite

Une fois la migration du compte terminée, vous verrez systématiquement les éléments suivants lors de l'ajout d'un nouveau client :

Nouveau client

Sélectionner le type de client

Avec un compte Licensing Management Platform actif

Avec les serveurs de produit existants qui doivent se connecter à ce compte

Suivant > Annuler

- **Avec un compte Licensing Management Platform actif** : si le nouveau client a déjà un compte dans Licensing Management Platform.
- **Avec les serveurs de produit existants qui doivent se connecter à ce compte** : si le nouveau client a un produit/service et si le compte n'a pas été intégré dans Licensing Management Platform.

Vérification de la licence du produit

Vérifiez régulièrement les licences des produits des serveurs gérés de vos clients pour assurer une protection continue.

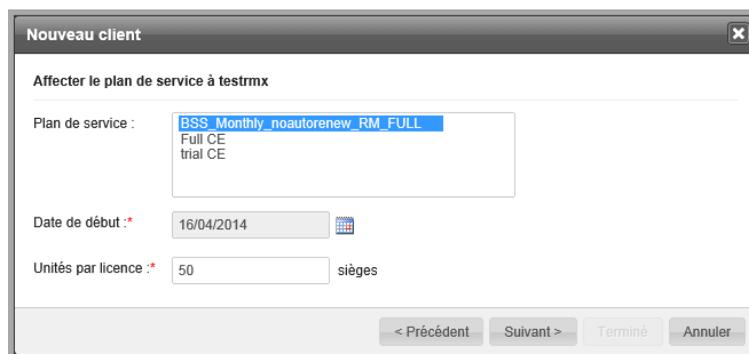
Procédure

1. Cliquez sur **Clients** > {client} > {produit} > **Licence (onglet)**.
 2. Vérifiez les informations concernant la licence de votre produit.
-

Ajout de produits/services

Procédure

1. Accédez à **Clients** > {nom du client} > **Produits (onglet)** > **Ajouter**.
 - Pour les comptes Licensing Management Platform :
 - a. Sélectionnez le plan de service, la date de début et le nombre d'unités par licence.



The screenshot shows a dialog box titled "Nouveau client" with a close button in the top right corner. The main heading is "Affecter le plan de service à testrmx". Below this, there are three input fields: "Plan de service :" with a dropdown menu showing "BSS_Monthly_noautorenew_RM_FULL", "Full CE", and "trial CE"; "Date de début :*" with a text box containing "16/04/2014" and a calendar icon; and "Unités par licence :*" with a text box containing "50" and the label "sièges". At the bottom, there are four buttons: "< Précédent", "Suivant >", "Terminé", and "Annuler".

- b. Ajoutez le produit ou le service.
Le produit/service est ajouté et les détails de l'ajout s'affichent.

- c. Cliquez sur **Terminé**.
- Si vous utilisez un compte qui a été intégré à Trend Micro Licensing Management Platform :
 - a. Sélectionnez le type de produit et saisissez une description de produit.



Ajouter produit

Type de produit :*

Description du produit :*

Utilisez 20 caractères alphanumériques au maximum.

Terminé Annuler

- b. Cliquez sur **Terminé**.
 - c. Notez le GUID ou la clé d'enregistrement. Vous en aurez besoin pour [enregistrer vos produits à la page 4-8](#).
-

Contacts

Si votre compte est associé à Licensing Management Platform, vous pouvez ajouter des contacts, modifier les renseignements sur les clients ou supprimer des contacts à partir de Licensing Management Platform. Pour cela, cliquez sur le lien **Licensing Management Platform** au-dessus de **Déconnexion**. Si ce lien n'est pas affiché, cela signifie que vous ne pouvez voir les informations sur les contacts qu'à partir de la console Web Remote Manager.

Ajout de contacts

Pour pouvoir s'abonner aux notifications d'événements et aux rapports, les utilisateurs de l'organisation de votre client doivent d'abord être ajoutés en tant que contacts.

**Remarque**

Si votre compte est associé à Licensing Management Platform, cliquez sur le lien **Licensing Management Platform** au-dessus de **Déconnexion** pour ajouter des contacts. Si ce lien n'est pas affiché, cela signifie que vous ne pouvez voir les informations sur les contacts qu'à partir de la console Web Remote Manager.

Procédure

1. Accédez à **Clients** > {client} > **Contact (onglet)**.
 2. Cliquez sur **Ajouter**.
 3. Dans **Ajouter un contact**, renseignez les informations suivantes :
 - Nom du contact
 - Numéro de téléphone
 - Code postal
 - **Adresse électronique** : Remote Manager enverra les notifications d'événements et les rapports à cette adresse.
 - Autre
 4. Cliquez sur **Enregistrer**.
-

Modification des informations client

Les onglets **Profil de la société** et **Contact** vous permettent de modifier les informations client.

**Remarque**

Si votre compte est associé à Licensing Management Platform, cliquez sur le lien **Licensing Management Platform** au-dessus de **Déconnexion** pour modifier les informations sur les contacts. Si ce lien n'est pas affiché, cela signifie que vous ne pouvez voir les informations sur les contacts qu'à partir de la console Web Remote Manager.

Procédure

1. Accédez à **Clients** > {client} > **Profil de la société (onglet)**.
2. Mettez à jour les informations concernant la société.



Remarque

Vous pouvez également modifier le logo que les clients verront lorsqu'ils se connecteront à la console Web Remote Manager.

3. Accédez à **Clients** > {client} > **Contact (onglet)**.
 4. Mettez à jour les informations des contacts.
 5. Cliquez sur **Enregistrer**.
-

Suppression de contacts

Les clients peuvent s'abonner aux notifications et rapports en tant que contacts. Il arrive cependant que les contacts changent et que certains contacts doivent être retirés de la liste des destinataires.



Remarque

Si votre compte est associé à Licensing Management Platform, cliquez sur le lien **Licensing Management Platform** au-dessus de **Déconnexion** pour modifier les informations sur les contacts. Si ce lien n'est pas affiché, cela signifie que vous ne pouvez voir les informations sur les contacts qu'à partir de la console Web Remote Manager.

Procédure

1. Accédez à **Clients** > {client} > **Contact (onglet)**.
 2. Sélectionnez le contact à supprimer.
 3. Cliquez sur **Supprimer**.
-

Suppression de clients

Si vous supprimez un produit ou un service, tous les enregistrements associés seront supprimés. Pour réenregistrer le produit ou le service auprès du serveur Trend Micro Remote Manager, vous devez créer un GUID pour ce client. Vous devrez également réinstaller l'agent Remote Manager sur le produit géré et utiliser le nouveau GUID.



Remarque

Cette fonction s'applique uniquement aux comptes qui n'ont pas été intégrés à Licensing Management Platform.

Procédure

1. Supprimez tous les produits/services associés pour ce client.
 - a. Cliquez sur **Clients** > {client}.
 - b. Sélectionnez tous les produits ou services dans l'onglet **Produit**.
 - c. Cliquez sur **Supprimer**.
2. Supprimez un ou plusieurs clients.
 - a. Cliquez sur **Clients**.
 - b. Sélectionnez les clients dans la liste.



Remarque

Sélectionnez uniquement les clients qui n'ont pas de produits, ni de services.

- c. Cliquez sur **Supprimer**.
-

Filtrage de la liste des clients

La longueur de la liste des clients dépend du nombre de vos clients. Pour accéder aux informations dont vous avez besoin, vous pouvez affiner le nombre de clients et afficher uniquement ceux qui correspondent au profil que vous avez défini.

Procédure

1. À partir de la console Web Remote Manager, cliquez sur **Clients**.

Tous vos clients s'affichent sur cette page.

2. Dans la partie droite, sélectionnez un ou plusieurs champs.



Remarque

Si vous sélectionnez plus d'un (1) champ, vous accédez peut-être correctement aux informations précises dont vous avez besoin. Cependant, vous risquez également d'avoir éliminé des informations nécessaires : sélectionnez donc ces champs avec soin.

3. (Facultatif) Cliquez sur **Exporter** pour générer un fichier CSV de vos clients filtrés.
-

Chapitre 6

Gestion des agents

Cette section contient les rubriques suivantes :

- *Gestion des agents à partir de la console Web Remote Manager à la page 6-2*
- *Gestion des agents à partir du serveur géré à la page 6-6*
- *Suppression d'agents à la page 6-14*

Gestion des agents à partir de la console Web Remote Manager

Cette section contient des informations sur la gestion des agents à partir de la console Web Trend Micro™ Remote Manager™.

Vérification de la connexion entre l'agent et le serveur

Pour vérifier que le service Trend Micro Remote Manager s'exécute correctement, assurez-vous que les agents s'affichent à l'état « Connecté » ou « En ligne » sur la console Web Remote Manager.

Accédez à **Clients** > {client} > **Produits (onglet)**.

L'arborescence répertorie l'état de chaque agent dans la colonne **État**. Pour obtenir des détails sur chaque état, voir [État de l'agent à la page 6-2](#)

En plus de la section en cours, consultez [Dépannage et problèmes connus à la page 11-1](#) pour d'autres problèmes de connectivité serveur/agent.

État de l'agent

L'état d'un agent Remote Manager indique si celui-ci est capable de collecter des données et de recevoir des commandes à partir du serveur Remote Manager. L'état indique également la raison pour laquelle l'agent ne fonctionne pas correctement et la façon de gérer la situation. Le tableau ci-dessous décrit les différents types d'états de l'agent et la façon de gérer la situation.

TABLEAU 6-1. Types d'états de l'agent

ÉTAT	DESCRIPTION	RÉSOLUTION
En ligne	L'agent s'exécute normalement.	N/A

ÉTAT	DESCRIPTION	RÉSOLUTION
Anormal	L'agent apparaît hors ligne et ne répond pas au serveur Remote Manager, mais n'a pas envoyé de demande de déconnexion.	Cet état survient si le serveur géré ne s'est pas éteint correctement. Vérifiez que l'administrateur du serveur géré connaît la situation. Contactez-le si nécessaire.
Désactivé	Cet état est défini manuellement au moyen de la console. Lorsqu'un agent est à l'état désactivé, il demande des commandes au serveur toutes les 10 minutes.	Envoyez une commande pour activer l'agent (voir Envoyer des commandes d'agent à la page 6-4).
Hors ligne	L'agent s'est fermé normalement après avoir envoyé une demande de déconnexion au serveur Remote Manager. Généralement, un agent présente cet état si un utilisateur a éteint le service d'agent ou si le serveur géré a été éteint.	Vérifiez que l'administrateur du serveur géré sait que le serveur s'est arrêté. Contactez-le si nécessaire.
Inconnu	L'agent ne fonctionne pas normalement.	Supprimez l'agent et demandez à l'administrateur du serveur géré de réinstaller l'agent. Si ce problème persiste, contactez votre service d'assistance.
Erreurs de plug-in	La console a détecté des erreurs au niveau du composant de plug-in du service de l'agent.	Supprimez l'agent et demandez à l'administrateur du serveur géré de le réinstaller. Si ce problème persiste, contactez votre service d'assistance.
Non enregistré	L'agent ne s'est pas enregistré auprès du serveur Remote Manager.	L'agent n'a peut-être pas été installé correctement ou n'a peut-être pas pu communiquer avec le serveur Remote Manager. Contactez l'administrateur du serveur géré.

ÉTAT	DESCRIPTION	RÉSOLUTION
Version non compatible	<p>Une incompatibilité a été détectée entre les versions de l'un des composants suivants :</p> <ul style="list-style-type: none"> • Agent • Remote Manager • Worry-Free Business Security (Standard et Advanced) 	Effectuez une mise à niveau de l'agent et du serveur géré. Si le problème persiste, rappez-le à l'administrateur du centre de données de Trend Micro.

Envoi des commandes d'agents

Les commandes d'agents vous permettent de résoudre à distance des problèmes affectant l'agent Worry-Free Business Security (Standard et Advanced). Si un agent se trouve dans l'état anormal ou non enregistré, vous ne pouvez pas lui envoyer une commande.

Procédure

1. Sélectionnez **Clients > {clients} > {produit} > Groupes (onglet)**.

Sélectionnez l'une des commandes suivantes :

- **Scan immédiat** : permet de lancer un scan du terminal.
- **Arrêter le scan** : permet d'arrêter la procédure de scan.

2. Sélectionnez **Clients > {clients} > {produit} > Paramètres de domaine (onglet)**.

Sélectionnez l'une des commandes suivantes :

- **Activer** : restaure l'état de l'agent, qui passe de désactivé à un fonctionnement normal.
- **Désactiver** : l'agent cesse de collecter des informations, mais continue de demander des commandes au serveur toutes les 10 minutes.
- **Démarrer l'évaluation des failles** : permet d'effectuer un scan d'évaluation des failles.

- **Démarrer Damage Cleanup Services** : permet d'effectuer un scan de l'ordinateur et d'en supprimer les virus de fichier et de réseau, ainsi que les résidus de virus et de vers.
3. Sélectionnez **Clients > {clients} > {produit} > Serveur géré (onglet)**.
- Sélectionnez l'une des commandes suivantes :
- **Mise à jour du serveur géré** : permet de télécharger et installer les mises à jour du serveur géré.
 - **Mise à jour de Security Agent** : permet de télécharger et installer les mises à jour de l'agent.

Affichage des détails relatifs à l'agent

Procédure

1. Accédez à **Clients > {client} > Produits (onglet) > WFBS-S/WFBS-A > Terminaux**.

Les informations suivantes s'affichent :

- **État**
- **Nom**
- **GUID** : Identificateur global unique ; Remote Manager génère automatiquement cette chaîne. Fournit le GUID à l'administrateur qui installera le programme agent.
- **Adresse IP** : adresse IP du serveur sur lequel l'agent est installé
- **Enregistré le**
- **Dernière mise à jour** : date et heure de la dernière mise à jour de l'agent
- **Version de l'agent**
- **Produit géré** : produit géré par l'agent

- **Version du produit géré** : version du produit géré par l'agent

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 6-2. Icônes de la barre d'état système

ICÔNE	DESCRIPTION
	Une icône verte indique que l'agent est connecté au serveur de communication Remote Manager. L'agent fonctionne normalement.
	Une icône rouge indique que l'agent n'est pas connecté au serveur de communication Remote Manager ou que sa version 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 saisi un identificateur global unique (GUID) incorrect au cours de l'installation de l'agent Remote Manager, supprimez l'agent et installez-le à nouveau en utilisant le GUID approprié. S'il vous est impossible de suivre cette procédure, vous pouvez effectuer les opérations suivantes :

Procédure

1. Accédez à `C:\Program Files\Trend Micro\TMRMAgentForCSM`.

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 d'agent Trend Micro Remote Manager de 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'apporter des modifications aux paramètres de configuration de l'agent Remote Manager.

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 6-8*.

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 :



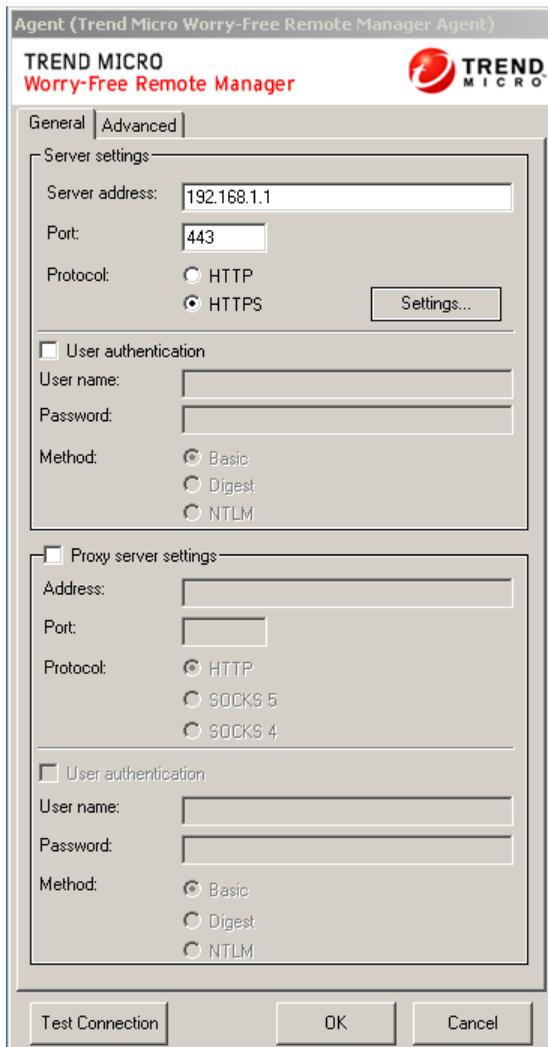
FIGURE 6-1. Menu contextuel de l'outil de configuration de l'agent

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** : Le fait de quitter l'outil 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.



The image shows a configuration dialog box titled "Agent (Trend Micro Worry-Free Remote Manager Agent)". The dialog has two tabs: "General" (selected) and "Advanced". The "General" tab contains the following sections:

- Server settings:**
 - Server address: 192.168.1.1
 - Port: 443
 - Protocol: HTTP, HTTPS
 - Settings... button
- User authentication:
 - User name: [text box]
 - Password: [text box]
 - Method: Basic, Digest, NTLM
- Proxy server settings:
 - Address: [text box]
 - Port: [text box]
 - Protocol: HTTP, SOCKS 5, SOCKS 4
- User authentication (for proxy):
 - User name: [text box]
 - Password: [text box]
 - Method: Basic, Digest, NTLM

At the bottom of the dialog are three buttons: "Test Connection", "OK", and "Cancel".

FIGURE 6-2. 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** : Le nom de domaine complet (FQDN) du serveur Remote Manager de communication. Le FQDN varie dans chaque région, comme suit :
 - **Asie/Pacifique** : `rm-apaca.trendmicro.com`
 - **Europe et Moyen-Orient** : `rm-emea.trendmicro.com`
 - **Japon** : `rm-jpa.trendmicro.com`
 - **Amérique latine** : `rm-lara.trendmicro.com`
 - **Amérique du Nord** : `rm-usa.trendmicro.com`
 - **Port** : port que le serveur Remote Manager utilise 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.
- **Paramètres du serveur proxy** : Activez cette zone en cochant la case **Paramètres du serveur proxy** si le réseau de l'utilisateur requiert 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 **Arrêter le 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\\WFRMAgentforCSM.
 - 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 si vous ne l'avez pas déjà fait. Pour obtenir des instructions détaillées, voir [Suppression des agents localement à la page 6-15](#).



Remarque

Lorsque vous supprimez l'agent localement, il se désenregistre de Remote Manager qui supprime automatiquement toutes les données associées. 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 **Arrêter le 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 **Démarrer le service** pour redémarrer le service d'agent.
-

Recherche du numéro de compilation de l'agent

Vous pouvez vérifier le numéro de compilation de l'agent à partir de la console ou directement, sur l'agent.

À partir de la console Web Remote Manager

Procédure

1. Cliquez sur l'onglet **Clients**.
 2. Sélectionnez le domaine cible dans la liste déroulante **Afficher par** du panneau de gauche.
 3. Cliquez sur **Tous les clients** > {client} > {agent} > **Détails du serveur/de l'agent** > **Détails de TMRM Agent**.
 4. Vérifiez la version de l'agent dans le tableau **Généralités**.
-

Sur l'agent

Procédure

1. Accédez au répertoire `C:\Program Files\Trend Micro\WFRMAgentForCSM`.
 2. Cliquez avec le bouton droit sur le fichier `csmpugin.dll`, puis cliquez sur **Propriétés** > **Version (onglet)** pour voir le numéro de compilation.
-

Emplacement des journaux de l'agent et des fichiers de configuration

Les fichiers de configuration de l'agent se trouvent dans :

- `<chemin d'installation>\Trend Micro\WFRMAgentForCSM*.xml`
- `<chemin d'installation>\Trend Micro\WFRMAgentForCSM*.ini`

Les fichiers journaux se trouvent dans :

- `<chemin d'installation>\Trend Micro\WFRMAgentForCSM\log\`

Activation du journal de débogage de l'agent

Normalement, l'agent enregistrera uniquement les informations d'avertissement et d'erreur. Pour obtenir des informations de journal plus détaillées, activez le journal de débogage de l'agent.

Résolution

1. Ouvrez le fichier `AgentLocalConfig.xml` dans le répertoire `<install path>\Trend Micro\WFRMAgentForCSM\` au moyen d'un éditeur de texte.
2. Modifiez la valeur `<DebugLogLevel>` de `LL_FOR_ERROR` sur `LL_FOR_ALL`.
3. Redémarrez le service d'agent en cliquant avec le bouton droit de la souris sur l'agent Remote Manager dans la barre des tâches, puis en cliquant sur **Redémarrer le service**.
4. Le fichier journal de l'agent est `<install path>\Trend Micro\WFRMAgentForCSM\log\TMICAgent.log`.

Suppression d'agents

Cette section contient des informations sur la suppression des agents.

Suppression des agents localement

Avant de supprimer un agent, consultez [Sauvegarde et restauration des paramètres de l'agent à la page 6-11](#).



AVERTISSEMENT!

L'annulation de l'enregistrement d'un agent depuis Remote Manager supprime toutes les données associées à l'agent Remote Manager. Pour éviter cette annulation (et la suppression des données), modifiez la valeur de l'adresse du serveur sur l'interface de l'agent Remote Manager avant de supprimer l'agent Remote Manager.

Il existe trois façons de supprimer un agent Remote Manager localement :

- Désinstallation directe de l'agent Remote Manager.
- Désinstallation de l'agent Remote Manager via le Panneau de configuration.
- Désinstallation manuelle de l'agent Remote Manager.

Désinstallation directe de l'agent Remote Manager

Procédure

1. Ouvrez le fichier d'installation de l'agent Remote Manager (WFRMAgentforCSM.exe ou WFRMAgentforWFBS.exe).
2. Cliquez sur **Oui** pour confirmer la boîte de dialogue **Confirmer désinstallation**.



Remarque

Durant la suppression, vous serez invité à fermer certaines applications. Fermez-les et cliquez sur **Réessayer** pour continuer.

3. Cliquez sur **Terminer** pour fermer l'assistant une fois la désinstallation terminée.
-

Désinstallation de l'agent Remote Manager via le Panneau de configuration

Procédure

1. Ouvrez l'applet **Ajout/Suppression de programmes** du Panneau de configuration (ou **Programmes et paramètres** dans Windows Vista™).
 2. Sélectionnez **Agent Trend Micro Remote Manager**, puis cliquez sur le bouton **Modifier/Supprimer**.
 3. Suivez les instructions indiquées à l'écran.
-

Désinstallation manuelle de l'agent Remote Manager

Si, pour une quelconque raison, un agent ne peut être supprimé de manière standard, essayez la procédure suivante :

Procédure

1. Arrêtez le service d'agent Remote Manager.
 - a. Accédez à **Démarrer > Exécuter**.
 - b. Saisissez `cmd` dans la ligne de commande et appuyez sur **Entrée**.
 - c. Exécutez la commande suivante :

```
net stop Trend Micro Worry-Free Remote Manager Agent
```
2. Supprimez le service d'agent Remote Manager :
 - a. Sur la ligne de commande, utilisez la commande de changement de répertoire (`cd`) pour accéder au répertoire de l'agent Remote Manager.
 - b. Exécutez la commande suivante :

```
TMICAgent -u
```
3. Supprimez les fichiers programme.

```
Delete {Agent install directory} / WFRMAgentForCSM
```

4. Ouvrez l'éditeur du registre (regedit.exe) et supprimez les clés de registre suivantes :



Remarque

créez toujours une sauvegarde avant de modifier le registre. En effet, des modifications incorrectes du registre peuvent entraîner de graves problèmes. Si cela devait arriver, vous pourriez alors le restaurer en vous reportant à la rubrique d'aide « Restauration du registre » dans regedit.exe ou à la rubrique d'aide « Restauration d'une clé de registre » dans regedt32.exe.

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMIC4CSM\Agent\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products\23FC8F347B51DD440AD13A73D13A73D22D58E6
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\23FC8F347B51DD440AD13A73D13A73D22D58E6
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{43F8CF32-15B7-44DD-A01D-A3372DD2856E}
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\InstallShield Uninstall Information\{43F8CF32-15B7-44DD-A01D-A3372DD2856E}
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\InstallShield_\{43F8CF32-15B7-44DD-A01D-A3372DD2856E}
5. Supprimez le raccourci de l'agent Remote Manager dans le menu Démarrer.
 - a. Sur le Bureau, cliquez sur **Poste de travail**.
 - b. Passez du répertoire en cours à ..\Documents and Settings\All Users\Menu Démarrer\Programmes.

- c. Supprimez le dossier de l'agent Remote Manager.
-

Chapitre 7

Gestion des licences

Cette section contient les rubriques suivantes :



Remarque

Cette fonction est applicable uniquement si vous utilisez un compte intégré dans Trend Micro Licensing Management Platform.

- *Ajout de sièges affectés à la page 7-2*
- *Renouvellement de licences à la page 7-2*

Ajout de sièges affectés

Chaque revendeur doit spécifier le nombre de sièges qu'il peut affecter par client. Si ce nombre dépasse le nombre de sièges affectés, les revendeurs peuvent ajouter plus de sièges par client.



Remarque

Cette fonction est applicable uniquement si vous utilisez un compte intégré dans Trend Micro Licensing Management Platform.

Procédure

1. Il y a plusieurs façons de faire apparaître la fenêtre **Ajouter des sièges** :
 - À partir de la console Web Remote Manager™ Trend Micro™ :
 - a. Cliquez sur **Clients**.
 - b. Sélectionnez le client qui a dépassé le nombre de sièges affectés.
 - c. Cliquez sur **Modifier le nombre de sièges**.
 - À partir du widget **Notifications**, cliquez sur le lien **Ajouter des sièges maintenant** qui se trouve à côté de la notification.
 - Dans l'e-mail de notification, cliquez sur le bouton **Ajouter des sièges maintenant**.
 2. Spécifiez le nombre de sièges affectés que vous voulez ajouter.
 3. Cliquez sur **Envoyer**.
-

Renouvellement de licences

Renouvelez les licences pour les clients que vous gérez.

**Remarque**

Cette fonction est applicable uniquement si vous utilisez un compte intégré dans Trend Micro Licensing Management Platform.

Procédure

1. Il y a plusieurs façons de faire apparaître la fenêtre **Renouveler les licences** :
 - À partir de la console WebRemote Manager :
 - a. Cliquez sur **Clients**.
 - b. Sélectionnez le client dont la licence a expiré ou arrivera bientôt à expiration.
 - c. Cliquez sur **Renouveler la licence**.
 - À partir du widget **Notifications**, cliquez sur le lien **Renouveler maintenant** qui se trouve à côté de la notification.
 - Dans l'e-mail de notification, cliquez sur le bouton **Renouveler maintenant**.
 2. Spécifiez les modifications à apporter aux termes de la licence.
 3. Cliquez sur **Envoyer**.
-

Chapitre 8

Gestion des paramètres

Cette section contient les rubriques suivantes :

- *Configuration des notifications à la page 8-2*
- *Configuration des paramètres de console à la page 8-3*
- *Configuration de modèles de paramètres par défaut à la page 8-4*

Configuration des notifications

Configurez des notifications si des événements requièrent votre attention. Vous pouvez recevoir ces notifications par courrier électronique, via le widget **Notifications** ou via votre logiciel tiers.

Procédure

1. Configurez les paramètres de notification généraux.
 - a. Cliquez sur **Administration** > **Configurer les notifications**.



Remarque

L'écran affiche l'adresse électronique qui recevra l'e-mail de notification. Si elle est incorrecte, sélectionnez **Mon compte** ou ouvrez la console Web Licensing Management Platform et modifiez le paramétrage du profil.

- b. Sélectionnez la langue.
 - c. (Facultatif) Activez ou désactivez l'e-mail de résumé de notification quotidien. Vous recevrez alors un e-mail de notification chaque jour vous informant de tous les événements déclenchés qui nécessitent une quelconque intervention.
 - d. Spécifiez les types de notifications qui seront envoyés une fois les événements déclenchés :
 - **Afficher dans Notifications** : Vous verrez les notifications de cet événement dans le widget Notifications. Vous verrez également le nombre d'événements dans l'icône Notifications, dans la bannière de la console.
 - **Adresse électronique** : Vous recevrez un e-mail de notification pour cet événement. Il est possible que vous puissiez renouveler les licences ou en ajouter à vos sièges affectés directement à partir du lien fourni dans ce message électronique.
 - e. Cliquez sur **Enregistrer**.
 2. Configurez les paramètres de notification spécifiques au client.

- a. Accédez à **Clients** > {nom du client} > **Notifications (onglet)**.
- b. Sélectionnez le paramètre de notification.
- c. Spécifiez des destinataires supplémentaires.

**Remarque**

Assurez-vous que les clients ont intégré les outils tiers avant d'autoriser les notifications pour Kaseya, Autotask ou ConnectWise.

Configuration des paramètres de console

Spécifiez le logo que les clients verront lorsqu'ils se connectent au service.

**Remarque**

Ce paramètre est facultatif.

Procédure

1. Cliquez sur **Administration** > **Paramètres de console**.
 2. Sélectionnez l'image que vous souhaitez utiliser. Le logo doit être une image `.png`, `.jpg`, `.bmp` ou `.gif`, aux dimensions recommandées de 600 (largeur) sur 55 (hauteur).
 3. Cliquez sur **Enregistrer**.
-

Configuration de modèles de paramètres par défaut



Remarque

Les modèles de paramètres par défaut sont disponibles uniquement si vous avez intégré Trend Micro Remote Manager avec Licensing Management Platform et uniquement pour votre produit Worry-Free Business Security Services.

Les modèles de paramètres par défaut sont des modèles comportant des paramètres préconfigurés pour un client. Il est ainsi plus facile d'assurer que les clients utilisent les mêmes paramètres.

Lorsque vous créez les modèles, une console similaire à Worry-Free Business Security Services s'affiche. Vous êtes donc déjà familiarisé avec la configuration des options par défaut utilisée par chaque client. Vous pouvez créer plusieurs modèles particuliers, pour des types de clients ou des groupes spécifiques.

Pour plus d'informations sur les paramètres que vous pouvez configurer à partir de ce modèle, reportez-vous à la documentation de Worry-Free Business Security Services à l'adresse suivante :

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

Procédure

1. Accédez à **Administration** > **Configurer les modèles de paramètres par défaut**.
2. Cliquez sur **Créer**.

Créer un modèle

Nom du modèle : *

Description :

i Cliquez sur **Configurer le modèle** pour ouvrir une console similaire à Worry-Free Business Security Services, laquelle vous permet de modifier plus facilement certains paramètres de votre produit et d'enregistrer la nouvelle configuration comme modèle.

Remarque : Seuls certains paramètres peuvent être modifiés à partir de cette console. Référez-vous à [ce guide](#) pour en savoir plus sur les paramètres que vous pouvez définir et les procédures de configuration.

Configurer le modèle Annuler

3. Indiquez le nom du modèle, et ajoutez quelques commentaires ou descriptions afin de vous rappeler plus facilement l'objectif de ce modèle.
4. Cliquez sur **Configurer le modèle**.



Remarque

Une console similaire à Worry-Free Business Security Services s'ouvre. Toutes les modifications apportées à ce site sont conservées sous forme de modèle et elles n'affectent aucun produit enregistré.

5. Configurer les paramètres suivants :
 - Stratégies
 - a. Accédez à **Dispositifs > Serveur (par défaut) > Configurer les stratégies**.
 - b. Configurez les paramètres de stratégies de serveur par défaut.
 - c. Accédez à **Scans > Dispositif (par défaut) > Configurer les stratégies**.
 - d. Configurez les paramètres de stratégies de dispositif par défaut.

- e. Cliquez sur **Enregistrer**.
- Paramètres de scan
 - a. Accédez à **Scans > Scan manuel (onglet)**.
 - b. Configurez les paramètres de serveur et de dispositif par défaut.
 - c. Accédez à **Scans > Scan programmé (onglet)**.
 - d. Configurez les paramètres de serveur et de dispositif par défaut.
 - e. Cliquez sur **Enregistrer**.
- Paramètres de notification
 - a. Accédez à **Administration > Notifications > Événements (onglet)**.
 - b. Indiquez les événements et les destinataires qui déclencheront une notification d'événement.
 - c. Cliquez sur **Enregistrer**.
- Paramètres généraux
 - a. Accédez à **Administration > Paramètres généraux > Paramètres de sécurité (onglet)**.
 - b. Apportez les modifications nécessaires aux paramètres de scan, de surveillance des comportements ou de prévention des épidémies.
 - c. Accédez à **Administration > Paramètres généraux > Paramètres d'approbation/de blocage (onglet)**.
 - d. Ajoutez ou retirez des sites dans les listes de sites approuvés ou bloqués.
 - e. Accédez à **Administration > Paramètres généraux > Contrôle d'agent (onglet)**.
 - f. Modifiez les paramètres d'agent.
 - g. Accédez à **Administration > Paramètres généraux > Gestion de dispositif (onglet)**.
 - h. Modifiez les paramètres de gestion de dispositif utilisateur.

- i. Cliquez sur **Enregistrer**.
-

Chapitre 9

Gestion des événements

Cette section contient les rubriques suivantes :

- *Gestion des événements à la page 9-2*
- *Affichage des événements à la page 9-4*
- *Types d'événement à la page 9-5*

Gestion des événements

Dans Trend Micro Remote Manager, un événement se produit lorsqu'un produit ou service requiert votre attention sur le site d'un client. L'écran **Journaux d'incidents** vous permet d'examiner et de gérer les événements de tous vos clients. Vous pouvez rechercher les événements qui se sont produits sur Worry-Free Business Security, Worry-Free Business Security Services et Hosted Email Security, par type ou par client. Vous pouvez également filtrer les événements par gravité et par état.

Remote Manager Bienvenue [nom] | Déconnexion

Notifications Nouveau client Rechercher un client Utilisation de l'exportation Commentaires Aide

Accueil > Journaux des événements

Exporter tout

Catégorie	Société	Produit	Plan de service/description du produit	Occurrences
Mises à jour des composants	Trend Micro	WFBS-A		0
Mises à jour des composants	Trend Micro	WFBS-A		0
Mises à jour des composants	Trend Micro	WFBS-A		11
Mises à jour des composants	Trend Micro RM	WFBS-A		11

Enregistrements : 1 - 4 / 4 Page 1 / 1 25 par page

FIGURE 9-1. Écran Journaux d'incidents affichant des événements d'antivirus

Événements

Les événements sont classés de la manière suivante :

- Menaces
 - *Défense anti-épidémies à la page 9-5*
 - *Antivirus à la page 9-7*
 - *Anti-spyware à la page 9-9*
 - *Anti-spam à la page 9-11*
 - *Virus de réseau à la page 9-11*

- *Réputation de sites Web à la page 9-12*
- *Surveillance des comportements à la page 9-13*
- *Filtrage des URL à la page 9-13*
- *Contrôle des périphériques à la page 9-14*
- Système
 - *Smart Protection Services à la page 9-14*
 - *Mise à jour des composants à la page 9-15*
 - *Espace disque utilisé à la page 9-16*
- Licence
 - Licence expirée
 - Licence bientôt à expiration
 - Utilisation des licences

Sévérité

La gravité est classée comme suit :

- **Action requise** : événements requérant une attention immédiate.
- **Avertissement** : les avertissements ou les notifications sont uniquement à but informatif.

État

L'état est classé comme suit :

- **Non résolu** : ces événements requièrent votre attention.
- **À réinitialiser/mettre à jour** : vous avez travaillé sur ces événements et ceux-ci sont en attente de mise à jour pour le produit ou le service.

Affichage des événements

Procédure

1. Accédez à **Accueil** > {tableau de bord} > {widget}
2. Choisissez l'un des incidents.

The screenshot shows the Trend Micro Remote Manager interface. The main content area displays the 'Journaux des événements' (Event Logs) page. The table below shows the data displayed in the interface:

Catégorie	Société	Produit	Plan de service/description du produit	Occurrences
Mises à jour des composants	Trend Micro	WFBS-A		0
Mises à jour des composants	Trend Micro	WFBS-A		0
Mises à jour des composants	Trend Micro	WFBS-A		11
Mises à jour des composants	Trend Micro_RM	WFBS-A		11

At the bottom of the table, the pagination control shows: Enregistrements : 1 - 4 / 4 | Page 1 / 1 | 25 par page

3. Effectuez l'une des actions suivantes :
 - afficher des incidents par type ou par client à l'aide de l'arborescence et de la fenêtre de recherche situées sur la gauche ;
 - afficher des événements pour un produit ou service spécifique à l'aide des onglets situés sur la droite ;
 - filtrer des événements par gravité ou état à l'aide des listes déroulantes situées dans le coin supérieur droit de l'écran ;
 - Explorez un événement particulier en cliquant sur les liens des widgets ou des notifications pour afficher des informations supplémentaires.
 - Sélectionnez un événement, puis cliquez sur **Réinitialiser** pour réinitialiser le nombre d'événements ou sur **Mettre à jour** pour mettre à jour les composants.

Pour plus d'informations sur chaque événement et sur les actions devant être prises, voir [Types d'événements à la page 9-5](#).

Types d'événement

Cela présente les différents types d'événements que Trend Micro Remote Manager peut vous afficher.

Détails sur l'état de défense anti-épidémies



Remarque

Cela est disponible uniquement pour Worry-Free Business Security (tous).

La défense anti-épidémies avertit dès les premiers signes des menaces Internet et autres conditions d'épidémies mondiales. La défense anti-épidémies répond automatiquement en prenant des mesures préventives pour assurer l'intégrité des ordinateurs et des réseaux, puis des mesures de protection pour identifier le problème et réparer les dommages. Tandis que la fonction de défense anti-épidémies protège les réseaux et les clients, les [TrendLabs à la page 12-5](#) créent des solutions permettant de remédier à la menace. Après avoir développé la solution, TrendLabs met à disposition des composants mis à jour, puis les serveurs Worry-Free Business Security (tous) téléchargent et déploient les composants mis à jour vers les clients. La défense anti-épidémies élimine ensuite tout reste de virus et répare les fichiers et répertoires endommagés par la menace.

La fonction de défense anti-épidémies peut prendre les mesures suivantes en cas d'épidémie :

- bloquer les ports
- interdire l'accès en écriture à certains fichiers et répertoires
- bloquer certaines pièces jointes

Pour déterminer l'état de défense anti-épidémies pour les réseaux gérés, Trend Micro vérifie si les TrendLabs ont déclaré une alerte virale. Un événement de défense anti-

épidémies ne s'affiche sur le tableau de bord que si au moins un événement de défense anti-épidémies s'est produit.

Le tableau ci-dessous présente les icônes d'état de défense anti-épidémies possibles.

TABLEAU 9-1. Icônes d'état de défense anti-épidémies

ICÔNE D'ÉTAT	DESCRIPTION
	Les TrendLabs ont déclaré une alerte jaune
	Les TrendLabs ont déclaré une alerte rouge

État d'alerte

Les informations d'état d'alerte s'affichent dès qu'une alerte jaune ou rouge est déclarée. Activez la défense anti-épidémies pour vous assurer que des mesures préventives se déploient automatiquement et protègent le réseau en attendant qu'un fichier de signatures soit disponible.

Ordinateurs vulnérables

Ordinateurs vulnérables sur lesquels n'ont pas été installés de correctifs pour les failles logicielles connues. Pour gérer les ordinateurs vulnérables, contactez l'administrateur du domaine concerné et fournissez-lui les noms des ordinateurs en question, ainsi que les problèmes qui les affectent. Pour obtenir ces informations, cliquez sur le nombre d'ordinateurs vulnérables.

Pour vérifier que la liste des ordinateurs vulnérables est à jour, exécutez un scan d'évaluation des failles. Pour plus d'informations, consultez [Commandes Worry-Free Business Security à la page 3-28](#).

Ordinateurs à nettoyer

Les ordinateurs à nettoyer sont des ordinateurs infectés par un virus ou un programme malveillant que le client de sécurité n'a pas réussi à nettoyer, à supprimer ou à mettre en quarantaine lors de sa détection. En général, un ordinateur infecté contient une copie en cours d'exécution du virus ou programme malveillant qui a configuré l'ordinateur pour l'autoriser à démarrer automatiquement et à rester en cours d'exécution.

Pour afficher une liste des ordinateurs infectés et les noms des virus, cliquez sur le nombre d'ordinateurs à nettoyer. Pour résoudre le problème des ordinateurs infectés, déployez Damage Cleanup Services (DCS) sur le domaine. Pour plus d'informations, consultez *Commandes Worry-Free Business Security à la page 3-28*.

Détails sur l'état antivirus



Remarque

Cela est disponible uniquement pour Worry-Free Business Security (tous).

Le tableau ci-dessous présente les icônes d'état d'antivirus possibles et le code de couleur.

TABLEAU 9-2. Icônes d'état antivirus

ICÔNE D'ÉTAT	DESCRIPTION
	<p>Cette icône d'état s'affiche si 15 incidents spywares/graywares ou plus ont été détectés en 1 heure (Worry-Free Business Security (tous), par défaut). Les administrateurs peuvent modifier le seuil sur le serveur géré. L'intervalle d'une heure représente la période de 60 minutes avant le point d'évaluation.</p>
	<p>Cette icône d'état s'affiche si l'une des éventualités suivantes se présente :</p> <ul style="list-style-type: none"> • Le scanner en temps réel du serveur Exchange est désactivé. • Un client de sécurité ne parvient pas à nettoyer ou à mettre en quarantaine un programme malveillant. • Pour Worry-Free Business Security (Standard or Advanced) versions 5.1 ou ultérieures : le scanner en temps réel est désactivé sur au moins un ordinateur.

Incidents de menaces de virus

Les incidents de menaces virales sont le nombre de détections de virus ou de programmes malveillants dans le domaine. La console regroupe ces informations statistiques dans les groupes suivants :

- **Postes de travail/serveurs** : virus ou programme malveillant détecté durant les scans manuels ou lors de l'accès à des fichiers sur les postes de travail et serveurs
- **Serveurs Exchange** : virus ou programme malveillant détecté dans les e-mails traités par un serveur Exchange

Accédez à des informations ou des actions supplémentaires, le cas échéant, en cliquant sur **Détails**.



AVERTISSEMENT!

Ne cliquez pas sur **Réinitialiser**, sauf si vous êtes certain que les incidents ont été résolus et contenus.

Échec de l'action Antivirus

Les applications de scan antivirus nettoient, mettent en quarantaine ou suppriment les fichiers contenant des programmes malveillants ou des virus. Généralement, le scanner effectue une action initiale. Si l'application de scan antivirus ne peut pas effectuer cette action, il effectue une action secondaire.

Les échecs de ces actions indiquent qu'un programme malveillant ou un virus a réussi à déjouer les défenses antivirus et a infecté l'ordinateur. Remote Manager suppose que les ordinateurs contenant un virus ou un programme malveillant qui n'a pas pu être nettoyé, mis en quarantaine ou supprimé sont infectés.

Accédez à des informations ou des actions supplémentaires, le cas échéant, en cliquant sur **Détails**.

Ordinateurs à nettoyer

Les ordinateurs à nettoyer sont des ordinateurs infectés par un virus ou un programme malveillant que le client de sécurité n'a pas réussi à nettoyer, à supprimer ou à mettre en quarantaine lors de sa détection. En général, un ordinateur infecté contient une copie en cours d'exécution du virus ou programme malveillant qui a configuré l'ordinateur pour l'autoriser à démarrer automatiquement et à rester en cours d'exécution.

Pour afficher une liste des ordinateurs infectés et les noms des virus, cliquez sur le nombre d'ordinateurs à nettoyer. Pour résoudre le problème des ordinateurs infectés,

déployez Damage Cleanup Services (DCS) sur le domaine. Pour plus d'informations, consultez *Commandes Worry-Free Business Security à la page 3-28*.

Pour corriger les ordinateurs ayant été infectés à la suite d'échecs d'actions antivirales, déployez DCS sur le domaine. Pour plus d'informations, consultez *Commandes Worry-Free Business Security à la page 3-28*.

Scan en temps réel désactivé

Lorsque le scan en temps réel est désactivé, les ordinateurs ne peuvent pas scanner les fichiers dès que ceux-ci arrivent ou sont traités. Cependant, ces fichiers sont scannés lorsque le scan programmé démarre. Ces ordinateurs comportent un risque élevé d'infection virale ou de programme malveillant. Les serveurs Exchange avec des scans en temps réel désactivés laissent passer tous les fichiers dans les messages électroniques (même ceux comportant des programmes malveillants), laissant le réseau du client sensible aux vers de publipostage.

Accédez à des informations ou des actions supplémentaires, le cas échéant, en cliquant sur **Détails**.

Pour activer le scanner en temps réel sur tous les ordinateurs et serveurs Exchange du domaine, sélectionnez le client, puis cliquez sur **Résoudre**.

Détails sur l'état anti-spyware



Remarque

L'anti-spyware est disponible uniquement pour Worry-Free Business Security (tous).

Pour illustrer l'état anti-spyware, la page **Clients** affiche les icônes d'état et un code de couleurs indiquant un taux d'incidents de spywares/graywares relativement élevé et la présence d'ordinateurs infectés par des spywares/graywares.

Le tableau ci-dessous présente les icônes d'état anti-spyware possibles.

TABLEAU 9-3. Icônes d'état anti-spyware

ICÔNE D'ÉTAT	DESCRIPTION
	Quinze incidents spywares/graywares ou plus ont été détectés en une heure (Worry-Free Business Security (tous), par défaut). Vous pouvez modifier le seuil sur le serveur géré. L'intervalle d'une heure représente la période de 60 minutes avant le point d'évaluation.
	Action requise. Au moins un ordinateur doit être redémarré pour supprimer complètement une infection par spyware/grayware.

Redémarrage de l'ordinateur requis pour Anti-spyware

Le redémarrage des ordinateurs requis pour l'anti-spyware affiche le nombre d'ordinateurs infectés par des spywares/graywares qui ont été partiellement nettoyés. Ces ordinateurs restent infectés car le spyware/grayware qui les affecte ne peut pas être complètement supprimé tant que chaque ordinateur n'est pas redémarré. Pour terminer complètement le processus de nettoyage sur ces ordinateurs, contactez un administrateur côté client pour qu'il redémarre les ordinateurs manuellement.

Accédez à des informations ou des actions supplémentaires, le cas échéant, en cliquant sur **Détails**.



AVERTISSEMENT!

Ne cliquez pas sur **Réinitialiser**, sauf si vous êtes certain que les incidents ont été résolus et contenus.

Incidents de menaces de spywares/graywares

Les incidents de menaces de spywares/graywares sont le nombre de détections de spywares/graywares dans le domaine. Pour afficher la liste des ordinateurs affectés et les noms des menaces de spywares/graywares, cliquez sur le nombre d'incidents. Pour réinitialiser le nombre actuel, cliquez sur **Réinitialiser**.

Accédez à des informations ou des actions supplémentaires, le cas échéant, en cliquant sur **Détails**.

**AVERTISSEMENT!**

Ne cliquez pas sur **Réinitialiser**, sauf si vous êtes certain que les incidents ont été résolus et contenus.

Détails sur l'état anti-spam

La section Détails de l'état Anti-spam prévient de l'augmentation du nombre de messages de spam traités par le serveur Exchange. L'écran affiche des icônes d'état pour indiquer si le pourcentage de messages de spam (par rapport au nombre total de messages que le serveur Exchange traite) a atteint un certain seuil. Un événement anti-spam s'affiche sur le tableau de bord uniquement si au moins un événement anti-spam se produit.

Le tableau ci-dessous présente les icônes d'état possibles.

TABLEAU 9-4. Icônes d'état anti-spam

ICÔNE D'ÉTAT	DESCRIPTION
	Avertissement. Les spams constituent 10 % ou plus du total des messages traités par le serveur Exchange (Client Server Messaging/Worry-Free Business Security Advanced, par défaut). Les administrateurs peuvent modifier le seuil sur le serveur géré.
	Cette icône n'est pas utilisée pour afficher ces détails.

Détails sur l'état des virus de réseau

La section Détails sur l'état des virus de réseau prévient toute activité de virus de réseau importante sur le réseau. L'écran Gestion des événements affiche des icônes d'état et un code de couleurs pour indiquer que l'activité virale du réseau de certains domaines client a atteint un seuil spécifique. Un événement de virus de réseau ne s'affiche sur le tableau de bord que si au moins un événement de virus de réseau se produit.

TABLEAU 9-5. Icônes d'état des virus de réseau

ICÔNE D'ÉTAT	DESCRIPTION
	Ceci est un message d'avertissement. Dix incidents de virus de réseau ou plus ont été détectés en une heure (Worry-Free Business Security (tous), par défaut). Les administrateurs peuvent modifier le seuil sur le serveur géré. L'intervalle d'une heure représente la période de 60 minutes avant le point d'évaluation.
	Cette icône n'est pas utilisée pour afficher ces détails.

Accédez à des informations ou des actions supplémentaires, le cas échéant, en cliquant sur **Détails**.

Détails sur l'état de réputation de sites Web

La réputation de sites Web évalue le risque de sécurité potentiel des pages Web demandées avant de les afficher. En fonction de l'évaluation que renvoie la base de données et du niveau de sécurité configuré, l'agent Client/Server Security Agent situé sur les ordinateurs gérés par Worry-Free Business Security (tous) bloquera ou approuvera la demande. La section Services de réputation de sites Web indique le nombre de tentatives de récupération de pages Web évaluées comme présentant un risque de sécurité. Un événement de réputation de sites Web s'affiche sur le tableau de bord uniquement si au moins un événement de réputation de sites Web se produit.

TABLEAU 9-6. Icônes d'état de réputation de sites Web

ICÔNE D'ÉTAT	DESCRIPTION
	Les clients signalent des violations d'URL nombreuses ou fréquentes. Plus de 200 violations ont été détectées en 1 heure (Worry-Free Business Security (tous), par défaut). Les administrateurs peuvent modifier le seuil sur le serveur géré. L'intervalle d'une heure représente la période de 60 minutes avant le point d'évaluation.
	Cette icône n'est pas utilisée pour afficher ces détails.

Détails sur l'état de surveillance des comportements

La surveillance des comportements surveille le client pour détecter les tentatives de modification du système d'exploitation et autres programmes. Quand un agent Client/Server Security Agent installé sur les ordinateurs gérés par Worry-Free Business Security (tous) détecte une tentative, Security Agent notifie la modification à l'utilisateur. L'utilisateur peut autoriser ou bloquer la demande. Les administrateurs (ou utilisateurs) Worry-Free Business Security (tous) peuvent créer des listes d'exceptions afin de bloquer totalement certains programmes ou de permettre à certains programmes de s'exécuter tout en outrepassant une modification surveillée. Lorsque le total de violations dépasse le seuil, l'icône d'état est modifiée et le nombre d'incidents est indiqué dans le **tableau de bord** et les écrans **Gestion des événements**.

TABEAU 9-7. Icônes d'état de réputation de sites Web

ICÔNE D'ÉTAT	DESCRIPTION
	Les clients signalent des violations d'URL nombreuses ou fréquentes. Plus de 200 violations ont été détectées en 1 heure (Worry-Free Business Security (tous), par défaut). Les administrateurs peuvent modifier le seuil sur le serveur géré. L'intervalle d'une heure représente la période de 60 minutes avant le point d'évaluation.
	Cette icône n'est pas utilisée pour afficher ces détails.

Détails sur l'état du filtrage d'URL

Le module de filtrage d'URL contient des outils puissants et efficaces pour gérer l'accès Internet des employés et bloquer les sites Web nuisibles ou de nature non professionnelle. Le filtrage d'URL filtre le contenu via une base de données contenant des millions d'URL répertoriées par catégorie et utilise une technologie d'évaluation dynamique pour classer les nouvelles pages Web, en temps réel ou en arrière-plan. Les responsables informatiques peuvent définir des stratégies d'URL par groupe ou utilisateur, par catégorie, par type de fichier, par heure, par jour, par bande passante et selon d'autres variables.

**Remarque**

Le filtrage d'URL concerne exclusivement Worry-Free Business Security Services et Worry-Free Business Security Standard et Advanced 6.0 et versions ultérieures.

TABLEAU 9-8. Icônes de l'état du filtrage d'URL

ICÔNE D'ÉTAT	DESCRIPTION
	Avertissement. Nombre d'événements de filtrage d'URL supérieur à 300 au cours de la dernière heure écoulée.
	Cette icône n'est pas utilisée pour afficher ces détails.

Détails sur l'état du contrôle des périphériques

Le module Contrôle des dispositifs offre des outils puissants et efficaces pour réguler l'accès aux périphériques de stockage externes et aux ressources du réseau.

**Remarque**

Le module Contrôle des dispositifs concerne uniquement les versions 7.x et ultérieures de Worry-Free Business Security Standard et Advanced.

TABLEAU 9-9. Icônes d'état du contrôle des périphériques

ICÔNE D'ÉTAT	DESCRIPTION
	Avertissement. Nombre d'incidents d'accès à des périphériques non autorisés supérieur à 300 au cours de la dernière heure écoulée.
	Cette icône n'est pas utilisée pour afficher ces détails.

Smart Scan

Trend Micro™ Worry-Free Business Security utilise une technologie appelée Smart Scan. Auparavant, les clients Worry-Free Business Security Services utilisaient uniquement le scan traditionnel : chaque client devait télécharger les composants liés aux

scans pour exécuter les scans souhaités. Le processus Smart Scan permet désormais au client d'utiliser le fichier de signatures sur le serveur Smart Protection. Seules les ressources de Smart Protection Server sont utilisées pour scanner les fichiers.



Remarque

La technologie Smart Protection est utilisée uniquement par les versions 6.x et ultérieures de Worry-Free Business Security Standard et Advanced et par les versions 3.x et ultérieures de Worry-Free Business Security Services.

TABLEAU 9-10. Icônes d'état de l'espace disque utilisé

ICÔNE D'ÉTAT	DESCRIPTION
	Le service Smart Protection a été interrompu sur un agent Worry-Free Business Security.
	Le service Smart Protection a été interrompu sur un agent Worry-Free Business Security.

Si le service Smart Protection ne fonctionne pas, patientez 30 minutes pour permettre à l'agent de se synchroniser avec le serveur de scan global. Si l'agent ne se connecte toujours pas au serveur de scan global, vérifiez sa connexion Internet. Contactez votre service d'assistance pour obtenir de l'aide.

Mise à jour des composants

Le tableau ci-dessous indique les icônes affichées par la page **Client** pour indiquer des problèmes de mise à jour.

TABLEAU 9-11. Icônes d'état de mise à jour

ICÔNE D'ÉTAT	DESCRIPTION
	<p>Avertissement. Cette icône d'état s'affiche si l'une des éventualités suivantes se présente :</p> <ul style="list-style-type: none"> • Le produit géré ne s'est pas mis à jour depuis plus de sept jours. • Le taux de déploiement de la signature et du moteur sur le poste de travail et le serveur est inférieur à 90%.
	<p>Action requise. Cette icône d'état s'affiche si l'une des éventualités suivantes se présente :</p> <ul style="list-style-type: none"> • Le produit géré ne s'est pas mis à jour depuis plus de 14 jours. • Le taux de déploiement de la signature et du moteur sur le poste de travail et le serveur est inférieur à 70 %. • Au moins un serveur Exchange est exécuté avec des composants de sécurité obsolètes.

Pour résoudre des problèmes de mise à jour, accédez à **Clients > {client} > Système > Mise à jour des composants > {type de produit}**, sélectionnez le produit ou le service, puis cliquez sur **Résoudre**.

Lorsque vous avez mis à jour le serveur géré et déployé les derniers composants, Trend Micro vous recommande d'exécuter la commande Scan manuel (dans le menu **Actions**). Un scan pourra détecter les menaces que les composants obsolètes ont manquées.

Espace disque utilisé

La page **Clients** vous permet de surveiller les problèmes d'espace disque utilisé sur les ordinateurs du domaine, car elle affiche des icônes pour indiquer les problèmes d'espace disque actuels et potentiels. Pour comprendre la signification de ces icônes, consultez le tableau ci-dessous.

TABLEAU 9-12. Icônes d'état de l'espace disque utilisé

ICÔNE D'ÉTAT	DESCRIPTION
	Cette icône n'est pas utilisée pour afficher ces détails.
	Action requise. Cette icône d'état s'affiche si deux ordinateurs ou plus disposent de moins de 1 % d'espace disque (cette valeur par défaut de Worry-Free Business Security Standard et Advanced peut être modifiée sur la console de ce produit).

Pour résoudre les problèmes d'espace disque utilisé, contactez l'administrateur du domaine concerné.

Chapitre 10

Rapports

Cette section contient les rubriques suivantes :

- *Présentation des rapports à la page 10-2*
- *Création de rapports à la page 10-3*
- *Affichage des rapports à la page 10-7*
- *Modification des rapports à la page 10-7*
- *Téléchargement et envoi de rapports à la page 10-8*
- *Abonnement aux rapports à la page 10-8*

Présentation des rapports

Trend Micro Remote Manager vous permet de générer, de télécharger et d'envoyer automatiquement des rapports. Les rapports présentent les états des licences, les résultats d'évaluation, les incidents de menaces, les menaces principales et les ordinateurs, fichiers et adresses e-mail les plus affectés des réseaux de vos clients.

Les rapports incluent des statistiques fournies par Worry-Free Business Security (tous) et Hosted Email Security. Remote Manager permet la génération de profils de rapport, de rapports à usage unique et périodiques, de plages de dates, de plusieurs destinataires d'e-mails. Remote Manager enregistre les 30 rapports quotidiens les plus récents, les dix rapports hebdomadaires les plus récents et les cinq rapports mensuels les plus récents. Les rapports généraux sont adaptés aux revendeurs et aux clients. Les rapports détaillés sont adaptés aux revendeurs et aux partenaires.

Rapports ?

Tous les rapports

<input type="checkbox"/>	Nom du rapport	Fichiers	Cible	Type de rapport	Fréquence	Dernier généré	État
<input type="checkbox"/>	IPDFILicense Report Daily_WFBSS	60	Moi	Partenaire	Quotidien	14/avr./2014 16:17:15	✔
<input type="checkbox"/>	CSV_LR_WFBSS_Daily	25	Moi	Partenaire	Quotidien	14/avr./2014 16:17:10	✔
<input type="checkbox"/>	ICSVILicense Report Daily_WFBSS	60	Moi	Partenaire	Quotidien	14/avr./2014 16:17:05	✔
<input type="checkbox"/>	ICSVILicense Report Daily_WFBSS	60	Moi	Partenaire	Quotidien	14/avr./2014 14:17:04	✔
<input type="checkbox"/>	ICSVIDetail Report Daily_ALL	60	1	Client	Quotidien	14/avr./2014 12:17:25	✔
<input type="checkbox"/>	IPDFIDetail Threat Report Daily_ALL	60	1	Client	Quotidien	14/avr./2014 12:17:18	✔
<input type="checkbox"/>	ICSVIGeneral Threat Report Daily_WFBSS	60	1	Client	Quotidien	14/avr./2014 12:17:13	✔
<input type="checkbox"/>	ICSVIGeneral Threat Report Daily_HES	76	1	Client	Quotidien	14/avr./2014 12:17:13	✔
<input type="checkbox"/>	IPDFIDetail Threat Report D	60	1	Client	Quotidien	14/avr./2014 12:17:	✔

Rapports

Rechercher un rapport

Utiliser " " pour une correspondance exacte

Type de rapport

Client

Partenaire

Généré

Tous

FIGURE 10-1. Page Rapports

Les profils de rapport vous permettent de créer plusieurs rapports à partir d'un seul profil. Par exemple, vous pouvez créer un rapport à usage unique aujourd'hui, le générer, puis modifier le lendemain certaines options et le générer à nouveau sans devoir recréer le rapport dans son intégralité. Remote Manager prend actuellement en charge des rapports généraux et détaillés.

Création de rapports

Trend Micro Remote Manager propose les moyens suivants pour la création d'un modèle de rapport :

- Cliquez sur un rapport existant, modifiez le rapport, puis cliquez sur **Enregistrer** en bas de l'écran.
- Créez un nouveau modèle de rapport. Pour plus d'informations, voir *Création d'un modèle de rapport à la page 10-3*.

Création de modèles de rapport

Procédure

1. Cliquez sur **Rapports > Nouveau rapport**.

L'écran **Nouveau rapport** s'ouvre.

Nouveau rapport

Saisir les informations générales

Nom du rapport : *

Type de rapport : Rapport client
 Rapport partenaire

Période : Usage unique
 Quotidien
 Hebdomadaire
 Mensuel

24 dernières heures

Plage spécifique

De 16/04/2014

À 16/04/2014

Format de rapport : PDF

Langue du rapport : Anglais

Logo partenaire : Remote Manager

Sélectionner une image

Téléchargez uniquement les fichiers png, jpg, bmp ou gif de 600 px de largeur et de 55 px de hauteur.

Remarque :

Suivant > Annuler

2. Si besoin, mettez à jour les éléments suivants :

- **Nom du rapport**
- **Type de rapport** : Pour plus d'informations, voir [Présentation des rapports à la page 10-2](#).

Seul Worry-Free Business Security possède un rapport détaillé.

3. Sélectionnez le rapport **intervalle de dates** :

- **Rapport à usage unique**

OPTION	DESCRIPTION
Aujourd'hui	<p>Calcule les rapports avec les données reçues depuis minuit et jusqu'au moment où le rapport est généré (sur la base du fuseau horaire sélectionné).</p> <hr/> <p> Remarque Le fuseau horaire utilisé dans le rapport dépend de celui qui a été sélectionné par le revendeur à la création du profil. Il n'est pas défini par l'ordinateur du client.</p>
7 derniers jours	Calcule le rapport avec les données des 7 derniers jours (sauf les données du jour même).
30 derniers jours	Calcule le rapport avec les données des 30 derniers jours (sauf les données du jour même).
Plage spécifique	La date « De » doit être postérieure ou égale à la première date du mois précédent (Remote Manager stocke uniquement les données du mois passé et du mois actuel) ; la date « À » doit être antérieure à aujourd'hui.

- **Rapport périodique**

OPTION	DESCRIPTION
Rapport quotidien	<p>La date de fin doit être postérieure à aujourd'hui. Chaque jour de la plage spécifique génère un rapport en fonction des données de la veille.</p> <p>Par exemple, si la plage spécifique est définie du 27 janvier 2009 au 29 janvier 2009 :</p> <ul style="list-style-type: none"> • Le 27, Remote Manager génère un rapport basé sur le 26 • Le 28, Remote Manager génère un rapport basé sur le 27 • Le 29, Remote Manager génère un rapport basé sur le 28

OPTION	DESCRIPTION
Rapport hebdomadaire	Remote Manager génère le rapport hebdomadaire chaque lundi avec les données de la semaine précédente. Par conséquent, pour générer un rapport relatif à la semaine actuelle, définissez la date de fin au lundi de la semaine suivante au plus tôt.
Rapport mensuel	Remote Manager génère le rapport mensuel chaque deuxième jour du mois avec les données du mois précédent. Par conséquent, pour générer un rapport relatif au mois actuel, définissez la date de fin au moins au deuxième jour du mois suivant.

4. Définissez le **contenu du rapport**. Cela comprend les éléments de format de rapport suivants :

OPTION	DESCRIPTION
Format de rapport	Format PDF ou CSV
Langue du rapport	La langue du rapport
Logo	Le logo est facultatif. Le logo du partenaire doit être une image au format .png, .jpg, .bmp ou .gif, et la dimension recommandée est 600 x 55 (largeur x hauteur) pixels.
Remarque	Le champ Remarque est destiné à l'utilisation en interne et ne s'affiche pas dans le rapport.

5. Cliquez sur **Suivant**.
6. Sélectionnez les données pour votre rapport. Sélectionnez un modèle de rapport et les données à générer.



Remarque

Si le revendeur n'est pas connecté au serveur client ou s'il n'y a aucune donnée, les informations pour le client ne s'affichent pas.

7. Cliquez sur **Suivant**.

- Sélectionnez les clients qui vont générer ce rapport.

**Remarque**

Vous pouvez cliquer sur **Terminé** pour que les rapports soient générés pour les clients sélectionnés.

- Indiquez les détails du rapport pour l'e-mail. Les destinataires figurant dans les options **Email to (Envoyer par e-mail à)** proviennent de la liste des contacts de la société. Voir *Ajout de contacts à la page 5-10*. Vous pouvez également ajouter l'adresse électronique qui recevra les rapports générés.

**Remarque**

Chaque client sélectionné aura des destinataires d'e-mails différents. Vous pouvez ajouter ou supprimer des destinataires d'e-mails ou un logo, selon les clients.

- Cliquez sur **Terminé**.

Remote Manager ajoute le modèle de rapport à la liste des modèles de rapport.

Affichage des rapports

Pour afficher un rapport, celui-ci doit avoir été généré au moins une fois.

Accédez à **Rapports** > {nom du rapport} > **Fichiers de rapport (onglet)** > {fichier dans Affichage}.

Pour plus d'informations, voir *Présentation des rapports à la page 10-2*.

Modification des rapports

Accédez à **Rapports** > {nom du rapport}.

Pour plus d'informations, voir *Création de modèles de rapport à la page 10-3*.

Téléchargement et envoi de rapports

Vous pouvez télécharger et envoyer des rapports aux destinataires. Même si les destinataires étaient spécifiés lorsque vous avez défini le rapport, la liste des destinataires peut être modifiée.

Procédure

1. Accédez à **Rapports** > {élément ou nombre d'éléments dans Fichiers de rapport} > {rapport dans Affichage}.
2. Sélectionnez les rapports à envoyer ou télécharger.
3. Cliquez sur **Envoyer** ou **Télécharger**.

Pour plus d'informations, voir *Abonnement aux rapports à la page 10-8*.

Abonnement aux rapports

Procédure

1. Accédez à **Rapports** > {nom du rapport} > **Public cible (onglet)** > **Ajouter une cible**.
2. Sélectionnez le rapport client.



Remarque

Lors de la création de rapports, la liste de destinataires possibles pour les e-mails provient des détails du contact.

3. Modifiez la ligne d'objet comme vous le souhaitez.
 4. Cliquez sur **Enregistrer**.
-

Chapitre 11

Dépannage et problèmes connus

Cette section contient les rubriques suivantes :

- *Dépannage de la console Web Trend Micro Remote Manager à la page 11-2*
- *Dépannage de l'agent à la page 11-6*
- *Problèmes de serveur connus à la page 11-11*
- *Problèmes d'agent connus à la page 11-14*
- *FAQ à la page 11-15*

Dépannage de la console Web Trend Micro Remote Manager

Cette section contient les rubriques suivantes :

Problèmes d'accès

Un utilisateur ne peut pas se connecter à Trend Micro Remote Manager.

Résolution

Il existe deux raisons possibles à ce problème :

- JavaScript est désactivé dans le navigateur. Remote Manager requiert que cette option soit activée. Reportez-vous à la documentation de votre navigateur pour obtenir des instructions.
- Le profil n'a pas été synchronisé. Si vous venez de vous enregistrer sur Trend Micro Licensing Management Platform et ne parvenez pas à vous connecter, attendez quelques minutes afin que les informations se synchronisent.

Arborescence des domaines invisible après l'installation de l'agent

L'arborescence des domaines n'apparaît pas sur la console après que vous avez installé l'agent Remote Manager sur le serveur géré.

- L'identificateur global unique (GUID) est incorrect.
- L'agent Remote Manager ne peut pas communiquer avec Remote Manager.

Résolution

1. Assurez-vous que l'entrée de GUID est correcte.
 - a. Sur Security Server, utilisez un éditeur de texte tel que le Bloc-notes pour ouvrir `C:\Program Files\Trend Micro\WFRMAgentForCSM\AgentSysConfig.xml`.

- b. Vérifiez le GUID situé juste après le paramètre.
 - c. Si vous corrigez le GUID, enregistrez le fichier, puis redémarrez le service d'agent Trend Micro Remote Manager.
 - d. Vérifiez l'état du domaine du client à partir de Remote Manager après quelques minutes.
2. Vérifiez la connexion agent/serveur à l'aide de la fonctionnalité Tester la connexion.
- a. Accédez à **Démarrer > Programmes > Trend Micro Remote Manager Agent > Outil de configuration de l'agent**.
 - b. Cliquez sur **Tester la connexion**.
 - c. Si le test échoue :
 - i. Vérifiez si le serveur géré peut se connecter à Internet.
 - ii. Vérifiez si vous avez correctement saisi l'adresse du serveur Trend Micro Remote Manager.
 - iii. Si Security Server utilise un proxy pour se connecter à Internet, vérifiez que vous avez également saisi les paramètres du serveur proxy.

Un nœud de l'arborescence ne se développe pas

Si un nœud de l'arborescence des domaines (sous l'onglet **Clients**) ne se développe pas lors d'un clic, cela signifie peut-être que les informations de groupes et de clients sur le serveur Worry-Free Business Security et le serveur Trend Micro Remote Manager ne sont pas synchronisées.

Résolution

Cliquez avec le bouton droit de la souris sur le nœud, puis cliquez sur **Action > Synchroniser avec le serveur géré** pour renvoyer les données de l'agent au serveur Trend Micro Remote Manager.

Impossible d'afficher la page

La mention Impossible d'afficher la page apparaît lors de la tentative d'ouverture de l'URL du serveur Trend Micro Remote Manager. Cela se produit si :

- L'URL est incorrecte.
- L'URL du serveur Trend Micro Remote Manager ne constitue pas un site de confiance Internet Explorer.

Résolution

1. Vérifiez que l'URL du serveur Trend Micro Remote Manager constitue un site de confiance Internet Explorer.
 - a. Ouvrez Internet Explorer.
 - b. Cliquez sur **Outils > Options Internet > Sécurité > Sites de confiance > Sites**.
 - c. Vérifiez que l'URL du serveur Trend Micro Remote Manager se trouve dans la liste. Sinon, tapez-le, puis cliquez sur **OK**.

Informations incorrectes sur le tableau de bord

Si le tableau de bord semble indiquer des informations incorrectes ou incomplètes au sujet d'un domaine particulier.

Résolution

- Vérifiez si le serveur géré est démarré.
- Vérifiez si l'agent est démarré et fonctionne correctement.
 - Dans la console Web Remote Manager, cliquez sur **Clients (onglet) > Tous les clients (dans l'arborescence) > {client} > WFBS-S/WFBS-A > Détails relatif au serveur/à l'agent (panneau de droite) > Détails de l'agent TMRM** (voir *État de l'agent à la page 6-2*).
 - Vérifiez l'état de l'agent sur le serveur géré (voir *Gestion des agents à partir du serveur géré à la page 6-6*, *État de l'agent à la page 6-2* et *Vérification de l'installation de l'agent à la page 4-10*).

- Vérifiez si le client a réinstallé l'agent. De même, vérifiez si le client a réinstallé l'agent et a utilisé un GUID différent ou en double. Par défaut, l'agent doit arriver jusqu'aux trois derniers jours de données du serveur géré.
- Vous pouvez essayer de générer un nouveau GUID et de réinstaller l'agent.

Impossible de déployer des commandes

Si vous ne parvenez pas à déployer des commandes de réseau sur un agent :

Résolution

- Le service Worry-Free Business Security Standard or Advanced est en cours d'exécution.
- L'agent client est en cours d'exécution. Sinon, pour démarrer l'agent, voir [Service de l'agent à la page 4-11](#).
- Les ports 80 et 443 sont ouverts. Vous pouvez vérifier cela en établissant une connexion Telnet du serveur Remote Manager vers les agents sur les ports 80 et 443, et inversement. Si les ports ne sont pas ouverts, l'administrateur client doit les ouvrir sur son pare-feu.

État de l'agent anormal

L'état de l'agent peut être anormal pour plusieurs raisons.

Résolution

1. L'état de l'agent sera anormal si l'agent n'a pas envoyé de demande de déconnexion au serveur Remote Manager avant de s'éteindre. Pour résoudre cela, redémarrez le service d'agent (voir [Service de l'agent à la page 4-11](#)).
2. Si cela ne résout pas le problème, ouvrez l'outil de configuration de l'agent en cliquant avec le bouton droit de la souris sur l'icône de l'agent et sélectionnez **Configurer**. Cliquez sur le bouton **Tester la connexion** pour tester la connexion du réseau au serveur Remote Manager.
3. Si vous recevez un message d'erreur, vérifiez votre stratégie de pare-feu.

4. Si la connexion fonctionne normalement, vérifiez le journal d'agent (voir *Emplacement des journaux et des fichiers de configuration d'agents à la page 6-14*).
5. Si le problème est critique et se reproduit après le redémarrage du service d'agent, activez le journal de débogage (voir *Activer le journal de débogage de l'agent à la page 6-14*) et contactez votre service d'assistance.

L'agent fonctionne de façon anormale en utilisant un GUID existant après...

Pourquoi l'agent ne fonctionne-t-il pas normalement en utilisant un GUID existant après la réinstallation du système d'exploitation, la réinstallation de l'agent Remote Manager, le changement de la carte réseau de l'ordinateur ou l'installation de l'agent sur un autre ordinateur ?

Résolution

Avant d'effectuer l'une des opérations ci-dessus, l'agent doit d'abord être désinstallé afin que les informations existantes soient supprimées sur le serveur Remote Manager. Sinon, un agent utilisant un GUID existant fonctionnera de façon anormale.

Dépannage de l'agent

Problèmes d'agent

Dès que vous placez votre souris sur l'icône de barre d'état système, elle affiche un message d'état indiquant si l'agent fonctionne normalement ou non.

TABEAU 11-1. Messages d'état affichés par l'icône de la barre d'état système de l'agent

MESSAGE	DESCRIPTION
Erreur inconnue rencontrée. Vérifiez le système ou redémarrez l'agent.	<p>Erreur inconnue rencontrée. Vérifiez le système ou redémarrez l'agent.</p> <p>Des erreurs inattendues, généralement des erreurs système, empêchent l'agent de fonctionner correctement.</p> <p>Résolution :</p> <p>Vérifiez une éventuelle insuffisance de mémoire ou tout autre problème lié au système sur le serveur géré.</p>
Enregistrement avec le serveur distant impossible.	<p>Il se peut que vous ayez utilisé un GUID incorrect ou qu'il y ait un problème de réseau.</p> <p>Résolution</p> <p>Deux situations peuvent entraîner ce problème :</p> <ul style="list-style-type: none"> • Vérifiez que vous avez utilisé le bon GUID. Pour trouver le GUID correct sur la console Web Remote Manager, reportez-vous à GUID de l'agent à la page 4-8. Pour vérifier (et éventuellement modifier) le GUID de l'agent, reportez-vous à Enregistrement avec le serveur distant impossible à la page 11-9. • S'il existe un problème de réseau, l'agent ne peut pas se connecter au serveur. Vérifiez la connexion réseau entre le serveur Worry-Free Business Security (Standard et Advanced) et le serveur Trend Micro Remote Manager.
Connexion au serveur distant impossible.	<p>Le serveur géré rencontre peut-être des problèmes de connectivité Internet.</p> <p>Résolution</p> <p>Vérifiez la connectivité Internet sur le serveur géré. De même, vérifiez les paramètres proxy de l'agent, ainsi que le port et l'adresse de serveur indiqués.</p>

MESSAGE	DESCRIPTION
Agent désactivé par Remote Manager.	L'agent a été momentanément désactivé via la console Web Remote Manager. Résolution Activez l'agent via la console Web Remote Manager.
L'agent ne correspond pas à Client Server Messaging Security (CSM).	Client Server ou Client Server Messaging Security Suite et les versions des agents ne correspondent pas. Résolution Mettez à niveau Client Server ou le serveur Client Server Messaging Security Suite vers la dernière version et installez le dernier agent.
Le service d'agent s'est arrêté.	L'agent s'est déconnecté de Remote Manager. Résolution Démarrez le service d'agent en cliquant avec le bouton droit sur l'icône de la barre d'état système de l'agent, puis en cliquant sur Démarrer le service .
Chargement des composants impossible. Vous devrez peut-être réinstaller l'agent.	L'agent a rencontré des problèmes au cours du chargement de certains composants. Résolution Essayez d'abord de redémarrer le service d'agent en cliquant avec le bouton droit sur l'icône de la barre d'état système de l'agent, puis en cliquant sur Redémarrer le service ou Démarrer le service . Si cela ne fonctionne pas, désinstallez, puis réinstallez l'agent. Assurez-vous d'utiliser le même GUID.

Connexion au serveur impossible

Lorsque vous cliquez sur le bouton Tester la connexion dans l'outil de configuration de l'agent Trend Micro Remote Manager et la mention Connexion au serveur impossible. Les paramètres sont peut-être invalides. Saisissez des paramètres valides et réessayez. apparaît.

Résolution

Effectuez l'une des actions suivantes :

- Le serveur géré ne peut pas se connecter à Internet. Vérifiez que Worry-Free Business Security Advanced peut accéder à Internet.
- Le nom de domaine complet (FQDN) de l'adresse du serveur de communication Remote Manager est incorrect. Utilisez le FQDN correspondant à votre région :
 - Asie/Pacifique : `rm-apaca.trendmicro.com`
 - Europe et Moyen-Orient : `rm-emeaa.trendmicro.com`
 - Japon : `rm-jpa.trendmicro.com`
 - Amérique latine : `rm-lara.trendmicro.com`
 - Amérique du Nord : `rm-usa.trendmicro.com`
- Si Security Server utilise un serveur proxy pour se connecter à Internet, vérifiez que le proxy et les paramètres d'authentification des utilisateurs sont correctement configurés.

Enregistrement avec le serveur distant impossible

La mention Enregistrement avec le serveur distant impossible s'affiche lorsque la souris est placée au-dessus de l'icône d'agent Trend Micro Remote Manager.

Résolution

Ce problème survient lorsque l'identificateur global unique (GUID) est incorrect. Pour résoudre ce problème :

1. Allez à l'`<install path>\Trend Micro\WFRMAgentForCSM`
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 d'agent Trend Micro Remote Manager de la barre des tâches, puis cliquez sur **Redémarrer le service**.

Problèmes de connexion avec Hosted Email Security

Si vous ne parvenez pas à connecter ou à déconnecter Hosted Email Security, les éléments suivants peuvent s'afficher en bas de la page :

MESSAGES	RÉSOLUTION
Connexion au serveur Remote Manager impossible. Veuillez vérifier la connexion réseau et l'état Remote Manager.	Vérifiez la connexion réseau et l'état Remote Manager, puis réessayez.
Clé d'autorisation invalide	Vérifiez le GUID. Si le GUID est incorrect, supprimez l'agent et réessayez de vous connecter.
Clé d'autorisation dupliquée	Vérifiez le GUID. Si le GUID est incorrect, supprimez l'agent et réessayez de vous connecter.
Connexion impossible au serveur Remote Manager Remote Manager. Vérifiez la connexion réseau et l'état du serveur Remote Manager.	Vérifiez la connexion réseau et l'état de Remote Manager puis réessayez.
Erreur interne de serveur	contactez votre service d'assistance.

Problèmes de serveur connus

Les problèmes de serveur connus pour cette version sont les suivants.

Icônes d'état incohérentes

Lors des étapes initiales de la collecte des données (juste après que l'agent s'enregistre auprès du serveur), Remote Manager peut afficher des icônes d'état d'antivirus et d'anti-spam ne correspondant pas au nombre affiché d'incidents de virus et de spam.

Juste après son enregistrement auprès du serveur, l'agent transmet les états actuels d'antivirus et d'anti-spam de Worry-Free Business Security (tous), mais ne transmet pas les données historiques sur lesquelles ces états sont basés. Ainsi, il est par exemple possible qu'une icône d'état rouge s'affiche sans toutefois indiquer d'incident.

Résolution

Remote Manager affichera l'icône et les données appropriées dès que Worry-Free Business Security (tous) aura détecté un incident.

Données de spam incohérentes avec Worry-Free Business Security Standard ou Advanced

Les données de spam peuvent différer entre Worry-Free Business Security Standard ou Advanced et Remote Manager si les serveurs exécutant les deux systèmes se trouvent dans des fuseaux horaires différents.

Résolution

Les incidents de spam dans la console Web Remote Manager et les rapports peuvent avoir des dates différentes en fonction du décalage horaire entre les serveurs.

Nom d'utilisateur incorrect sur la console Worry-Free Business Security Services

Une fois que vous vous êtes connecté à Worry-Free Business Security Services via la console Web Remote Manager, la console Worry-Free Business Security Services affiche le nom du revendeur au lieu du nom du client Worry-Free Business Security Services.

Résolution

Ce problème n'a pas encore été résolu.

Infos sur la licence incohérentes sur la console Worry-Free Business Security Services

Lorsqu'un revendeur modifie les informations sur la licence sur la console Web Remote Manager en réponse à un événement de licence, l'alerte ne change pas avant la synchronisation de Worry-Free Business Security Services avec Remote Manager.

Résolution

Attendez environ cinq minutes afin de permettre à Worry-Free Business Security Services de se synchroniser avec Remote Manager.

Les connexions simultanées à partir de deux onglets/fenêtres du même navigateur ne sont pas autorisées

Si un revendeur tente de se connecter plusieurs fois à partir d'un autre onglet ou d'une autre fenêtre du même navigateur, il est automatiquement redirigé vers l'onglet ou la fenêtre ouvert(e).

Résolution

Fermez la session initiale avant de démarrer une nouvelle session.

Les rapports historiques sont automatiquement supprimés

Vous pouvez uniquement modifier le nombre maximum de rapports quotidiens stockés par Remote Manager. Une fois le quota atteint, les rapports plus anciens sont automatiquement supprimés.

Résolution

Trend Micro recommande de télécharger les rapports plus anciens vers des ordinateurs ou d'autres périphériques de stockage.

Un compte Worry-Free Business Security Services arrivé à expiration ne peut pas être géré

Remote Manager n'affiche pas les informations du compte Worry-Free Business Security Services arrivés à expiration, car Worry-Free Business Security Services supprime les informations de compte les plus anciennes.

Résolution

Trend Micro recommande de renouveler les comptes Worry-Free Business Security Services selon les besoins.

Connexion ConnectWise interrompue

La connexion ConnectWise avec un client s'interrompt si l'ID de la société est mis à jour dans ConnectWise.

Résolution

Dans l'écran Client Remote Manager de ConnectWise, mettez à jour le nouvel ID de la société.

Problèmes d'agent connus

Les problèmes d'agent connus pour cette version sont les suivants.

Les agents réinstallés fournissent des données se chevauchant

Les agents transmettent automatiquement certaines données Worry-Free Business Security (tous) correspondant à 3 jours de collecte lors de l'enregistrement. Si un agent est désinstallé puis réinstallé sous trois jours, il extraira probablement des données redondantes par rapport à celles qu'il a extraites avant d'être désinstallé.

Résolution

Sauvegardez les fichiers de configuration de l'agent avant de le désinstaller puis restaurez-les après l'avoir réinstallé. Pour plus d'informations, consultez [Sauvegarde et restauration des paramètres de l'agent à la page 6-11](#).

Les résultats de la commande de scan ne peuvent pas être vérifiés

L'agent ne peut pas vérifier si Worry-Free Business Security Standard or Advanced a correctement déployé la commande « scan » vers le réseau. Cela empêche Remote Manager de vérifier les résultats de la commande « scan ».

Résolution

Vous devrez peut-être vérifier l'état de la commande de scan via l'administrateur informatique de votre client.

L'outil de configuration de l'agent n'est pas visible après la mise à niveau de ce dernier

L'outil de configuration de l'agent n'est pas visible après la mise à niveau de ce dernier sur un système d'exploitation Windows Vista™ ou Windows Server 2008™. Avant la mise à niveau, l'utilisateur exécute habituellement l'outil de configuration de l'agent avec

le compte de l'utilisateur. Pendant le processus de mise à niveau, l'outil est arrêté puis redémarré par LocalSystem et non par le compte de l'utilisateur. C'est pourquoi l'utilisateur ne peut pas le voir bien qu'il soit en cours d'exécution.

Résolution

L'ordinateur doit être redémarré afin de relancer l'outil de configuration de l'agent avec le compte de l'utilisateur.

FAQ

Foire aux questions de la console Web

Pourquoi l'agent affiche la version 1.6 sur la console Remote Manager alors qu'il s'agit de la version 3.2 du serveur Remote Manager ?

Remote Manager 3.2 utilise toujours l'agent 1.6 (sur les serveurs antérieurs à WFBS 6.0) ; seule la version du serveur est 3.2.

Un revendeur peut-il avoir plusieurs comptes sur Remote Manager ?

Non. Avec Remote Manager 3.1, un revendeur ne peut avoir qu'un seul compte.

Lorsque Hosted Email Security est sélectionné dans la liste « Afficher par » au-dessus de l'arborescence clients, pourquoi l'arborescence est-elle toujours triée par nom de client ?

La sélection de HES filtre tous les clients HES ; elle n'entraîne pas de tri par HES. En d'autres termes, lorsque Hosted Email Security est sélectionné dans la liste déroulante, seuls les clients disposant de Hosted Email Security sont affichés.



Remarque

Les autres produits de ce client HES sont aussi affichés.

Pourquoi certains éléments de menu ou options sont-ils grisés ?

Il se peut que certains éléments de menus utilisés pour envoyer des commandes à un agent soient grisés. Cela peut se produire si un agent n'est pas encore enregistré sur le

serveur Remote Manager ou si les données nécessaires n'ont pas encore été communiquées (à cause d'un délai au niveau du réseau ou pour d'autres raisons).

Pourquoi ne puis-je pas modifier mon mot de passe sur Trend Micro Licensing Management Platform ?

Il est possible que Licensing Management Platform soit en cours de maintenance. Essayez de modifier votre mot de passe dans quelque temps. Si le problème persiste, contactez votre service d'assistance.

Je viens de mettre à jour quelque chose sur la console. Cependant, l'état reste le même. Qu'est-ce qui se passe ?

La synchronisation des données dans tous les services prend quelques minutes. La mise à jour de licences ou de postes, la réinitialisation de compteurs, etc. sont autant d'exemple de modifications retardées.

Je ne vois pas le service Worry-Free Business Security Services d'un client sur la console. Pourquoi ?

Si le service a expiré il y a 60 jours, il n'est plus répertorié.

J'ai cliqué sur le lien pour me connecter à Worry-Free Business Security Services. Le système renvoie une erreur. Pourquoi ?

Ceci se produit lorsque Worry-Free Business Security Services est arrêté à des fins de maintenance ou lorsque Licensing Management Platform rencontre un problème. Vous pouvez essayer de cliquer sur le lien après quelques temps.

Pourquoi le client que j'ai créé sur Licensing Management Platform n'est-il pas visible dans Remote Manager ?

La synchronisation des données dans tous les services prend quelques minutes.

Pourquoi le voyant « Serveurs gérés obsolètes » s'affiche-t-il toujours en rouge même après avoir cliqué sur le bouton Mettre à jour ?

Le bouton **Mettre à jour** envoie seulement des commandes au serveur Worry-Free Business Security Standard or Advanced. Voici ce qui peut se produire ensuite :

- Le serveur Worry-Free Business Security Standard or Advanced reçoit la commande de mise à jour mais, en raison de sa configuration, l'opération de mise à jour ne peut pas être effectuée.

- Le serveur Worry-Free Business Security Standard or Advanced a été mis à jour, mais la plupart des agents CSA qui en font partie ne l'ont pas été. C'est pourquoi il continue d'envoyer une alerte rouge à Remote Manager. La mise à jour de la plupart des agents CSA peut prendre quelques instants.

Foire aux questions Hosted Email Security

Pourquoi les données des 3 dernières heures ne sont-elles pas affichées dans l'état actuel ?

Sur le serveur Hosted Email Security (HES), la collecte des données a lieu sur une période de 2 heures. Pour garantir que le serveur Remote Manager aura intégré les données provenant du serveur Hosted Email Security, la collecte des données est retardée de 3 heures.

Pourquoi les options Synchroniser avec le serveur et Accéder à la console client sont-elles grisées lorsque je clique avec le bouton droit de la souris sur HES dans l'arborescence clients ?

Trois raisons peuvent expliquer pourquoi Hosted Email Security est inactif.

- Hosted Email Security n'a pas encore été connecté à Remote Manager.
- Le client a mis fin à la connexion. Consultez [Connexion d'un client Hosted Email Security à la console Remote Manager à la page 4-14](#).
- L'arborescence client doit être actualisée.

Pourquoi le message d'erreur « Votre client HES ne s'est pas connecté à Remote Manager ou a été déconnecté par HES. Contactez votre administrateur » s'affiche-t-il lors d'une tentative de redirection vers la console Hosted Email Security du client après une connexion par le client de Hosted Email Security à Remote Manager ?

Une fois que vous avez saisi le GUID ou la clé d'enregistrement et cliqué sur **Se connecter**, la connexion de Hosted Email Security à la console Web Remote Manager peut prendre jusqu'à dix minutes. Si le problème persiste, contactez l'assistance de Trend Micro.

Pourquoi le code d'activation et la date d'expiration d'un client HES s'affichent-ils à l'état « S/O » sur la console Web Remote Manager ?

Si un client Hosted Email Security n'a pas connecté le service Hosted Email Security à la console Remote Manager ou l'a déconnecté, Remote Manager ne peut pas récupérer les données. Il se peut aussi que Hosted Email Security ne parvienne pas à trouver un code d'activation et une date d'expiration valides pour ce client. Ce problème ne survient toutefois que rarement.

Foire aux questions sur les rapports

Le nombre de rapports pouvant être stockés est-il limité ?

Oui. Remote Manager limite le nombre de rapports stockés. Une fois le quota atteint, les rapports plus anciens sont automatiquement supprimés. Le nombre de rapports stockés est le suivant :

- **Rapports quotidiens** : un maximum de 30 rapports sont stockés.
- **Rapports hebdomadaires** : un maximum de 10 rapports sont stockés.
- **Rapports mensuels** : un maximum de 5 rapports sont stockés.

Pourquoi aucun rapport n'est-il généré ?

Vérifiez si le disque est saturé. Remote Manager offre actuellement 512 Mo d'espace. Essayez de télécharger quelques rapports sur votre disque local, supprimez-les de la console, puis réessayez de générer des rapports.

Pourquoi l'historique de rapports ne contient-il pas de nouveau rapport après la création d'un profil de rapport à usage unique ?

Patientez une ou deux minutes après la création d'un profil de rapport. Le rapport apparaîtra alors dans l'historique de rapports. Si le rapport n'est toujours pas généré, ouvrez le profil de rapport et enregistrez-le à nouveau. Si le problème persiste, contactez l'assistance de Trend Micro.

Pourquoi ne reçois-je aucun rapport quotidien/hebdomadaire/mensuel par e-mail lorsque l'historique de rapports contient des rapports ?

Vérifiez que l'adresse e-mail du client est valide et qu'elle est présente dans la liste des destinataires du profil de rapport. Si c'est le cas, il s'agit peut-être d'un problème de réseau.

Sur un rapport généré, pourquoi les heures des données ne sont-elles pas affichées conformément à mes paramètres de fuseau horaire ?

Le fuseau horaire utilisé dans le rapport dépend de celui qui a été sélectionné par le revendeur à la création du profil. Il n'est pas défini par l'ordinateur du client.

Que signifie « S/O » après la création d'un rapport à usage unique ?

Pour un rapport à usage unique, la colonne état affiche toujours « S/O ». Cela se produit parce qu'il n'existe pas d'état pour les rapports à usage unique (impossibles à désactiver, activer, interrompre, etc.).

Impossible d'afficher les rapports avec une connexion SSL (HTTPS).

L'option « Ne pas enregistrer les pages chiffrées sur le disque » est un paramètre de sécurité d'Internet Explorer 7.0/8.0 qui intervient dans le cadre de connexions SSL (HTTPS). Si vous activez ce paramètre, aucune donnée ne sera enregistrée dans la mémoire cache et vous ne pourrez pas afficher ni télécharger de rapports.

Afin de résoudre ce problème, dans IE 7.0 ou 8.0, cliquez sur **Outils > Options Internet > Avancé > Sécurité** et décochez l'option « **Ne pas enregistrer les pages chiffrées sur le disque** ».

Chapitre 12

Obtenir de l'aide

Cette section comprend les rubriques suivantes :

- *Comment contacter Trend Micro à la page 12-2*
- *Optimisation de la demande d'assistance à la page 12-2*
- *Utilisation du portail d'assistance à la page 12-3*
- *Encyclopédie des menaces à la page 12-3*
- *À propos de Trend Micro à la page 12-4*
- *TrendLabs à la page 12-5*

Comment contacter Trend Micro

En France, vous pouvez contacter les représentants de Trend Micro par téléphone ou message électronique :

Adresse	Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France
Tél. :	+33 (0) 1 76 68 65 00
Internet	www.trendmicro.fr
E-mail	support@trendmicro.com

- Centres d'assistance mondiaux :
<http://www.trendmicro.fr/apropos/contact/index.html>
- Documentations de produits Trend Micro :
<http://docs.trendmicro.com/fr-fr/home.aspx>

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 connecté à vos terminaux
- Quantité de mémoire et d'espace disque disponible
- Version du système d'exploitation et du Service Pack
- Version du client des terminaux
- Numéro de série ou code d'activation

- Description détaillée de l'environnement d'installation
- Texte exact du message d'erreur affiché.

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 <http://esupport.trendmicro.com>.
2. Sélectionnez un produit ou un service dans la liste déroulante appropriée et spécifiez toute autre information le concernant.

La page de produit **Assistance Technique** apparaît.
3. Utilisez la zone **Parcourir l'assistance** pour rechercher les solutions disponibles.
4. Si aucune solution n'est trouvée, cliquez sur **Envoyer une demande d'assistance** depuis le volet de navigation gauche et ajoutez tout détail pertinent ou envoyez une demande d'assistance ici :

<http://esupport.trendmicro.com/srf/srfmain.aspx>

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 <http://www.trendmicro.com/vinfo/fr/virusencyclo/default.asp> pour en savoir plus sur :

- Les programmes malveillants et les codes mobiles malicieux 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
- Les rapports hebdomadaires sur les programmes malveillants.

À propos de Trend Micro

En tant que leader mondial de la sécurité cloud, Trend Micro développe des solutions de sécurité de contenu Internet et de gestion des menaces pour que les entreprises et les consommateurs puissent échanger des informations numériques dans un environnement sécurisé. Avec plus de 20 ans d'expérience, Trend Micro fournit des solutions client, serveur et cloud de premier plan qui arrêtent les menaces plus rapidement et qui protègent les données des environnements physiques, virtuels et cloud.

À mesure de l'apparition de nouvelles menaces et failles, Trend Micro s'engage à aider les clients à sécuriser les données, à assurer la conformité, à réduire les coûts et à protéger l'intégrité de l'entreprise. Pour plus d'informations, rendez-vous sur :

<http://www.trendmicro.com>

Trend Micro et le logo t-ball de Trend Micro sont des marques commerciales de Trend Micro Incorporated et sont enregistrées dans certains pays. Toutes les autres marques sont des marques commerciales ou déposées de leurs propriétaires respectifs.

TrendLabs

TrendLabsSM est un réseau mondial de centres de recherche, de développement et d'action qui s'engage à surveiller les menaces, à prévenir les attaques et à fournir des solutions transparentes et en temps opportun 24 h/24 et 7 j/7. Jouant le rôle de la colonne vertébrale de l'infrastructure des services de Trend Micro, TrendLabs est constitué d'une équipe de plusieurs centaines d'ingénieurs et de personnel d'assistance qualifié qui fournissent une large gamme de services d'assistance technique et de produits.

TrendLabs surveille l'environnement mondial des menaces afin de fournir des mesures de sécurité efficaces pour pouvoir détecter, anticiper et éliminer les attaques. Tous ces efforts sont partagés avec les clients via des mises à jour de fichiers de signatures de virus fréquentes et des perfectionnements des moteurs de scan.

Pour en savoir plus sur TrendLabs, rendez-vous sur :

<http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs>

Index

A

assistance

base de connaissances, 12-3

résout les problèmes plus rapidement,

12-2

TrendLabs, 12-5

C

conventions typographiques du document,

viii

T

TrendLabs, 12-5



TREND MICRO INCORPORATED

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

www.trendmicro.fr

Code élément : APFM36398/140410