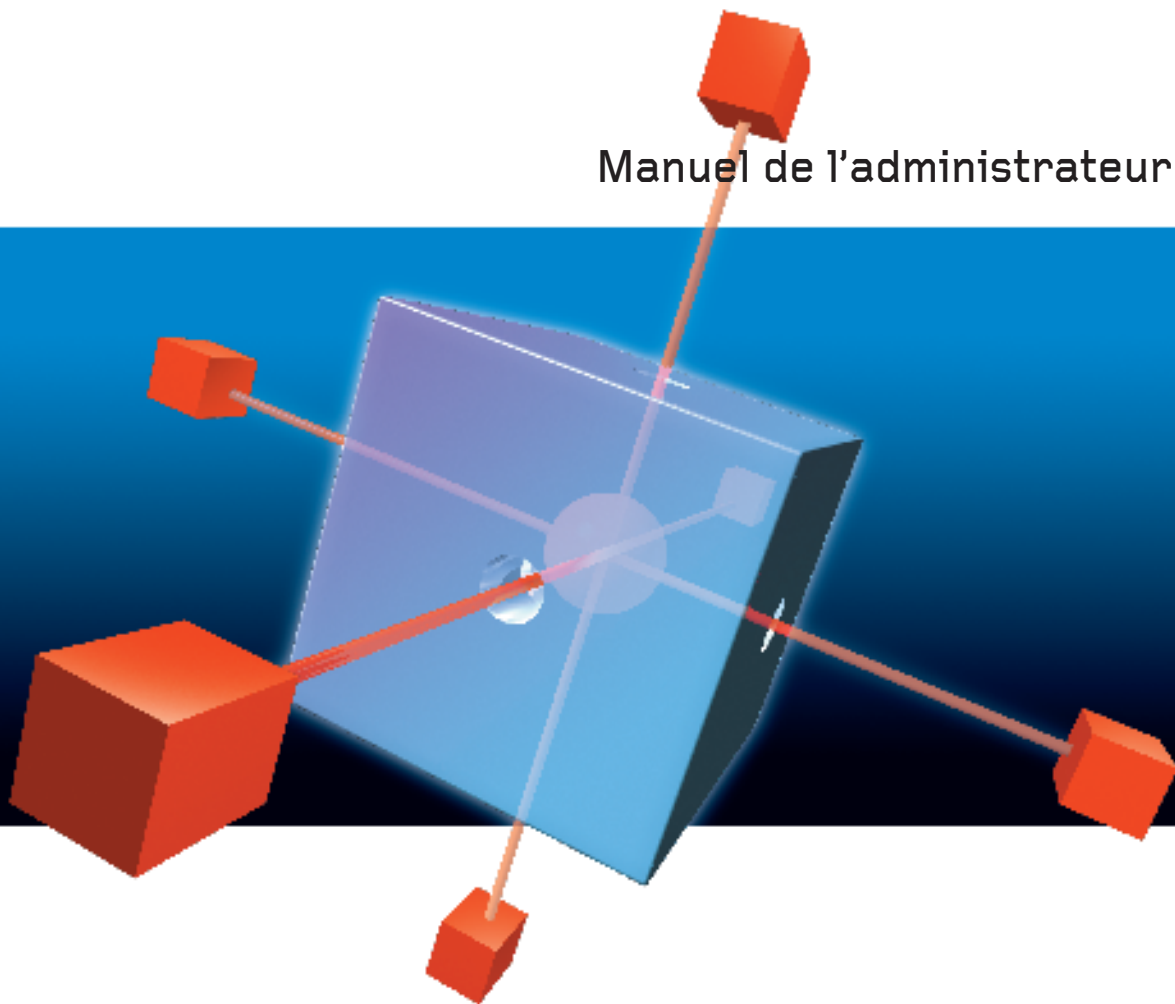


TREND MICRO™

OfficeScan™ 7

Protection complète pour les postes de travail d'entreprise

Manuel de l'administrateur



Trend Micro Incorporated se réserve le droit de modifier ce document et les produits décrits ici sans préavis. Avant d'installer et d'utiliser le logiciel, veuillez lire les fichiers Lisez-moi, les notes de mise à jour et la toute dernière version de la documentation utilisateur applicable, disponibles sur le site Web de Trend Micro à l'adresse suivante :

<http://www.trendmicro-europe.com/download>

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

Copyright©2005-2006 Trend Micro Incorporated. Tous droits réservés.

Partie du document n° OSEM72658/60206

Date de publication : janvier 2006

Protégée par le brevet américain n° 5,623,600; 5,889,943; 5,951,698; 6.119,165

La documentation utilisateur pour Trend Micro OfficeScan présente les fonctions principales du logiciel et les instructions d'installation pour votre environnement de production. Nous vous conseillons de lire cette documentation avant d'installer ou d'utiliser le logiciel.

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

Sommaire

Chapitre 1: Présentation d'OfficeScan™

Nouveautés de la version OfficeScan 7.3	1-3
Nouvelles fonctionnalités côté client	1-3
Nouvelles fonctionnalités côté serveur	1-5
La technologie OfficeScan	1-6
Définition des virus	1-6
Définition des programmes espions et autres types de graywares	1-7
Définition des composants OfficeScan	1-9
Possibilités offertes par OfficeScan	1-15
Avantages et capacités	1-18
Architecture du serveur OfficeScan	1-20
Serveur OfficeScan	1-20
Client OfficeScan	1-22
Clients 32 et 64 bits	1-25
Console Web	1-26
Utilisation de la Documentation OfficeScan	1-27

Chapitre 2: Démarrage d'OfficeScan

Exploration de la console Web	2-2
Présentation de la console Web	2-3
Autres liens disponibles sur la console	2-8
Définition de l'arborescence du domaine d'OfficeScan	2-9
Définition des icônes de l'arborescence du domaine	2-10
Utilisation des domaines OfficeScan	2-10
Sélection de clients et de domaines OfficeScan dans l'arborescence des domaines	2-12
Recherche de clients	2-13
Mise à jour d'OfficeScan	2-15
Choisir une source de mise à jour	2-15
Mise à jour du serveur	2-17
Utilisation d'un agent de mise à jour	2-21
Mise à jour des clients	2-24
Utilisation de la mise à jour programmée avec le mode NAT	2-33
Rétrogradation des composants	2-34
Vérification de la Connexion serveur-client	2-36
Configuration des alertes	2-38
Utilisation des variables de jetons avec les alertes standards et les alertes d'épidémie	2-39
Configuration des alertes standards	2-40
Configuration des alertes d'épidémies	2-42
Modification des messages d'alerte du client	2-45
Définition des options de scan	2-46
À propos de ActiveAction	2-47
À propos de IntelliScan	2-48
Configuration du scan manuel	2-48
Configuration du scan en temps réel	2-51
Configuration du scan programmé	2-54
Fichiers et dossiers exclus des actions de scan	2-57
Exécution du scan immédiat	2-59
Configuration des privilèges et paramètres clients	2-63
Configuration des paramètres généraux	2-67
Importation et exportation des stratégies	2-71

Chapitre 3: Suppression des programmes espions, des autres types de graywares, et des menaces des chevaux de Troie

Définition des programmes espions et autres types de graywares	3-2
Types de graywares	3-2
Le mode d'infiltration des programmes espions et autres graywares sur votre réseau	3-3
Risques et menaces potentiels	3-3
La solution Trend Micro	3-4
Grayware inconnu	3-4
À propos d'ActiveX	3-5
Fonctionnement des services Damage Cleanup	3-6
Chevaux de Troie	3-6
Graywares	3-6
La solution Services Damage Cleanup	3-6
Exécution du nettoyage immédiat	3-8
Configuration des paramètres anti-programmes espions	3-9
Affichage du Pourcentage de protection contre les programmes espions	3-11
Protection contre les programmes espions	3-12

Chapitre 4: Exécution des tâches administratives supplémentaires

Modification du mot de passe de la console Web	4-2
Définition du proxy intranet	4-3
Modification des informations du serveur Web OfficeScan	4-4
Suppression des clients inactifs	4-5
Configuration du gestionnaire de quarantaine	4-6
Participation au programme international de pistage des virus	4-7
Sauvegarde de la base de données OfficeScan	4-8

Chapitre 5: Gestion des épidémies

Mise en œuvre de la prévention contre les épidémies virales	5-2
Blocage des dossiers partagés	5-2
Blocage des ports	5-4
Accès en écriture interdit aux fichiers et aux dossiers	5-7
Configuration de la notification des clients en cas d'épidémies	5-9
Désactivation de la prévention des épidémies	5-10
Configuration du moniteur d'activité virale	5-11

Chapitre 6: Configuration du Pare-feu pour clients – version d’entreprise

Définition du Pare-feu pour clients – version d’entreprise	6-2
Définition des stratégies, des exceptions et des profils	6-3
Pare-feu par défaut	6-5
Fonctions du Pare-feu pour clients – version d’entreprise	6-6
Déploiement du pare-feu	6-9
Vérification du déploiement	6-12
Configuration du Pare-feu pour clients – version d’entreprise	6-13
Configuration des stratégies	6-13
Configuration des exceptions	6-14
Configuration des profils	6-18
Configuration du moniteur d'activité virale du pare-feu	6-21
Test du pare-feu	6-22
Désactivation du pare-feu	6-23

Chapitre 7: Affichage et interprétation des journaux

Affichage et interprétation des journaux	7-2
Affichage des journaux de virus	7-2
Suppression des journaux de virus	7-4
Affichage des journaux de mise à jour du serveur	7-5
Affichage des journaux de mise à jour du client	7-5
Affichage des journaux des événements du système	7-6
Affichage des journaux de vérification de la connexion	7-7
Affichage des journaux du pare-feu pour clients – version d'entreprise	7-8
Gestion des journaux	7-9

Chapitre 8: Utilisation des outils administrateurs et clients

Résumé des outils	8-2
Outils administrateurs	8-3
Configuration du script de connexion	8-3
Vulnerability Scanner	8-3
Server Tuner	8-9
Outils clients	8-10
Client Packager	8-10
Utilitaire de création d'image	8-10

Décodeur de fichiers	8-11
Client Mover I	8-13
Outil Touch	8-15
Outil ServerProtect Normal Server Migration	8-16
Outils intégrés	8-19
Client Mover II	8-19
Sauvegarde de la base de données	8-19
Database Packer	8-19
Icon Cleaner	8-20
Network Scan Switch	8-20
Register Shell	8-20
Remote Agent	8-21
GUID Changer	8-21

Chapitre 9: Questions fréquemment posées, Dépannage et Support technique

Foire aux questions (FAQ)	9-2
Installation et mise à niveau	9-2
Enregistrement	9-2
Compatibilité	9-2
Pare-feu pour clients – version d’entreprise	9-3
Mise à jour du serveur et des clients	9-4
Messages d'alerte	9-5
Scan en cours	9-5
Support technique du serveur de stratégie de Trend Micro pour Cisco Network Admission Control (NAC)	9-6
Console Web	9-7
Documentation	9-7
Dépannage	9-8
Communication client-serveur	9-8
Le client OfficeScan ne s'installera pas sur des ordinateurs exécutant Windows XP	9-8
Certains composants OfficeScan ne sont pas installés	9-8
Impossible d’accéder à la console Web	9-9
Nombre de clients incorrect sur la console Web	9-10
Etat du client incorrect sur la console Web	9-11
Les numéros de versions des composants sont incorrects	9-12

Echec de l'installation à partir d'une page Web ou avec installateur à distance	9-13
L'icône du client n'apparaît pas sur la console Web après l'installation	9-14
Problèmes pendant la migration à partir d'un logiciel antivirus tiers	9-15
Le délai de connexion du client se produit fréquemment	9-17
Téléchargement impossible du courrier électronique (POP3)	9-18
Problèmes dans les environnements utilisant le mode Traduction d'adresses réseau (NAT)	9-19
Contacteur Trend Micro	9-20
Le Centre d'informations sur les virus de Trend Micro	9-20
Problèmes connus	9-21
Contacteur le Support technique	9-22
La Base de connaissances Trend Micro	9-23
Envoi de fichiers suspects à Trend Micro	9-23
À propos de TrendLabs	9-24

Annexe A: Policy Server pour Cisco™ NAC Primer

Présentation de Trend Micro Policy Server pour Cisco NAC	A-2
Composants et terminologie	A-3
Composants	A-3
Terminologie	A-4
Architecture Cisco NAC	A-5
La séquence de validation du client	A-6
Définition du serveur de stratégie	A-8
Définition du serveur de stratégie, des stratégies et des règles	A-9
Définition de la synchronisation	A-16
Définition des certificats	A-16
Définition du certificat CA	A-18
Configuration minimale requise pour le serveur de stratégie	A-19
Configuration requise pour Cisco Trust Agent (CTA)	A-20
Modèles de dispositifs Cisco acceptés	A-20

Annexe B: Déploiement du Policy Server pour Cisco NAC

Présentation générale du déploiement de Policy Server pour NAC ..	B-2
Inscription du serveur ACS sécurisé de Cisco :	B-4
Exporter et installer le certificat CA	B-8
Préparation du certificat SSL du serveur de stratégie	B-10
Déploiement de Cisco Trust Agent	B-13
Mise à niveau et déploiement de Cisco Trust Agent 2.0	B-15
Vérification de l'installation de Cisco Trust Agent	B-15
Installation du Policy Server pour Cisco NAC	B-16
Configuration du serveur ACS	B-19
Configuration du Policy Server pour Cisco NAC	B-21
Ajout et suppression de serveurs de stratégie	B-22
Consultez le résumé des informations d'un serveur de stratégie	B-23
Ajout ou modification de serveurs OfficeScan	B-26
Configuration des règles	B-28
Configuration des stratégies	B-30
Utilisation des journaux de validation du client	B-33
Exécution des tâches d'administration	B-35

Annexe C: Utilisation de Control Manager™ avec OfficeScan

Présentation du Control Manager	C-2
Possibilités offertes par Control Manager et OfficeScan	C-2
Présentation de Control Manager Agent	C-3
Prérequis à l'installation de l'Agent	C-3
Informations requises pour l'installation de l'agent	C-4
Obtention de la Clé d'encodage publique	C-4
Installation de l'agent Control Manager	C-5
Accès à OfficeScan par le Control Manager	C-8
Suppression de l'agent	C-9

Annexe D: Configuration d'OfficeScan grâce à des compagnons et des logiciels tiers

À propos de Wireless Protection Manager	D-2
Configuration minimale requise du PDA	D-3
Installation de Wireless Protection Manager	D-4
Utilisation de Wireless Protection Manager	D-5
Mise à jour OfficeScan pour Wireless	D-5
Téléchargement des mises à jour des composants	D-6
Activation de la configuration des paramètres proxy	D-7
Synchronisation avec votre PDA	D-8
Utilisation des journaux	D-8
Aperçu de l'architecture et de la configuration de	
Check Point Firewall	D-10
Intégration avec OfficeScan	D-11
Configuration de Check Point pour OfficeScan	D-13
Installation du support SecureClient sur le client OfficeScan	D-15

Annexe E: Glossaire terminologique

Présentation d'OfficeScan™

OfficeScan de Trend Micro est une solution antivirus à gestion centralisée, contre les programmes espions, destinée aux postes de travail, aux ordinateurs portables et aux serveurs. OfficeScan protège les ordinateurs Windows™ NT/2000/XP/Server 2003 et Windows 95/98/Me de votre entreprise contre un grand nombre de menaces et de nuisances potentielles telles que les virus de fichiers, les virus de macros ainsi que les applets Java™ et les contrôles ActiveX™ malicieux.

Dans OfficeScan, la fonction antivirus est fournie via le client qui communique avec le serveur et obtient les mises à jour à partir de ce dernier. La console Web OfficeScan vous permet de configurer, de surveiller et de mettre à jour les clients.

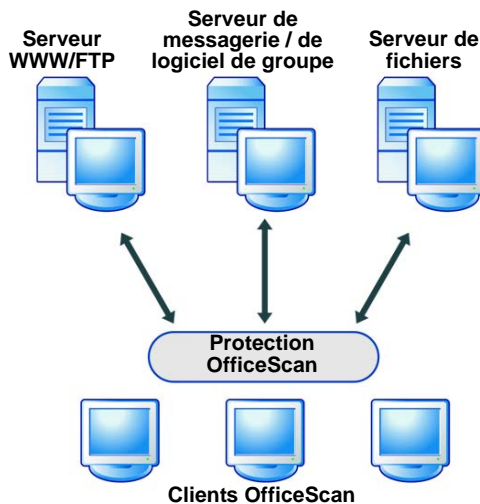


FIGURE 1-1 Protection OfficeScan

OfficeScan comprend :

- le serveur OfficeScan, qui héberge la console Web, télécharge des mises à jour du serveur Trend Micro ActiveUpdate, collecte et enregistre des journaux et vous aide à contrôler les attaques de virus ;
- OfficeScan client, qui protège vos ordinateurs Windows NT/2000/XP/Server2003 et Windows 95/98/Me contre les virus, chevaux de Troie et autres menaces ;
- la console de management OfficeScan, aussi appelée console Web, utilisée pour gérer vos clients depuis un emplacement unique.

Nouveautés de la version OfficeScan 7.3

Cette version d'OfficeScan dispose de toutes les fonctions des précédentes versions et offre les nouvelles fonctions suivantes :

Nouvelles fonctionnalités côté client

- **Protection contre les programmes espions et autres types de graywares :**
OfficeScan peut vous aider à protéger vos ordinateurs contre les diverses menaces et nuisances potentielles que Trend Micro classe comme *graywares*, y compris le type le plus connu – programme espion (voir *Définition des programmes espions et autres types de graywares* à la page 1-7 pour obtenir de plus amples informations). OfficeScan scanne et nettoie les programmes espions et autres graywares tout comme les virus et les chevaux de Troie. Cependant, vous pouvez souhaiter que les clients conservent certaines applications que OfficeScan considère comme graywares. Pour empêcher OfficeScan de répertorier en permanence ces applications comme étant des graywares, vous pouvez configurer une liste d'exceptions spécifiques aux graywares.
- **Prise en charge des plates-formes Windows server pour les clients :** installez le client OfficeScan sur tout serveur Windows, tel que Windows Server 2003. Reportez-vous au *Guide de déploiement et d'installation* pour obtenir de plus amples renseignements.
- **Mise à jour incrémentielle :** pour les fichiers de signatures (y compris la signature de scan pour les programmes espions, la signature Cleanup de programmes espions et le modèle Damage Cleanup) dont sept versions de fichiers de signatures sont disponibles sur le serveur OfficeScan. Les clients OfficeScan peuvent mettre à jour leurs fichiers de façon incrémentielle au lieu d'actualiser l'ensemble des fichiers. Cela limite le temps et la bande passante nécessaires pour la mise à jour des clients OfficeScan.
- **Amélioration de la mise à jour programmée des clients :** configurez les clients OfficeScan pour effectuer des mises à jour de composants programmées à la minute près. Autorisez également les utilisateurs du client OfficeScan à modifier les paramètres des mises à jour programmées.
- **Scan des fichiers adaptable :** afin que les ressources des CPU clients soient moins sollicitées par le scan des fichiers, réglez manuellement le temps d'attente entre le scan d'un fichier et le suivant.

- **Prise en charge des plates-formes Windows server sur différentes architectures de processeur** : exécution d'OfficeScan sur Windows 2000, NT et Server 2003. OfficeScan est compatible avec les ordinateurs équipés de Windows XP/Server 2003 et dotés d'une architecture processeur 64 bits Itanium 2 (IA-64) et x86. Consultez la rubrique *Clients 32 et 64 bits* à la page 1-25 pour obtenir plus d'informations.
- **Contrôle des journaux des virus réseau/réduction de la bande passante** : un simple virus réseau peut souvent donner lieu à un grand nombre d'épidémies dans un court laps de temps. Si OfficeScan détecte plusieurs infections récurrentes causées par le même virus réseau, il consolide les entrées de journal créées lors des détections et les envoie au serveur OfficeScan toutes les heures. Cela permet de réduire la bande passante nécessaire pour les journaux ainsi que le nombre de notifications de détection de virus envoyées à vos administrateurs IT.
- **Liste d'exclusion des programmes espions/graywares** : OfficeScan peut identifier certains types de fichiers en tant que graywares bien que des applications légitimes de votre ordinateur puissent en avoir besoin. Pour éviter qu'OfficeScan n'identifie ces fichiers en tant que graywares, configurez la liste d'exclusion critique des programmes espions/graywares qui s'applique à tous les types de scan.
- **Serveurs alternatifs pour application de règles de pare-feu** : les ordinateurs clients peuvent ne pas être connectés à un serveur OfficeScan mais être connectés à d'autres ordinateurs que vous avez définis en tant que serveurs OfficeScan alternatifs. Dans ce cas, le programme client OfficeScan considère que ces ordinateurs clients sont « en ligne » et les règles de pare-feu à appliquer uniquement aux clients en ligne peuvent donc être appliquées à ces clients.
- **Prise en charge de Cisco NAC version 2.0** : il suffit d'une simple mise à niveau de Cisco Trust Agent pour permettre aux clients OfficeScan de continuer à envoyer leurs informations sur les virus aux comptes serveurs à accès contrôlé et serveurs de stratégie dans un système Cisco NAC version 2.0.

Nouvelles fonctionnalités côté serveur

- **Intégration de la sauvegarde de la base de données** : vous pouvez créer une sauvegarde de la base de données OfficeScan manuellement à tout moment ou configurer un programme de sauvegarde automatique par la console Web. S'il y a le moindre problème d'intégrité lié à votre base de données OfficeScan, vous pouvez restaurer vos paramètres à partir de la sauvegarde.
- **Plusieurs sources de mise à jour** : vous pouvez configurer jusqu'à 10 sources de mise à jour tant pour les mises à jour programmées que manuelles.
- **Outil de migration pour ServerProtect Normal Server** : utilisez cet outil Windows pour vous aider dans le processus de migration vers le client OfficeScan d'ordinateurs exécutant Trend Micro™ ServerProtect Normal Server.
- **Support technique pour l'installation de serveurs multiples et de serveurs distants** : installation ou mise à niveau du serveur OfficeScan sur plusieurs serveurs distants simultanément.
- **Journaux des virus réseau communiqués au Control Manager** : autorisez les clients à envoyer leurs journaux de virus réseau au serveur OfficeScan, lequel, en retour, les enverra à un serveur Control Manager enregistré. Utilisez ces informations dans Control Manager pour générer des rapports d'analyse de virus de réseau.

La technologie OfficeScan

OfficeScan utilise une technologie fiable de recherche et de suppression de virus afin de vous aider à protéger votre environnement réseau des codes malicieux.

Définition des virus

Il existe des milliers de virus, de nouveaux sont créés chaque jour. Auparavant, la plupart des virus étaient basés sur des fichiers et se répandaient lors de l'échange de disquettes. Actuellement, les virus se répandent couramment via Internet, en exploitant les points sensibles des réseaux d'entreprise, les systèmes de messagerie électronique et les applications telles que les navigateurs Web.

La plupart des virus informatiques font partie des catégories suivantes :

- **Code ActiveX malicieux** : réside dans les pages Web qui exécutent des contrôles ActiveX
- **Virus du secteur d'amorçage** : infectent le secteur d'amorçage d'une partition ou d'un disque
- **Virus qui infectent les fichiers COM et EXE** : programmes exécutables avec extensions .com ou .exe
- **Code Java malicieux** : virus indépendant du système d'exploitation écrit ou incorporé à Java
- **Virus Macro** : encodés comme application macro et qui se trouvent souvent dans un document
- **Chevaux de Troie** : programmes exécutables qui ne se multiplient pas mais reposent sur les systèmes pour effectuer des opérations malveillantes telles que l'ouverture des ports aux pirates
- **Virus HTML, VBScript ou JavaScript** : résident dans des pages Web et sont téléchargés par un navigateur.
- **Vers** : programme automatique (ou ensemble de programmes) qui peut répandre des copies fonctionnelles de lui-même ou de ses segments dans d'autres systèmes informatiques, souvent par courrier électronique
- **Packers** : programmes exécutables compressés et/ou encodés Windows ou Linux, souvent des chevaux de Troie. La compression de fichiers exécutables les rend plus difficiles à détecter par les logiciels antivirus.

Virus de réseau

Un virus qui se répand sur le réseau n'est pas, à strictement parler, un virus réseau. Seules certaines des menaces mentionnées ci-dessus, comme les vers, peuvent être appelées virus de réseau. Plus spécifiquement, les virus de réseau utilisent les protocoles réseaux tels que TCP, FTP, UDP, HTTP et e-mail pour se multiplier. Souvent, ils n'affectent pas les fichiers systèmes ou ne modifient pas les secteurs d'amorçage des disques durs. Par contre, les virus de réseau infectent la mémoire des postes clients en l'obligeant à inonder le réseau de trafic, ce qui peut entraîner des ralentissements, voire même une panne complète du réseau. Comme les virus de réseau restent en mémoire, ils sont souvent indétectables par les méthodes de recherche conventionnelles sur le disque, qui sont axées sur l'examen des fichiers entrants et sortants.

Le pare-feu pour clients – version d'entreprise fonctionne avec un fichier de signatures de virus réseau afin d'identifier et de bloquer ces derniers (consultez la rubrique *Configuration du Pare-feu pour clients – version d'entreprise* à la page 6-1 pour obtenir de plus amples informations à ce sujet).

Définition des programmes espions et autres types de graywares

Vos ordinateurs courent d'autres menaces potentielles que les virus. Les graywares sont des applications ou des fichiers non répertoriés comme virus ou chevaux de Troie mais pouvant toutefois avoir un effet négatif sur les performances des ordinateurs de votre réseau. Ils font courir un risque significatif à la sécurité, à la confidentialité et à la légalité de votre entreprise. Les graywares réalisent souvent des actions variées non souhaitées et menaçantes qui irritent les utilisateurs avec des fenêtres pop-up, enregistrent les séquences de frappe des touches du clavier et exposent les failles de l'ordinateur à des attaques.

Types de graywares

OfficeScan est à même de détecter plusieurs types de graywares, y compris les suivants :

- **Programmes espions** : récoltent des données, telles que des noms d'utilisateur de compte, de mots de passe, des numéros de cartes de crédit et d'autres informations confidentielles pour les transmettre à des tiers
- **Programmes publicitaires** : affichent des publicités et récoltent des données utilisateurs, telles que des préférences de navigation, pouvant être utilisées à des fins publicitaires
- **Composeurs de numéros** : modifient les paramètres Internet et obligent un ordinateur à composer des numéros de téléphone préconfigurés à l'aide d'un modem. Ce sont souvent des numéros de services téléphoniques facturés à l'utilisation (pay-per-call) ou internationaux qui peuvent entraîner une dépense significative pour votre société.
- **Canulars** : entraîne un fonctionnement anormal d'un ordinateur, en faisant par exemple vibrer l'écran ou en modifiant l'apparence du curseur
- **Outils de piratage** : aident les pirates informatiques malveillants à s'infiltrer sur un ordinateur
- **Outils d'accès à distance** : aident les pirates informatiques malveillants à accéder à distance à un ordinateur et à le contrôler
- **Applications de piratage des mots de passe** : aident à déchiffrer des noms d'utilisateurs et des mots de passe
- **Autres** : autres types de programmes potentiellement malveillants

Définition des composants OfficeScan

OfficeScan utilise les composants suivants pour identifier et effectuer les tâches de nettoyage des dommages, afin de contribuer à protéger et à nettoyer les clients OfficeScan :

- **Programme client** : le programme client OfficeScan, utilise le fichier de signatures des virus et le moteur de scan pour identifier les infections et entreprendre les actions nécessaires sur les fichiers infectés
- **Moteur de scan** : le moteur utilisé par OfficeScan pour rechercher les virus
- **Fichier de signatures des virus** : fichier qui aide OfficeScan à identifier les signatures de virus – signatures uniques des octets et des bits qui signalent la présence d'un virus (consultez la rubrique *À propos du fichier de signatures des virus* à la page 1-10 pour obtenir de plus amples informations)
- **Moteur Damage Cleanup** : le moteur utilisé par les services Damage Cleanup pour rechercher et supprimer les chevaux de Troie et leurs processus
- **Modèle Damage Cleanup** : modèle utilisé par le moteur Damage Cleanup qui contribue à identifier les fichiers des chevaux de Troie et leurs processus, de manière à les éliminer
- **Signature de scan pour les programmes espions/graywares** : un fichier aidant OfficeScan à identifier les signatures de virus, signature unique des octets et bits, et signaler la présence de certains types de fichiers et de programmes indésirables tels que les logiciels publicitaires et les logiciels espions
- **Signature pour le nettoyage des programmes espions/graywares** : fichier utilisé par le moteur Damage Cleanup pour aider à éliminer les fichiers espions/publicitaires et leurs processus
- **Pilote du pare-feu commun** : le pare-feu pour clients – version d'entreprise utilise le pilote contenant les signatures de virus réseau pour rechercher ces derniers sur les postes clients
- **Fichier de signatures des virus réseau** : comme le fichier de signatures des virus, ce fichier aide OfficeScan à identifier les signatures de virus
- **Cisco Trust Agent (si Policy Server pour Cisco NAC est installé)** : le programme qui active la communication entre le client OfficeScan et les routeurs qui prennent en charge Cisco NAC.
- **Correctifs (hot fixes) et correctifs de sécurité** : solutions globales pour les problèmes liés à la clientèle ou les failles récemment découvertes en matière de sécurité que vous pouvez télécharger à partir du site Web de Trend Micro et déployer vers le serveur OfficeScan et/ou le programme client.

Outre ces composants, les clients OfficeScan reçoivent également des fichiers de configuration mis à jour du serveur OfficeScan. Les clients ont besoin des fichiers de configuration pour appliquer les nouveaux paramètres. Chaque fois que vous modifiez les paramètres OfficeScan via la console Web, le fichier de configuration est modifié.

À propos du fichier de signatures des virus

Le moteur de scan Trend Micro utilise un fichier de données externe appelé fichier de signatures des virus. Il contient des informations qui aident OfficeScan à identifier les virus les plus récents et autres menaces Internet, telles que les chevaux de Troie, les expéditeurs de courrier en masse, les vers et les attaques mixtes. De nouveaux fichiers de signatures des virus sont créés et publiés plusieurs fois par semaine et à chaque fois qu'une menace particulière est découverte.

Tous les programmes antivirus Trend Micro qui utilisent la fonction ActiveUpdate peuvent détecter la présence d'un nouveau fichier de signatures des virus sur le serveur Trend Micro et / ou peuvent être programmés pour se connecter automatiquement au serveur une fois par semaine, par jour ou par heure afin d'y télécharger le fichier le plus récent.

Conseil : Trend Micro vous conseille de programmer les mises à jour automatiques au moins une fois par semaine, qui est le paramètre par défaut de tous les produits livrés.

Vous pouvez télécharger les fichiers de signatures des virus à partir du site Web suivant, sur lequel vous trouverez la version actuelle, sa date d'émission et une liste de toutes les nouvelles définitions de virus comprises dans le fichier :

<http://fr.trendmicro-europe.com/enterprise/support/pattern.php>

Le moteur de scan travaille avec le fichier de signatures des virus afin de réaliser le premier niveau de détection en utilisant un processus appelé correspondance de signature. Comme chaque virus contient une « signature » ou une chaîne de caractères unique, le distinguant de tous les autres codes, les experts de TrendLabs™ capturent des parties inertes de ce code dans le fichier de signatures. Le moteur compare alors certaines parties de chaque fichier scanné aux signatures qui se trouvent dans le fichier de signatures, afin de rechercher les correspondances. Lorsqu'une correspondance est découverte, un virus a été détecté et une notification est envoyée par message électronique à l'administrateur du système.

Numérotation du fichier de signatures

Pour vous permettre de comparer le fichier de signatures actuel de vos produits logiciels aux fichiers de signatures les plus récents disponibles chez Trend Micro, les fichiers de signatures portent un numéro de version.

Il existe actuellement deux systèmes de numérotation des fichiers de signatures chez Trend Micro.

1. Le modèle traditionnel de numéro de fichier est de 3 chiffres, sous le format *xxx*, par exemple : 786.
2. Le nouveau système de numérotation du fichier de signatures, entré en vigueur en 2003, utilise 6 chiffres sous le format *x.xxx.xx*.
 - Le premier chiffre est actuellement fixé à 2, il indique le nouveau système de numérotation.
 - Les 3 chiffres suivants représentent le numéro de fichier de signatures traditionnel.
 - Les 2 derniers chiffres donnent des informations complémentaires au sujet de l'édition du fichier de signatures, ces informations sont destinées aux ingénieurs Trend Micro.

L'édition 786 dans le nouveau format peut être numérotée 1.786.01.

Gardez votre fichier de signatures à jour et veillez à disposer de la version actuelle afin de vous protéger contre les menaces les plus courantes.

À propos du moteur de scan Trend Micro

Un moteur de scan est la partie centrale de tous les produits Trend Micro. Initialement développé pour répondre aux premiers virus en mode fichier, le moteur de scan est devenu un outil exceptionnellement sophistiqué et capable de détecter des vers Internet, des expéditeurs de courrier en masse, des menaces représentées par les chevaux de Troie, les sites hameçon, les logiciels espions et les formes d'exploitation du réseau, ainsi que les virus. Le moteur de scan détecte deux types de menaces :

- « dans la nature » – qui circulent activement
- « en cage » – virus contrôlés qui ne sont pas en circulation mais qui sont développés et utilisés à des fins de recherche

Plutôt que de scanner chaque partie de chaque fichier, le moteur et le fichier de signatures travaillent ensemble à la fois pour identifier les caractéristiques révélatrices du code de virus, mais aussi pour trouver l'emplacement précis d'un fichier où le virus est susceptible de se cacher. Si OfficeScan détecte un virus, il peut le supprimer et restaurer l'intégrité du fichier.

Le moteur de scan comprend une routine de nettoyage automatique des anciens fichiers de signatures des virus (contribue à gérer l'espace disque), ainsi que des mises à jour de signatures incrémentielles (contribue à gérer la bande passante).

De plus, le moteur de scan est capable de décoder les principaux formats d'encodage (y compris MIME et BinHex). Il reconnaît et vérifie aussi les formats de compression communs, entre autres Zip, Arj et Cab. OfficeScan vous permet aussi de déterminer le nombre de couches de compression qu'il convient de scanner (jusqu'à maximum 20), dans les fichiers comprimés contenus dans un fichier.

Il est important que le moteur de scan reste à jour pour les nouvelles menaces. Trend Micro garantit cette mise à jour de deux façons :

- De fréquentes mises à jour du fichier de signatures, qui peut être téléchargé et lu par le moteur de scan, sans que le code du moteur soit modifié (consultez la rubrique suivante *À propos du fichier de signatures des virus* à la page 1-10)
- Des mises à jour technologiques dans le logiciel du moteur, déclenchés par une modification de la nature des menaces des virus, par exemple une augmentation des menaces mixtes telles que SQL Slammer

Le moteur de scan Trend Micro est certifié chaque année par des organisations internationales de sécurité informatique, par exemple l'ICSA (International Computer Security Association).

Mise à jour du moteur de scan

Grâce à l'enregistrement des informations de virus les plus sensibles au temps dans le fichier de signatures des virus, Trend Micro peut minimiser le nombre de mises à jour du moteur de scan, tout en maintenant la protection à jour. Trend Micro met néanmoins périodiquement à disposition de nouvelles versions du moteur du scan. Trend Micro émet de nouveaux moteurs dans les circonstances suivantes :

- De nouvelles technologies de recherche et de détection sont intégrées dans le logiciel
- Un nouveau virus, potentiellement dangereux est découvert et le moteur de scan n'est pas capable de le traiter

- Les performances de recherche sont améliorées
- Une assistance est ajoutée pour les formats de fichiers supplémentaires, pour les langages d'élaboration de script, les encodages et / ou les formats de compression

Pour consulter le numéro de la version la plus récente du moteur de scan, consultez le site Web Trend Micro :

<http://www.trendmicro-europe.com>

À propos des correctifs, corrections, et service packs

Après la publication officielle d'un produit, Trend Micro développe souvent des correctifs (hot fixes), corrections et service packs afin de corriger les problèmes, améliorer les performances des produits et ajouter de nouvelles fonctionnalités.

Le paragraphe suivant résume les éléments que Trend Micro peut publier :

- **Correctif (hot fix)** : moyen ou solution à un problème signalé par un seul utilisateur. Les correctifs (hot fixes) sont spécifiques à un problème et ne sont dès lors pas proposés à tous les clients. Les correctifs (hot fixes) Windows contiennent un programme d'installation, contrairement aux autres. En général, vous devez arrêter les démons, copier le fichier pour remplacer celui de l'installation, puis redémarrer les démons.
- **Correctif de sécurité** : correctif (hot fix) centré sur les problèmes de sécurité pouvant être déployé sur tous les clients. Les correctifs de sécurité Windows comprennent un programme d'installation, alors que les correctifs non-Windows disposent en général d'un script d'installation.
- **Correctif** : groupe de correctifs (hot fixes) et de correctifs de sécurité qui résolvent plusieurs problèmes du programme. Trend Micro publie régulièrement des correctifs. Les correctifs Windows comprennent un programme d'installation, alors que les correctifs non-Windows disposent en général d'un script d'installation.
- **Service Pack** : consolidation de correctifs (hot fixes), correctifs et améliorations de fonctions suffisamment significatives pour être considérées comme une mise à niveau de produit. Les service packs Windows et autres contiennent un programme et un script d'installation.

Vous pouvez obtenir les correctifs auprès du responsable technique de votre compte.

Vérifiez le site Web de Trend Micro régulièrement pour télécharger les correctifs et les service packs :

<http://www.trendmicro-europe.com/download/>

Toutes les éditions comportent un fichier Lisez-moi incluant les informations dont vous avez besoin pour installer, déployer et configurer votre produit. parcourez attentivement le fichier Lisez-moi avant d'installer un correctif (hot fix), une correction ou un service pack.

Remarque : Par défaut, les clients OfficeScan peuvent recevoir des déploiement de correctifs (hot fixes). Afin d'empêcher les clients de recevoir des déploiements de correctifs (hot fixes), modifiez les paramètres de mise à jour sur l'écran **Privilèges et paramètres clients** (consultez la rubrique suivante *Configuration des privilèges et paramètres clients* à la page 2-63).

Possibilités offertes par OfficeScan

La console Web OfficeScan vous permet d'exécuter des tâches administratives :

- Analyser la protection du réseau
- Mettre en œuvre des stratégies antivirus et anti-programmes espions
- Mettre à jour la protection
- Exécuter des scans antivirus à partir d'un seul emplacement
- Débarrasser les ordinateurs clients des programmes espions et graywares
- Mettre en quarantaine les fichiers infectés
- Surveiller les épidémies sur le réseau
- Gérer les domaines et les clients OfficeScan
- Protéger vos clients des attaques pirates grâce au pare-feu pour clients – version d'entreprise
- Protéger les PDA des virus
- Evaluer l'état antivirus du client et agir chez les clients à risque

Analyser la protection du réseau

OfficeScan génère divers types de journaux, notamment des journaux de virus, des journaux d'événements système, des journaux de mise à jour et des journaux de vérification de la connexion. Utilisez ces journaux pour contrôler le déploiement de vos mises à jour, vérifier la communication client-serveur et déterminer quels sont les ordinateurs exposés aux infections virales.

Les journaux vous permettent aussi de concevoir et de perfectionner la protection de votre réseau, d'identifier les ordinateurs les plus menacés et de modifier en conséquence les paramètres antivirus afin de mieux protéger ces ordinateurs.

Mettre en œuvre des stratégies antivirus et anti-programmes espions

OfficeScan met à votre disposition trois types de scan : le scan en temps réel, le scan programmé et le scan manuel. En configurant ces trois types de scan selon ces stratégies de protection, vous pouvez renforcer les stratégies antivirus et de lutte contre les programmes espions de votre entreprise à travers le réseau. Ainsi, vous pouvez spécifier le type des fichiers à scanner et l'action à mettre en œuvre si OfficeScan détecte un virus.

Pour vous assurer que les paramètres de scan seront appliqués uniformément à tous les clients, vous pouvez choisir de n'accorder aucun privilège aux clients. Vous pouvez également verrouiller le programme client à l'aide d'un mot de passe afin d'empêcher les utilisateurs de le désinstaller ou de le désactiver.

Mettre à jour la protection

De nouveaux virus sont créés et mis en circulation chaque jour par des médias différents, principalement sur Internet. Pour vous aider à garantir une protection permanente contre les dernières menaces virales, vous devez mettre à jour régulièrement vos composants OfficeScan. C'est pourquoi Trend Micro publie chaque semaine de nouveaux fichiers de signatures.

Exécuter des scans antivirus à partir d'un seul emplacement

La console Web donne accès à l'option d'exécution du scan immédiat (scan manuel) et à l'option de configuration de scans programmés de telle sorte qu'ils s'exécutent durant les heures creuses, lorsque le trafic du réseau est au plus bas.

Débarrasser les ordinateurs clients des programmes espions et graywares

En plus de la recherche de virus, OfficeScan analyse également les programmes espions et d'autres types de graywares, tels que les programmes publicitaires et les canulars.

Mettre en quarantaine les fichiers infectés

Vous pouvez préciser un dossier de quarantaine pour contrôler les virus et les fichiers infectés. OfficeScan envoie alors automatiquement les fichiers infectés dans le dossier de quarantaine.

Surveiller les épidémies sur le réseau

En définissant les critères d'une épidémie et en configurant les notifications d'alerte virale, vous êtes certain de pouvoir réagir plus rapidement aux épidémies qui peuvent se déclarer sur votre réseau. Dès que vous recevez une notification d'alerte, vous pouvez en effet activer la fonction de prévention manuelle afin d'empêcher la propagation des virus.

Il est également possible de bloquer les dossiers partagés et les ports vulnérables ainsi que d'interdire l'accès en écriture aux fichiers de vos clients ; ces mesures de prévention manuelle contribuent à éviter la contamination du réseau entier. Téléchargez le dernier fichier de signatures et exécutez un scan immédiat sur tous les clients afin de supprimer le moindre virus existant.

Gérer les domaines et les clients OfficeScan

Sous OfficeScan, un domaine est un groupe de clients partageant une configuration commune et exécutant des tâches similaires. Un domaine OfficeScan est différent d'un domaine Windows. Plusieurs domaines OfficeScan peuvent être intégrés dans un domaine Windows quelconque.

Vous pouvez regrouper plusieurs clients à l'intérieur d'un même domaine OfficeScan afin de leur appliquer simultanément la même configuration, ce qui facilite grandement vos opérations de gestion des clients.

Protéger vos clients des attaques pirates grâce au pare-feu pour clients – version d'entreprise

Contribue à protéger les clients OfficeScan sous Windows NT/2000/XP/Server 2003 des attaques pirates et des virus de réseau en créant une barrière entre la machine du client et le réseau. Le pare-feu pour clients – version d'entreprise vous permet de créer des stratégies et des profils destinés à bloquer ou à autoriser certains types de trafic réseau. De plus, le système de détection d'intrusions peut contribuer à identifier des signatures dans les paquets réseau indiquant une attaque des clients.

Protéger les PDA des virus

Les virus et les autres codes mal peuvent infecter vos assistants numériques personnels (PDA) pendant les opérations de projection et de synchronisation, ou via l'accès Internet. Vous devez donc protéger vos assistants Palm™, Pocket PC™ ou EPOC™ en installant OfficeScan pour Wireless.

Pour installer OfficeScan pour Wireless sur vos assistants Palm™, Pocket PC™ ou EPOC™, ouvrez la console du client et téléchargez Wireless Protection Manager.

Pour obtenir des informations détaillées sur l'installation du programme OfficeScan pour Wireless, consultez la page d'aide intitulée *Protection de votre PDA*, accessible sur votre client OfficeScan.

Pour obtenir de plus amples informations sur OfficeScan pour Wireless, consultez le *Manuel de l'administrateur*. Dans Windows Explorer, vous pouvez ouvrir le Guide de démarrage en double-cliquant sur Wireless Protection Manager Manuel.pdf dans le dossier Trend Micro\Wireless Protection Manager.

Remarque : Pour ouvrir Wireless Protection Manager Manuel.pdf, Adobe™ Reader™ doit être installé sur votre ordinateur. Vous pouvez télécharger gratuitement Acrobat Reader sur le site www.adobe.fr.

Evaluer l'état antivirus du client et agir chez les clients à risque

Trend Micro™ Policy Server pour Cisco Network Admission Control (NAC) évalue l'état de la solution antivirus du client et détermine les actions que ce dernier doit entreprendre, par exemple la mise à jour des composants ou l'activation du scan en temps réel, en fonction des stratégies que vous configurez. Le serveur de stratégie vous permet d'intégrer les clients OfficeScan dans un serveur Cisco NAC et des dispositifs d'accès réseau tels que les routeurs Cisco.

Avantages et capacités

OfficeScan apporte de nombreux avantages à votre société en vous fournissant une méthode complète mais conviviale de gestion de vos initiatives antivirus. Le paragraphe suivant est un résumé des avantages que vous offre OfficeScan.

Opération sur une console unique

Le serveur OfficeScan vous permet de gérer votre système antivirus dans son ensemble à l'aide d'une console Web unique. La console Web est installée lorsque vous installez le serveur OfficeScan, qui utilise des technologies Internet standard comme Java, CGI, HTML et http.

Damage Cleanup Services de Trend Micro

OfficeScan utilise les services Damage Cleanup (DCS) pour protéger vos ordinateurs Windows contre les chevaux de Troie et pour nettoyer vos clients des programmes espions et autres types de graywares éventuellement non désirés (consultez la rubrique *Fonctionnement des services Damage Cleanup* à la page 3-6 pour obtenir une explication sur la manière dont DCS fonctionne pour éliminer les chevaux de Troie, les programmes espions et les autres types de graywares).

Moniteur d'activité virale

Le moniteur de l'activité virale implique les clients OfficeScan dans la détection des virus. Les clients peuvent notifier le serveur OfficeScan lorsqu'ils détectent une activité douteuse sur le réseau. OfficeScan peut alors envoyer un message de notification automatique à l'administrateur, afin que celui-ci prenne les mesures adéquates.

Prévention des épidémies

La prévention des épidémies vous permet de prendre des mesures prophylactiques visant à protéger votre réseau :

- Bloquer les dossiers partagés pour empêcher les virus d'infecter les fichiers contenus dans ces dossiers
- Bloquer les ports pour empêcher les virus d'exploiter les ports vulnérables afin d'infecter les fichiers en réseau
- Interdire tout accès en écriture aux fichiers et aux dossiers afin d'empêcher les virus de modifier les fichiers
- Lorsque vous créez une stratégie de prévention des épidémies, créez un message d'alerte qui s'affichera chez les clients OfficeScan

Communication sécurisée de la console Web

OfficeScan permet des communications sécurisées entre le serveur OfficeScan et le navigateur de la console Web par le biais de la technologie Secure Socket Layer (SSL).

Le serveur OfficeScan peut générer un certificat pour chaque session de la console Web, ce qui permet au navigateur de la console Web d'encoder des données suivant les normes d'encodage des infrastructures à clés publiques (PKI). La validité par défaut de ce certificat est de trois années.

Architecture du serveur OfficeScan

OfficeScan est une application à deux niveaux composée des éléments suivants :

- le serveur, qui héberge la console Web, télécharge les composants depuis une source de mise à jour (telle que le serveur Trend Micro ActiveUpdate) et fournit des composants mis à jour aux clients.
- Le client, qui protège vos ordinateurs Windows NT/2000/XP/Server2003 et Windows 95/98/Me des virus, chevaux de Troie et autres programmes malveillants.

Remarque : Consultez le *Guide de déploiement et d'installation* ou le fichier Lisez-moi pour connaître la configuration minimale requise spécifique pour le serveur OfficeScan et le client.

Serveur OfficeScan

Le serveur OfficeScan est un référentiel central contenant toutes les configurations de vos clients, ainsi que les journaux de virus, le programme client et les mises à jour des clients.

Le serveur exécute les fonctions primordiales suivantes :

- Installation, surveillance et gestion des clients sur le réseau.
- Téléchargement des mises à jour des fichiers de signatures des virus, des moteurs de scan et des programmes depuis le serveur de mise à jour de Trend Micro, puis distribution aux clients.

Serveur en mode HTTP

Les serveurs OfficeScan en mode HTTP sont installés sur un serveur Windows NT, Windows 2000, Windows XP ou Windows Server 2003 équipé d'Internet Information Server™ (IIS) version 4.0 ou supérieure. Vous pouvez également installer le serveur Web Apache 2.0 ou supérieur sur des ordinateurs sous Windows 2000/XP/Server 2003 uniquement. Les serveurs en mode HTTP sont capables d'établir une communication bidirectionnelle en temps réel entre le serveur et les clients.

Vous pouvez assurer la gestion des clients en mode Web à partir d'une console Web à laquelle vous pouvez accéder depuis littéralement n'importe quel point du réseau.

Le serveur communique avec le client (et inversement) grâce au protocole HyperText Transfer Protocol (HTTP). Le serveur en mode HTTP peut uniquement installer des clients en mode HTTP. Il est impossible d'installer un client en mode HTTP si votre ordinateur client ne prend pas en charge le protocole TCP/IP (consultez la rubrique Figure 1-2).

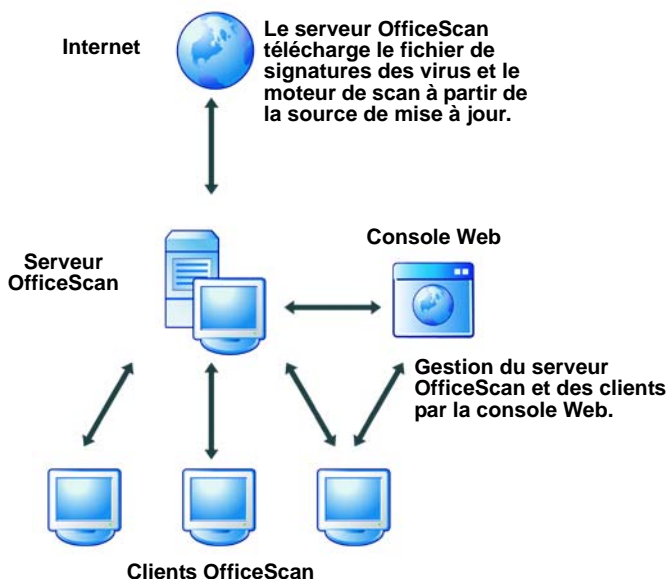


FIGURE 1-2 **Fonctionnement du serveur en mode HTTP**

Client OfficeScan

Protège vos ordinateurs Windows contre les attaques de virus en installant le logiciel client OfficeScan sur chacun de ces ordinateurs. Le client offre trois méthodes de scan – le scan en temps réel, le scan programmé et le scan manuel.

Le client effectue son rapport sur le serveur parent à partir duquel il a été installé. Il est possible que les clients fassent un rapport à un autre serveur en utilisant l'outil Client Mover (consultez la rubrique *Client Mover I* à la page 8-13 pour obtenir de plus amples informations). Le client envoie les informations relatives aux événements et à l'état au serveur en temps réel, afin de vous fournir des informations actualisées sur le client. Les événements transmis sont notamment la détection d'un virus, le démarrage d'un client, la déconnexion d'un client et la réalisation d'une mise à jour.

Configurez les paramètres de scan sur la console du client (si les utilisateurs jouissent de ce privilège) et sur le serveur console Web. Pour assurer une protection uniforme des postes de travail sur l'ensemble du réseau, vous pouvez choisir de n'accorder aucun privilège aux clients OfficeScan afin qu'ils ne puissent en aucun cas modifier les paramètres de scan ou désinstaller le programme client (consultez la rubrique *Configuration des privilèges et paramètres clients* à la page 2-63 pour obtenir de plus amples informations).











Il existe deux types de clients OfficeScan :

- Clients normaux
- Clients itinérants

Clients normaux

Les clients normaux sont les ordinateurs sur lesquels OfficeScan est installé et sont des ordinateurs stationnaires qui maintiennent une connexion réseau permanente avec le serveur.

Les icônes qui apparaissent dans la barre d'état système d'un client indiquent l'état du client normal. Consultez Tableau 1-1 pour connaître la signification de ces icônes.

Icône	Description	Scan en temps réel
	Client normal	Activé
	Fichier de signatures obsolète	Activé
	Un scan immédiat, manuel, ou programmé est en cours	Activé
	Scan en temps réel désactivé	Désactivé
	Scan en temps réel désactivé et fichier de signatures obsolète	Désactivé
	Service de scan en temps réel non démarré (icône rouge)	Désactivé
	Service de scan en temps réel non démarré et fichier de signatures obsolète (icône rouge)	Désactivé
	Connexion au serveur interrompue	Activé
	Connexion au serveur interrompue et fichier de signatures obsolète	Activé
	Connexion au serveur interrompue et scan en temps réel désactivé	Désactivé

TABEAU 1-1. Icônes qui apparaissent chez les clients normaux

Clients itinérants

Les clients itinérants sont les ordinateurs sur lesquels OfficeScan est installé et sont des ordinateurs qui ne maintiennent pas toujours une connexion réseau permanente avec le serveur (par exemple un ordinateur portable). Ces clients participent à la protection antivirus du réseau mais communiquent leur état au serveur avec un certain délai de retard.

Attribuez des privilèges itinérants aux clients déconnectés du serveur OfficeScan pendant une période prolongée.

Les clients itinérants sont mis à jour lors des occasions suivantes :

- Lorsque le client clique sur Mise à jour immédiate
- Lorsque vous configurez le déploiement automatique des mises à jour et que vous sélectionnez **Inclure les clients itinérants** dans l'écran **Déploiement automatique**

Pour obtenir des informations sur les modalités de mise à jour des clients, consultez *Mise à jour des clients* à la page 2-24.

L'état d'un client itinérant est indiqué par des icônes qui apparaissent dans la barre des tâches. Consultez Tableau 1-2 pour obtenir la liste des icônes qui apparaissent chez les clients itinérants.















icône	Description	Scan en temps réel
	Clients itinérants (icône bleue)	Activé
	Scan en temps réel désactivé	Désactivé
	Fichier de signatures obsolète	Activé
	Scan en temps réel désactivé et fichier de signatures obsolète	Désactivé
	Service de scan en temps réel non démarré (icône rouge)	Désactivé
	Service de scan en temps réel non démarré et fichier de signatures obsolète (icône rouge)	Désactivé

TABLEAU 1-2. Icônes qui apparaissent chez les clients itinérants

Clients 32 et 64 bits

OfficeScan est compatible avec les ordinateurs équipés de Windows XP/Server 2003 et dotés d'une architecture processeur 64 bits Itanium 2 (IA-64) et x86. Le tableau ci-dessous propose une comparaison des fonctionnalités d'OfficeScan pour les ordinateurs clients 32 et 64 bits :

Fonctionnalité	clients 32 bits	clients 64 bits
Scan manuel, en temps réel et programmé des virus, programmes espions et autres types de graywares		
Mode itinérance		
Services Damage Cleanup		n/a
Mailsan		n/a
Wireless Protection Manager		n/a
Support SecureClient		n/a

Console Web

La console Web est un poste de commande centralisé permettant de contrôler OfficeScan à travers le réseau d'entreprise et de configurer les paramètres du serveur et des clients.

Elle vous donne le contrôle complet sur les paramètres antivirus du poste de travail et de l'ordinateur portable. Utilisez la console Web pour effectuer les opérations suivantes :

- Déployer le programme client sur vos postes de travail et vos ordinateurs portables
- Regrouper les postes de travail et les ordinateurs portables dans des domaines logiques pour permettre leur configuration et leur gestion simultanées
- Définir des profils de scan et exécuter un scan manuel sur un ou plusieurs ordinateurs
- Recevoir des notifications et consulter les journaux d'activité virale
- Reçoit des notifications lorsque des virus sont détectés sur les postes clients et envoie des alertes virales par e-mail, pageur, déroutement SNMP ou Journal d'événement Windows
- Contrôle les épidémies par la configuration et l'activation de la prévention des épidémies

La console Web est installée lors de l'installation du serveur OfficeScan. La console Web utilise des technologies Internet standard telles que Java, CGI, HTML et HTTP.

Ouvrez la console Web à partir de n'importe quel ordinateur en réseau, à condition qu'il soit équipé du navigateur Web et des protocoles de communication requis (consultez le *Guide de déploiement et d'installation*).

Utilisation de la Documentation OfficeScan

La documentation sur OfficeScan contient :

- **Guide de déploiement et d'installation** : ce guide vous aide à planifier et à installer le programme serveur OfficeScan, à modifier les paramètres importants du client par défaut et à déployer vos clients. La dernière version du *Guide de déploiement et d'installation* est disponible sous forme électronique à l'adresse suivante :

<http://www.trendmicro-europe.com/download/>

- **Manuel de l'administrateur** : ce guide vous aide à configurer les options d'OfficeScan. La dernière version du *Manuel de l'administrateur* est disponible sous forme électronique à l'adresse suivante :

<http://www.trendmicro-europe.com/download/>

- **Aide en ligne** : l'objectif de l'aide en ligne est de fournir une description permettant d'exécuter toutes les tâches principales du produit, des conseils d'utilisation et des informations spécifiques aux champs, telles que les plages de paramètres et les valeurs optimales. L'aide en ligne est accessible à partir de la console Web OfficeScan
- **Le fichier Lisez-moi** : le fichier Lisez-moi contient des informations de dernière minute sur le produit qui ne se trouvent pas dans la documentation en ligne ou imprimée. Les rubriques contiennent une description des nouvelles fonctionnalités, des conseils d'installation, les problèmes connus et l'historique qui s'y rapporte.
- **Base de connaissances** : la base de connaissances est une base de données en ligne contenant des informations sur la résolution des problèmes et le dépannage. Elle contient les informations les plus récentes sur les problèmes relatifs au produit. Pour accéder à la base de connaissances, consultez le site Web suivant :

<http://www.trendmicro-europe.com/kb/>

Démarrage d'OfficeScan

Ce chapitre explique comment utiliser la console Web OfficeScan et comment configurer les paramètres de base.

Les rubriques présentées dans ce chapitre incluent :

- *Exploration de la console Web* à la page 2-2
- *Mise à jour d'OfficeScan* à la page 2-15
- *Vérification de la Connexion serveur-client* à la page 2-36
- *Configuration des alertes* à la page 2-38
- *Définition des options de scan* à la page 2-46
- *Configuration des privilèges et paramètres clients* à la page 2-63
- *Configuration des paramètres généraux* à la page 2-67
- *Importation et exportation des stratégies* à la page 2-71

Exploration de la console Web

Lorsque vous installez le serveur OfficeScan, vous installez également la console Web, qui utilise des technologies Internet standard comme Java, CGI, HTML et HTTP.

Pour ouvrir la console Web :

1. Sur chaque ordinateur du réseau, ouvrez un navigateur Web et tapez `http:// {OfficeScan_Server_Name} : {port number} /officescan` dans la barre d'adresses.

Si vous utilisez le protocole SSL, saisissez `https://`

`{OfficeScan_Server_Name} : {port number} /officescan` dans la barre d'adresses.

2. Le navigateur Web affiche l'écran de connexion d'OfficeScan.



FIGURE 2-1. Le navigateur Web affiche l'écran de bienvenue de la console Web.

3. Saisissez votre mot de passe dans la zone de texte **Mot de passe**, puis cliquez sur le bouton **Entrée**. Le navigateur Web affiche l'écran **Résumé** de la console Web.

Remarque : Si vous avez procédé à une mise à jour à partir d'une version antérieure d'OfficeScan, les fichiers caches du serveur proxy peuvent empêcher le chargement correct de la console Web d'OfficeScan. Videz la mémoire cache de votre navigateur et celle de tout serveur proxy situé entre le serveur OfficeScan et l'ordinateur que vous utilisez pour accéder à la console Web.

Présentation de la console Web

La console Web comprend deux éléments majeurs : la barre latérale et le cadre principal. La barre latérale regroupe, dans différentes sections, toutes les tâches que vous pouvez exécuter (exception faite de la section Boîte à outils). Ainsi, Nettoyage immédiat et Scan immédiat sont des tâches que vous pouvez exécuter à partir de la section Clients. Lorsque vous cliquez sur une tâche dans la barre latérale, le cadre principal de la console Web affiche les informations dont vous avez besoin pour exécuter cette tâche.

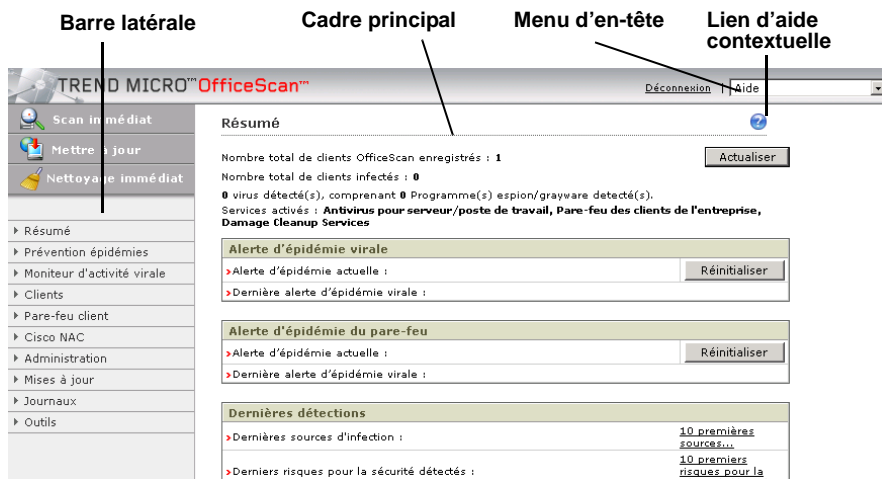


FIGURE 2-2 Le navigateur Web affiche l'écran de bienvenue de la console Web

La barre latérale regroupe les sections suivantes :

- **Scan immédiat** : cliquez ici pour effectuer un scan manuel sur les ordinateurs susceptibles d'être infectés (consultez [Exécution du scan immédiat](#) à la page 2-59)
- **Mettre à jour** : cliquez ici pour rechercher les derniers composants mis à jour sur le serveur ActiveUpdate de Trend Micro, y compris les fichiers de signatures de virus, le programme et le moteur de scan, le modèle et le moteur de scan de Damage Cleanup ainsi que les fichiers de signatures anti-programmes espions. Consultez la rubrique [Mise à jour manuelle du serveur](#) à la page 2-19)

- **Nettoyage immédiat** : cliquez ici pour exécuter les services Damage Cleanup sur les clients sélectionnés afin de rechercher les chevaux de Troie, les programmes espions et autres types de graywares. (consultez la rubrique *Exécution du nettoyage immédiat* à la page 3-8)

Le tableau suivant résume les tâches à exécuter pour chaque catégorie dans la barre latérale :

Résumé	
Résumé	Afficher un résumé de l'état de l'épidémie, des incidents viraux récents et de l'état de mise à jour et de connexion des clients.

Prévention des épidémies	
Déployer maintenant	Appliquer une stratégie de prévention des épidémies pour contrôler une épidémie qui pourrait se développer sur votre réseau.
Restaurer	Désactiver la stratégie de prévention des épidémies pour restaurer les paramètres habituels de votre réseau après la maîtrise d'une épidémie.

Moniteur d'activité virale	
Moniteur d'activité virale	Activer la surveillance de l'activité virale et permettre à OfficeScan de vous envoyer un message lorsque les clients détectent un trafic réseau anormalement élevé.

Clients	
Options de scan	Configurer les options du scan en temps réel, du scan manuel et du scan programmé.
Privilèges/Paramètres Clients	Accorder certains privilèges aux utilisateurs pour leur permettre de modifier les paramètres de scan individuels, de mettre à jour les composants et de supprimer ou de télécharger le client.
Exporter/Importer	Importer et exporter des paramètres de scan et des paramètres de privilège.

Scan immédiat	Exécuter un scan manuel sur les postes clients sélectionnés, à partir de la console Web.
Nettoyage immédiat	Recherche et nettoyage de chevaux de Troie et d'autres types de graywares sur les postes clients sélectionnés à l'aide de Services Damage Cleanup.
Désinstallation des clients	Supprimer le programme client à partir de la console Web.
Afficher l'état	Afficher les informations relatives au client, y compris ses privilèges et les versions de ses différents composants.
Notification d'installation	Envoyer un e-mail aux utilisateurs pour les informer qu'ils doivent installer le client OfficeScan.
Installation à distance	Utiliser la console Web pour installer le programme client sur les ordinateurs distants Windows NT/2000/XP/Server 2003. Vous pouvez exécuter l'installation sur plusieurs ordinateurs en même temps, sans avoir à accéder physiquement à chaque ordinateur.
Vérifier la connexion	Vérifier l'état de connexion des clients, manuellement ou automatiquement.
Paramètres clients généraux	Configurer les paramètres clients optionnels et avancés, y compris les paramètres de scan, les paramètres d'alerte, l'espace disque réservé et les paramètres de surveillance, les paramètres de mise à jour programmée et les paramètres de connexion.

Pare-feu pour clients – version d'entreprise

Liste des profils	Configurer une liste de profils de pare-feu associés à une stratégie. Appliquer les profils aux clients sélectionnés.
Liste des stratégies	Configurer une liste de stratégies de pare-feu qui définit le niveau de sécurité et les paramètres du pare-feu pour clients. Modifier également le modèle des exceptions du pare-feu.
Moniteur de l'activité virale sur le pare-feu	Envoyer des alertes vers votre poste et vers les autres administrateurs de votre entreprise chaque fois que les critères d'épidémie du pare-feu sont remplis.

Cisco NAC	
Serveurs de stratégie	Gérer une liste de serveurs de stratégie sur votre réseau.
Déploiement de l'agent	Enregistrer les paramètres d'installation et de désinstallation de l'agent CISCO NAC.
Certificat client	Importer un certificat client utilisé avec les agents Cisco NAC.
Mise à niveau de l'agent	Mise à niveau vers Cisco Trust Agent 2.0.

Administration	
Définir le mot de passe de la console	Changer le mot de passe de la console Web à intervalle régulier afin d'empêcher tout utilisateur non-autorisé de modifier vos paramètres et de supprimer des clients.
Alerte standard	Envoyer des alertes vers votre poste et vers les autres administrateurs de votre entreprise chaque fois qu'OfficeScan détecte un virus sur l'un des clients.
Alerte d'épidémie	Envoyer des alertes vers votre poste et vers les autres administrateurs de votre entreprise chaque fois que les critères d'épidémie sont remplis.
Message d'alerte du client	Modifier le message qui s'affiche sur les postes clients lorsqu'un virus est détecté.
Proxy Intranet	Activer et configurer les paramètres si un proxy intranet est présent sur votre réseau.
Serveur Web	Mettre à jour les paramètres chaque fois que les paramètres du serveur Web sont modifiés.
Clients inactifs	Supprimer automatiquement les clients inactifs pour s'assurer que l'arborescence des domaines affiche uniquement les clients actifs.
Gestionnaire de quarantaine	Définir la capacité globale du dossier de quarantaine et la taille maximale autorisée pour chaque fichier infecté déposé dans le dossier de quarantaine.
Licence du produit	Activer et vérifier l'état des licences des composants.

Programme international de pistage des virus	Choisissez si vous souhaitez participer au Programme international de pistage des virus
Sauvegarde de la base de données	Effectuez une sauvegarde de la base de données d'OfficeScan afin de réinitialiser vos paramètres OfficeScan en cas de corruption de la base de données.

Mises à jour	
Mise à jour du serveur	Mettre à jour manuellement ou automatiquement les composants du serveur et configurer les paramètres proxy pour permettre le téléchargement des mises à jour à partir du serveur de mise à jour Trend Micro.
Déploiement du client	Mettre à jour les clients manuellement ou automatiser le déploiement des mises à jour.
Rétrograder	Rétablir la version précédente du fichier de signatures ou du moteur de scan, si vous rencontrez des problèmes après le déploiement de la version la plus récente.

Journaux	
Journaux de virus	Afficher la liste des virus ayant infecté les clients sur le réseau, avec des informations détaillées sur l'infection.
Journaux de mise à jour	Afficher des informations détaillées sur la mise à jour du serveur et des clients. Utiliser les journaux pour consigner l'historique de mise à jour du serveur et pour s'assurer que les mises à jour ont été déployées avec succès sur les postes clients.
Journaux des événements du système	Afficher les événements système survenus sur le serveur, comme un arrêt suivi d'un redémarrage. Utiliser les journaux pour vérifier le bon fonctionnement du serveur et des services permettant à OfficeScan de fonctionner en réseau.
Vérifier les journaux de connexion	Afficher les journaux de vérification de la connexion afin de déterminer l'état de la connexion entre le serveur et les clients.

Journaux du pare-feu	Afficher les journaux du pare-feu client Utilisez ces journaux pour déterminer les performances des paramètres du pare-feu sur les clients OfficeScan.
Maintenance des journaux	Définir un calendrier de suppression des journaux afin de libérer de l'espace disque sur le serveur.


Outils	
Outils administrateurs	Afficher les outils qui peuvent vous aider à gérer le serveur et les clients.
Outils clients	Afficher les outils qui peuvent améliorer la performance des clients.

Autres liens disponibles sur la console

La console Web affiche également d'autres liens permettant de déconnecter la console, d'ouvrir l'aide en ligne et d'afficher les informations relatives aux virus. Ces liens sont affichés dans l'angle supérieur droit de l'écran et sous le cadre principal.

Liens d'en-tête	
Déconnexion	Cliquez sur ce lien pour fermer la session en cours. Déconnecter la console Web empêche les utilisateurs non autorisés de modifier les paramètres ou de supprimer des clients.
Aide	Sélectionnez l'une des rubriques suivantes dans le menu :
•Sommaire et Index	Cliquez sur ce lien pour ouvrir le fichier d'aide en ligne.
•Base de connaissances	Cliquez sur ce lien pour ouvrir la base de connaissances en ligne de Trend Micro ; vous y trouverez un forum aux questions et des informations mises à jour sur les produits Trend Micro ; vous pourrez également accéder au support clientèle et enregistrer votre version d'OfficeScan.
•Infos Sécurité	Cliquez sur ce lien pour afficher la page Infos Sécurité du site Trend Micro ; vous y trouverez toutes sortes d'informations sur les dernières menaces virales.

•Acheter	Cliquez sur ce lien pour afficher la page Web du service commercial de Trend Micro et pour connaître votre distributeur local.
•Support	Cliquez sur ce lien pour afficher la page Web du support technique de Trend Micro ; vous pourrez y poser vos questions et trouver des réponses aux questions les plus fréquentes concernant les produits de Trend Micro.
•À propos de	Cliquez sur ce lien pour afficher la page Produits du site Trend Micro ; vous y trouverez un aperçu général des produits et des instructions vous permettant de vérifier la version de vos composants.

Lien affiché sous le cadre principal	
	Cliquez sur ce lien pour ouvrir le fichier d'aide en ligne (n'est pas disponible sur tous les écrans).

Définition de l'arborescence du domaine d'OfficeScan

L'arborescence du domaine d'OfficeScan est une arborescence basée sur Java qui affiche les clients et les domaines d'OfficeScan sur le réseau. Elle apparaît dans le cadre principal lorsque vous cliquez sur **Prévention des épidémies**, **Clients** ou **Journaux** ou lorsque vous sélectionnez **Afficher la console client** dans l'éditeur des profils du Pare-feu pour clients – version d'entreprise.

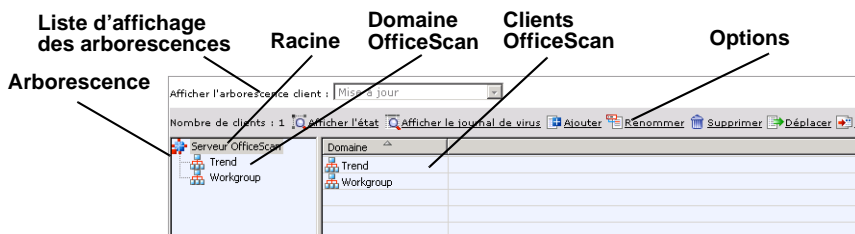







FIGURE 2-3 L'arborescence des domaines du client OfficeScan

Définition des icônes de l'arborescence du domaine

Les icônes suivantes indiquent l'état des clients dans les domaines OfficeScan.

Clients Windows 95/98/Me	Description	Serveurs et clients Windows NT/2000/XP/Server 2003
	Domaines OfficeScan : cliquez deux fois pour afficher les clients appartenant à ce domaine	
	Client/serveur normal	
	Client avec installation de l'agent de mise à jour	

Utilisation des domaines OfficeScan

Sous OfficeScan, un domaine est un groupe de clients partageant une configuration commune et exécutant des tâches similaires. En regroupant vos clients GateLock en domaines, vous pouvez configurer, gérer et appliquer simultanément la même configuration à tous les membres du domaine. Vous pouvez également regrouper vos clients en fonction des domaines NetBIOS, Windows Active Directory ou DNS existants.

Pour une gestion plus simple, regroupez les clients en fonction du service auquel ils appartiennent ou des fonctions qu'ils exécutent. Regroupez également les clients exposés à un risque d'infection plus élevé afin de leur appliquer une configuration plus sécurisée par l'intermédiaire d'un seul paramètre.

Un domaine OfficeScan est différent d'un domaine Windows NT/2000/XP/Server 2003. Plusieurs domaines OfficeScan peuvent être intégrés à un même domaine Windows NT/2000/XP/Server 2003.

Par défaut, OfficeScan crée des domaines basés sur les domaines Windows NT/2000/XP/Server 2003 existants et s'adresse à chaque client en fonction de son nom d'ordinateur. Vous pouvez supprimer ou renommer les domaines qu'OfficeScan a créés pour vous, créer un nouveau domaine ou transférer les clients d'un domaine à l'autre.

Pour ajouter un domaine OfficeScan :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Cliquez sur **Ajouter** dans le cadre principal. L'écran **Ajouter un domaine** apparaît.
3. Entrez un nom correspondant au domaine OfficeScan à ajouter, puis cliquez sur **OK**. Le nouveau domaine OfficeScan apparaît dans l'arborescence de domaines.

Pour déplacer un client OfficeScan :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence de domaines apparaît.
2. Sélectionnez le client à déplacer, puis cliquez sur **Déplacer**. L'écran **Déplacer les clients** apparaît. Vous pouvez également utiliser la fonction glisser-coller pour déplacer un client vers un autre domaine OfficeScan.
3. Effectuez l'une des actions suivantes :
 - Pour déplacer des clients vers un autre domaine OfficeScan :
 - i. Sélectionnez le domaine OfficeScan pour déplacer le client sous **Déplacer le(s) client(s) sélectionné(s) dans un autre domaine**.
 - ii. Cliquez sur **OK**. Le client apparaît sous le domaine OfficeScan sélectionné.
 - Pour déplacer des clients vers un autre serveur OfficeScan :
 - i. Saisissez le nom du serveur et le numéro de port sous **Déplacer le(s) client(s) sélectionné(s) sur un autre serveur OfficeScan**.
 - ii. Cliquez sur **OK**.

Pour supprimer un domaine OfficeScan :



1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Dans l'arborescence de domaines OfficeScan, cliquez sur le domaine OfficeScan à supprimer. Les clients qui appartiennent au domaine OfficeScan s'affichent.
3. Déplacez les clients vers d'autres domaines OfficeScan. Faites-le en sélectionnant les clients et en les faisant glisser vers les autres domaines.
4. Lorsque le domaine OfficeScan est vide, cliquez sur **Supprimer**. Un écran de confirmation apparaît.
5. Cliquez sur **OK**.

Pour renommer un domaine OfficeScan :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez le domaine OfficeScan à renommer puis cliquez sur **Renommer**. L'écran **Renommer un domaine** apparaît.
3. Entrez un nouveau nom pour le domaine OfficeScan, puis cliquez sur **OK**. Le nouveau domaine OfficeScan apparaît dans l'arborescence de domaines.

Sélection de clients et de domaines OfficeScan dans l'arborescence des domaines

Sélectionner des clients ou des domaines OfficeScan pour appliquer les paramètres simultanément.

- Pour sélectionner un seul client ou domaine OfficeScan, cliquez sur le nom du domaine ou du client.
- Pour sélectionner plusieurs domaines ou clients OfficeScan à la suite, cliquez sur le premier domaine ou client de la liste, maintenez la touche MAJ enfoncée et cliquez sur le dernier domaine ou client à sélectionner.
- Pour sélectionner un ensemble de domaines ou de clients OfficeScan qui ne se suivent pas, cliquez sur le premier domaine ou client de la liste. Maintenez la touche CTRL enfoncée et cliquez sur les domaines ou clients OfficeScan à sélectionner.
- Pour sélectionner tous les clients de votre serveur, cliquez sur l'icône racine .
- Pour actualiser l'arborescence du domaine, cliquez sur l'icône Actualiser .

Recherche de clients

Il existe deux méthodes différentes pour rechercher des clients :

Pour effectuer une recherche simple :

1. Entrez un nom de client dans la zone de texte **Recherche simple**.

Remarque : Si vous ne connaissez pas le nom complet du client, saisissez une partie du nom. OfficeScan sélectionne dans la liste le premier nom du client qui correspond à votre saisie.

2. Cliquez sur **Rechercher**. La liste des clients trouvés apparaît en surbrillance dans l'arborescence des domaines.

Pour effectuer une recherche avancée :

1. Cliquez sur **Recherche avancée**. L'écran **Recherche avancée** apparaît.
2. Vous pouvez rechercher les clients en fonction de trois types de critères :

- Basic

Plage IP : cliquez ici et définissez une plage d'adresses IP.

Segment IP : cliquez ici et saisissez une partie d'une adresse IP (en commençant par le premier octet) ; la fonction de recherche localisera tous les ordinateurs dont l'adresse IP contient les éléments saisis ; si vous tapez 10.5 (par exemple), vous trouverez tous les ordinateurs dont l'adresse IP est incluse dans un intervalle allant de 10.5.0.0 à 10.5.255.255.

Plates-formes : cliquez ici et sélectionnez les plates-formes des clients.

Architecture du processeur : cliquez ici et sélectionnez un type de processeur client : **x86** ou Itanium Architecture-64 (**IA-64**)

Domaine : cliquez sur ce critère et sélectionnez un domaine client dans la liste

Adresses MAC : définissez une plage d'adresses MAC (en notation hexadécimale).

- Version : cochez la case qui correspond au composant sur lequel effectuer la recherche, choisissez **antérieur à** ou **antérieur ou égal à** dans la liste et saisissez un numéro de version dans la zone de texte.

Version du moteur de scan

Version du fichier de signatures de virus

Version du programme client

Version du modèle Damage Cleanup

Version de la signature pour le nettoyage des programmes espions/graywares

Version du moteur Damage Cleanup

Version de la signature de scan pour les programmes espions/graywares

Version du pilote du pare-feu commun

Version du fichier de signatures de virus de réseau

Version du programme Cisco Trust Agent

- **État**

Connexion : sélectionnez un état de connexion : **En ligne**, **Hors ligne** ou **Itinérant**.

Prévention des épidémies : sélectionnez le mode **Activé** ou **Normal**

Pare-feu pour clients – version d'entreprise : sélectionnez soit **Activé**, soit **Désactivé**

Système de détection d'intrusions : sélectionnez soit **Activé**, soit **Désactivé**

Client infecté : sélectionnez et saisissez le nombre de clients infectés

Agents de mise à jour : sélectionnez soit **Activé**, soit **Désactivé**

3. Cliquez sur **OK**. Une liste de clients qui correspondent s'affiche dans l'arborescence du domaine.

Mise à jour d'OfficeScan

Pour vous aider à garantir la protection permanente de vos clients contre les dernières menaces, vous devez mettre à jour régulièrement vos composants OfficeScan. Suivez les instructions ci-dessous pour configurer OfficeScan afin d'exécuter les mises à jour :

1. Configurez le serveur OfficeScan pour les mises à jour.
2. Si vous utilisez des agents de mise à jour, spécifiez les clients agissant comme des agents et configurez les paramètres des agents (consultez la rubrique *Utilisation d'un agent de mise à jour* à la page 2-21 pour obtenir plus d'informations).
3. Configurez des clients OfficeScan pour recevoir des mises à jour depuis une source de mise à jour.

Choisir une source de mise à jour

Lorsque vous choisissez les emplacements à partir desquels vous souhaitez mettre à jour les clients, prenez en compte la bande passante des sections de votre réseau qui se trouvent entre les clients et la (les) source(s) de mise à jour (consultez le *Guide de déploiement et d'installation* pour obtenir plus d'informations sur la manière dont les mises à jour affectent le trafic du réseau). Le tableau suivant décrit les différentes options de mise à jour des composants et les recommandations d'utilisation.

Option de mise à jour	Description	Recommandation
Serveur ActiveUpdate > serveur OfficeScan > clients.	Le serveur OfficeScan reçoit les composants mis à jour à partir du serveur ActiveUpdate (ou une autre source de mise à jour) et les déploie directement vers les clients.	Utilisez cette méthode s'il n'existe aucune section de votre réseau entre le serveur OfficeScan et les clients que vous identifiez comme à 'faible bande passante'.
Serveur ActiveUpdate > serveur OfficeScan > Agents de mise à jour > clients	Le serveur OfficeScan reçoit les composants mis à jour à partir du serveur ActiveUpdate (ou une autre source de mise à jour) et les déploie directement vers les agents de mise à jour qui déploient les composants vers les clients.	Utilisez cette méthode pour équilibrer le volume du trafic sur votre réseau s'il existe des sections de votre réseau entre le serveur OfficeScan et les clients que vous identifiez comme à 'faible bande passante'.

Option de mise à jour	Description	Recommandation
Serveur ActiveUpdate > Agents de mise à jour > clients	Les agents de mise à jour reçoivent les composants mis à jour directement à partir du serveur ActiveUpdate (ou une autre source de mise à jour) et les déploient directement vers les clients.	Utilisez cette méthode uniquement si vous avez des difficultés à mettre à jour les agents de mise à jour à partir du serveur OfficeScan ou des autres agents de mise à jour. Dans la majorité des cas, les agents de mise à jour reçoivent les mises à jour plus rapidement à partir du serveur OfficeScan ou des autres agents de mise à jour qu'à partir d'une source de mise à jour externe.
Serveur ActiveUpdate > clients	Les clients OfficeScan reçoivent les composants mis à jour directement depuis le serveur ActiveUpdate (ou une autre source de mise à jour).	Utilisez cette méthode uniquement si vous avez des difficultés à mettre à jour les clients à partir du serveur OfficeScan ou des agents de mise à jour. Dans la majorité des cas, vos clients reçoivent les mises à jour plus rapidement à partir du serveur OfficeScan ou des agents de mise à jour qu'à partir d'une source de mise à jour externe.

Mise à jour du serveur

Pour garantir la protection permanente de vos clients contre les dernières menaces virales et contre les programmes espions et autres types de graywares, vous devez mettre à jour régulièrement vos composants OfficeScan. Configurer le serveur pour télécharger les mises à jour de composants OfficeScan à partir du serveur ActiveUpdate de Trend Micro. Une fois toutes les mises à jour disponibles téléchargées, le serveur les déploie sur les clients en suivant le programme de déploiement spécifié dans la section *Déploiement du client* sur l'écran du même nom.

Généralement, Trend Micro effectue la mise à jour du moteur de scan ou du programme uniquement lors de la diffusion d'une nouvelle version d'OfficeScan. Toutefois, Trend Micro publie des fichiers de signatures toutes les semaines pour maintenir à jour la protection antivirus de vos clients.

Conseil : Trend Micro recommande la mise à jour quotidienne du serveur et du client pour s'assurer que le serveur OfficeScan ait les versions actuelles des composants.

OfficeScan propose les méthodes suivantes pour la mise à jour de votre serveur :

- Mise à jour manuelle de votre serveur
- Mise à jour programmée de votre serveur

Pour obtenir plus d'informations sur la mise à jour programmée du serveur, consultez la rubrique *Configuration des mises à jour automatiques programmées* à la page 2-18.

Pour obtenir des informations sur le mode de mise à jour manuelle de votre serveur, consultez la rubrique *Mise à jour manuelle du serveur* à la page 2-19.

Si vous utilisez un serveur proxy pour vous connecter à Internet, vérifiez que vos paramètres proxy sont correctement configurés pour réussir le téléchargement des mises à jour. Pour obtenir des informations sur le mode de configuration des paramètres proxy, consultez la rubrique *Définition du proxy Internet* à la page 2-20.

Pour obtenir des informations sur le mode de mise à jour d'un client OfficeScan en tant qu'agent de mise à jour, consultez la rubrique *Spécification d'un client comme agent de mise à jour* à la page 2-22.

Configuration des mises à jour automatiques programmées

Configurez le serveur afin de vérifier régulièrement la source de mise à jour et de télécharger automatiquement les mises à jour disponibles. Comme les clients reçoivent normalement des mises à jour du serveur, l'utilisation de la mise à jour automatique programmée des clients est un moyen simple et efficace d'assurer aux clients la mise à jour permanente de leur protection.

Pour programmer la mise à jour de votre serveur :

1. Dans la barre latérale, cliquez sur **Mises à jour > Mise à jour du serveur > Mise à jour automatique**. L'écran **Mise à jour automatique** apparaît.
2. Cochez la case **Activer la mise à jour programmée du serveur OfficeScan**.
3. Dans la zone **Composants** sélectionnez les composants que vous souhaitez mettre à jour (consultez la rubrique *Définition des composants OfficeScan* à la page 1-9 pour obtenir une explication détaillée des composants OfficeScan).
4. Spécifiez un programme d'exécution de la mise à jour programmée sous **Planification des mises à jour**.
 - **Horaire** : cliquez ici pour exécuter une mise à jour programmée toutes les heures
 - **Quotidienne** : cliquez ici pour exécuter une mise à jour programmée tous les jours
 - **Hebdomadaire** : cliquez ici pour exécuter une mise à jour programmée une fois par semaine. Sélectionnez dans la liste un jour, une heure de début et une période de temps. La période donnée correspond à un nombre d'heures pendant lequel OfficeScan procédera à la mise à jour. OfficeScan exécute la mise à jour à un moment aléatoire pendant cette période qui débute à l'heure de début que vous avez précisée.
 - **Mensuelle** : cliquez ici pour exécuter une mise à jour programmée une fois par mois. Vous devez sélectionner une date dans la liste.Quelle que soit la sélection, indiquez à quel moment exécuter des mises à jour programmées dans les listes **Heure**.
5. Sous **Source de mise à jour**, sélectionnez l'emplacement à partir duquel télécharger la mise à jour. Sélectionnez le **serveur ActiveUpdate de Trend Micro** ou une Autre source de mise à jour et saisissez l'URL de la source.

6. Pour que le serveur effectue une nouvelle tentative de mise à jour échouée, cochez la case **Réessayer si la tentative de mise à jour échoue** sous **Nouvelle tentative de mise à jour du programme**.

Dans la liste **Nombre de tentatives**, sélectionnez le nombre de tentatives de mises à jour effectuées par le serveur.

Dans la liste **Intervalle**, sélectionnez l'intervalle de temps, en minutes, devant s'écouler avant que le serveur ne tente une nouvelle mise à jour.

7. Cliquez sur **Enregistrer** pour sauvegarder vos paramètres.

Mise à jour manuelle du serveur

Mettez également à jour manuellement les composants sur le serveur. Trend Micro recommande la mise à jour manuelle du serveur immédiatement après le déploiement d'OfficeScan et à chaque épidémie.

Pour effectuer une mise à jour manuelle du serveur :

1. Dans la barre latérale, cliquez sur **Mises à jour > Mise à jour du serveur > Mise à jour manuelle**. L'écran **Mise à jour manuelle** contenant les composants actuels, leur numéro de version ainsi que la date de dernière mise à jour, apparaît.
2. Sous **Source de mise à jour**, sélectionnez la source de mise à jour (serveur ActiveUpdate ou autre source) et entrez l'URL source.
3. Cliquez sur **Mettre à jour**. Le serveur vérifie la présence de composants mis à jour sur le serveur source de mise à jour. Les mises à jour disponibles figurent sur l'écran **Mise à jour disponible** et contiennent le nom des composants et leur numéro de version.
4. Cochez les composants que vous souhaitez mettre à jour.
5. Cliquez sur **Mettre à jour**. Le serveur télécharge les composants mis à jour.

Remarque : Si vous ne planifiez pas les déploiements dans la section **Déploiement du client** de l'écran **Déploiement automatique**, le serveur téléchargera les mises à jour mais ne les déploiera pas vers les clients.

Pour vérifier si vous avez planifié les téléchargements, cliquez sur **Mises à jour > Mise à jour du serveur > Mise à jour automatique** dans la barre latérale.

Définition du proxy Internet

La console Web utilise deux paramètres proxy : un pour la communication client-serveur sur le réseau local et un autre pour le serveur lorsqu'il se connecte à Internet pour télécharger les mises à jour depuis le serveur de mise à jour Trend Micro ou une autre source de mise à jour.

Si votre réseau utilise un serveur proxy pour se connecter à Internet, vous devez configurer les paramètres du proxy Internet afin que votre serveur puisse télécharger des mises à jour depuis le serveur Trend Micro ActiveUpdate ou toute autre source de mise à jour.

Pour paramétrer le proxy Internet :

1. Dans la barre latérale, cliquez sur **Mises à jour > Serveur de mise à jour > Proxy Internet**. L'écran **Proxy Internet** apparaît.
2. Cochez la case **Activer le proxy Internet**.
3. Saisissez ensuite l'adresse du serveur proxy et son numéro de port.
 - Si le serveur proxy utilise la version 4 du protocole SOCKS pour traiter les transmissions TCP, cochez la case **Utiliser SOCKS 4**.
4. Si le serveur proxy requiert un mot de passe, saisissez votre nom d'utilisateur et votre mot de passe dans les champs prévus à cet effet.
5. Cliquez sur **Enregistrer**.

Vérification de la mise à jour du serveur

Pour vérifier que le serveur OfficeScan a bien réussi sa mise à jour, vérifiez les journaux de mise à jour du serveur.

Utilisation d'un agent de mise à jour

Si vous identifiez des sections sur votre réseau entre les clients et le serveur OfficeScan comme "faible bande passante" ou "trafic dense", vous pouvez spécifier des clients OfficeScan comme sources de mise à jour pour d'autres clients. Ceci permet de distribuer la charge du déploiement des composants sur tous les clients.

Par exemple, si votre réseau est segmenté par emplacement et que le lien du réseau entre les segments subit un volume de trafic dense, Trend Micro recommande d'autoriser au moins un client sur chaque segment, faisant office d'agent de mise à jour.

Remarque : Seuls les clients Windows NT/2000/XP/Server 2003 peuvent faire office d'agents de mise à jour. Vérifiez que les postes d'agents de mise à jour disposent d'au moins 15 Mo d'espace disque disponible.

La configuration des agents de mise à jour s'effectue en trois étapes :

1. Accorder aux clients le privilège de faire office d'agents de mise à jour (consultez la rubrique *Spécification d'un client comme agent de mise à jour* à la page 2-22)
2. Sélectionner une source de mise à jour à partir de laquelle l'agent de mise à jour peut recevoir des composants mis à jour (consultez la rubrique *Sélection d'une source de mise à jour de l'agent de mise à jour* à la page 2-22)
3. Sélectionner les clients que vous souhaitez mettre à jour depuis l'agent de mise à jour et définir les agents de mises à jour comme la source de mise à jour des clients.


Remarque : Le nombre maximum d'agents de mise à jour autorisé est de **1024**.

Le nombre maximum de demandes de mises à jour simultanées qu'un agent de mise à jour peut traiter est de **250**. Ce nombre peut légèrement varier en fonction des spécifications matérielles de l'ordinateur faisant office d'agent de mise à jour.


Spécification d'un client comme agent de mise à jour

Pour que les clients fassent office d'agents de mise à jour, vous devez d'abord leur accorder le privilège de le faire.

Pour spécifier un client comme agent de mise à jour :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez les domaines ou les clients auxquels vous souhaitez accorder ce privilège, en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine .
3. Cliquez sur **Privilèges/Paramètres Clients** dans la barre latérale.
4. Sous **Mise à jour**, cochez la case **Faire office d'agent de mise à jour**.

Remarque : Si vous sélectionnez des clients multiples, vous ne pouvez pas modifier le privilège **Faire office d'agent de mise à jour**. Pour modifier simultanément ce privilège chez plusieurs clients, créer et exporter une stratégie pour les paramètres des privilèges clients (consultez la rubrique [Configuration des privilèges et paramètres clients](#) à la page 2-63). Sélectionnez ensuite plusieurs clients et importez la stratégie. Les paramètres des privilèges clients, y compris le privilège **Faire office d'agent de mise à jour**, s'appliquent à tous les clients sélectionnés.

5. Cliquez sur **Enregistrer**. Les clients qui font office d'agents de mise à jour apparaissent avec l'icône  dans l'arborescence de domaine.

Sélection d'une source de mise à jour de l'agent de mise à jour

Permet aux agents de mise à jour d'obtenir leurs mises à jour de composants à partir du serveur OfficeScan sur l'écran **Agent de mise à jour**. Si vous ne permettez pas aux agents de mise à jour d'obtenir leurs mises à jour de composants à partir du serveur OfficeScan, ils reçoivent des mises à jour à partir de la source spécifiée sur l'écran **Source de mise à jour**.

Pour sélectionner l'emplacement où les agents de mise à jour reçoivent leurs mises à jour :

1. Dans la barre latérale, cliquez sur **Mises à jour > Déploiement du client > Agent de mise à jour**. L'écran **Agent de mise à jour** apparaît.
2. Cliquez sur **Toujours effectuer la mise à jour depuis la source de mise à jour standard (serveur OfficeScan)** pour que les agents aient toujours les mises à jour sur le serveur OfficeScan.
Pour que les agents obtiennent les mises à jour à partir des sources spécifiées sur l'écran **Source de mise à jour**, désactivez la case (consultez la rubrique *Sélection d'une source de mise à jour* à la page 2-25 pour obtenir plus d'informations).
3. Cliquez sur **Enregistrer**.

Configuration d'un agent de mise à jour en tant que source de mise à jour des clients

Pour que les clients OfficeScan reçoivent leurs mises à jour d'un ou de plusieurs agents de mise à jour, ajoutez cet agent dans la liste **Sources de mises à jour personnalisées** dans l'écran **Source de mise à jour**. Vous pouvez aussi spécifier (par adresse IP) les clients qui reçoivent des mises à jour d'une source de mise à jour.

Pour configurer un agent de mise à jour en tant que source de mise à jour des clients :

1. Dans la barre latérale, cliquez sur **Mises à jour > Déploiement du client > Source de mise à jour**. L'écran **Source de mise à jour** apparaît.
2. Cliquez sur **Source de mise à jour personnalisée**.
3. Dans la liste **Source de mise à jour personnalisée**, cliquez sur **Ajouter**. L'écran **Ajout d'une plage d'adresses IP et d'une source de mise à jour** apparaît.
4. Saisissez une plage d'adresses IP de clients que vous souhaitez voir recevoir des mises à jour à partir d'un agent de mise à jour.
5. Près de **Source de mise à jour**, cliquez sur **Agent de mise à jour** et sélectionnez un agent dans la liste.

Remarque : Les clients auxquels vous avez accordé le privilège de faire office d'agents de mise à jour apparaissent dans la liste. S'il manque un agent de mise à jour, appliquez le privilège **Faire office d'agent de mise à jour** aux clients sur l'écran **Privilèges et paramètres clients** (consultez la rubrique *Spécification d'un client comme agent de mise à jour* à la page 2-22).

6. Cliquez sur **Enregistrer**.

Mise à jour des clients

Pour vous aider à garantir la protection permanente de vos clients contre les dernières menaces virales et les graywares, mettez régulièrement à jour leurs composants. Les clients peuvent se procurer les mises à jour auprès du serveur Trend Micro ActiveUpdate ; vous avez également la possibilité de définir une autre source de mise à jour.

Avant de mettre à jour les clients, vérifiez que le serveur possède les tous derniers composants. Pour obtenir des informations sur la mise à jour du serveur, consultez la rubrique *Mise à jour du serveur* à la page 2-17.

Trend Micro met à jour des composants sur une base quotidienne (et parfois toutes les heures) afin de s'assurer que la protection du client reste actuelle.

Conseil : Trend Micro recommande la mise à jour quotidienne du serveur et du client pour s'assurer que le serveur OfficeScan ait les versions actuelles des composants.

OfficeScan propose les méthodes suivantes pour la mise à jour des clients :

- Déploiement automatique (déclenché par événement et programmé)
- Déploiement manuel
- Mise à jour immédiate sur le client

Excepté pour la Mise à jour immédiate sur le client, ces méthodes peuvent mettre à jour tous les composants sur le client (consultez la rubrique *Définition des composants OfficeScan* à la page 1-9 pour obtenir des descriptions de chaque composant).

Ces méthodes s'appliquent à la mise à jour des composants suivants sur le client :

- Programme client
- Fichier de signatures des virus
- Moteur de scan
- Signature Cleanup/de scan pour les programmes espions/graywares
- Modèle et moteur Damage Cleanup
- Paramètres de configuration, y compris les privilèges, les paramètres de scan et les paramètres de prévention des épidémies
- Pilote du pare-feu commun et fichier de signatures des virus réseau
- Cisco Trust Agent

Outre ces composants, les clients OfficeScan reçoivent également des fichiers de configuration mis à jour du serveur OfficeScan. Les clients ont besoin des fichiers de configuration pour appliquer les nouveaux paramètres. Chaque fois que vous modifiez les paramètres OfficeScan via la console Web, le fichier de configuration est modifié.

Sélection d'une source de mise à jour

Il est possible de changer la source à partir de laquelle les clients reçoivent leurs mises à jour :

- Serveur OfficeScan
- Une source personnalisée de mise à jour, comme un agent de mise à jour
- Le serveur Trend Micro ActiveUpdate (consultez la rubrique *Configuration des privilèges et paramètres clients* à la page 2-63 pour obtenir des instructions)

Priorité de la source de mise à jour

Si les clients OfficeScan ne peuvent pas obtenir les mises à jour depuis la source de mise à jour sélectionnée, ils essaieront d'autres sources. La priorité en ce qui concerne la source de mise à jour est établie comme suit :

1. La première entrée de la liste des sources de mise à jour personnalisée (en cas de mise à jour à partir de sources personnalisées), puis la deuxième entrée, etc.
2. Le serveur OfficeScan (si vous décidez de procéder à la mise à jour directement à partir de la source de mise à jour standard ou si vous décidez d'effectuer la mise à jour à partir du serveur OfficeScan lorsque toutes les sources de mise à jour personnalisées sont indisponibles).
3. Le serveur ActiveUpdate de Trend Micro. Il s'agit de la dernière source de mise à jour disponible.

Sélection d'une source de mise à jour des clients :

1. Dans la barre latérale, sélectionnez **Mises à jour > Déploiement du client > Source de mise à jour**. L'écran **Source de mise à jour** apparaît.
2. Sélectionner une source de mise à jour :
 - Pour que le serveur OfficeScan devienne la source de toutes les mises à jour client, cliquez sur **Source de mise à jour standard (mise à jour depuis le serveur OfficeScan)**.
 - Pour que les clients reçoivent leurs mises à jour à partir d'une autre source, cliquez sur **Source de mise à jour personnalisée** et configurez la **Liste des sources de mise à jour personnalisées** :
 - i. Cliquez sur **Ajouter**. L'écran **Ajout d'une plage d'adresses IP et d'une source de mise à jour** apparaît.
 - ii. Définissez la plage des adresses IP qui recevront les mises à jour à partir de cette source.
 - iii. Cliquez sur une **Source de mise à jour** :
 - iv. **Agent de mise à jour** : sélectionnez l'agent de mise à jour dans la liste. Précisez les agents de mise à jour sur l'écran **Privilèges et paramètres clients**(consultez la rubrique *Configuration des privilèges et paramètres clients* à la page 2-63).
 - v. **Spécifique** : saisissez l'adresse IP ou le chemin d'accès complet d'une source de mise à jour
 - vi. Cliquez sur **Enregistrer** pour enregistrer les modifications apportées à la liste des sources de mises à jour personnalisées et pour revenir à l'écran **Source de mise à jour**.

Remarque : Vous pouvez ajouter au maximum **1024** sources de mises à jour à la liste des **Sources de mises à jour personnalisées**.

Si les clients ne peuvent pas obtenir les mises à jour à partir des sources de mises à jour sélectionnées, ils peuvent toujours essayer de procéder à la mise à jour à partir du serveur OfficeScan. Pour utiliser le serveur OfficeScan en tant que source de mise à jour de sauvegarde, cochez la case **Mise à jour à partir du serveur OfficeScan** si toutes les sources de mises à jour personnalisées sont indisponibles ou introuvables.

3. Cliquez sur **Informez tous les clients**.

Mise à jour depuis le serveur ActiveUpdate de Trend Micro


Si les ordinateurs clients sont connectés à Internet, les composants peuvent être mis à jour directement à partir du serveur ActiveUpdate de Trend Micro. Il y a deux façons d'implémenter cette option :

- utiliser le serveur ActiveUpdate en tant que source de sauvegarde pour les mises à jour si les clients ne peuvent pas se connecter à leur source de mise à jour principale
- Forcer les clients à effectuer une mise à jour à partir du serveur ActiveUpdate (comme premier choix)

Conseil : Trend Micro recommande d'utiliser le serveur ActiveUpdate en tant que source de sauvegarde.

Le fait de forcer les clients à effectuer des mises à jour à partir du serveur ActiveUpdate (comme premier choix) peut monopoliser considérablement la bande passante du réseau entre votre réseau local et Internet. Trend Micro recommande cette option seulement si vous rencontrez des problèmes de mise à jour depuis le serveur OfficeScan ou les agents de mise à jour.

Pour autoriser les clients à réaliser une mise à jour à partir du serveur ActiveUpdate en tant que sauvegarde :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Cliquez sur les domaines ou les clients en cliquant sur les icônes correspondantes dans l'arborescence du domaine. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine .
3. Cliquez sur **Privilèges/Paramètres Clients** dans la barre latérale. L'écran **Privilèges et paramètres clients** s'affiche.
4. Dans **Mettre à jour les privilèges**, cochez la case **Télécharger depuis le serveur ActiveUpdate de Trend Micro**.

5. Cliquez sur **Enregistrer**.

Remarque : Les clients sélectionnés n'effectuent leur mise à jour depuis le serveur ActiveUpdate que s'ils ne parviennent pas à l'effectuer depuis leur source de mise à jour principale. Consultez la rubrique *Priorité de la source de mise à jour* à la page 2-25 pour obtenir une explication sur l'ordre dans lequel les clients effectuent une mise à jour à partir de différentes sources.

Pour obliger les clients à effectuer une mise à jour à partir du serveur ActiveUpdate :

1. Dans la barre latérale, cliquez sur **Mises à jour>, Déploiement du client** puis sur **Source de mise à jour**. L'écran **Source de mise à jour** apparaît.
2. Cliquez sur **Source de mise à jour personnalisée**. Les clients se mettront à jour à partir de la première source de mise à jour sur la liste **Source de mise à jour personnalisée**. Si le serveur de mise à jour Trend Micro n'apparaît pas dans la liste, vous devez l'y ajouter en effectuant les opérations suivantes :

- a. Cliquez sur **Ajouter**. L'écran **Ajout d'une plage d'adresses IP et d'une source de mise à jour** apparaît.
- b. Définissez la plage des adresses IP qui recevront les mises à jour à partir de cette source.
- c. Cliquez sur **Spécifié**.
- d. Ajouter l'URL suivant :

`http://officescan-p.activeupdate.trendmicro.com/activeupdate`

- e. Cliquez sur **Enregistrer**.

Remarque : Assurez-vous que la source ActiveUpdate est la première de la **Liste des sources de mises à jour personnalisées**.

3. Cliquez sur **Informez tous les clients**.

Remarque : Le serveur ActiveUpdate doit être le premier de la liste **Sources de mises à jour personnalisées** pour être utilisé comme source de mise à jour principale. Consultez la rubrique *Priorité de la source de mise à jour* à la page 2-25 pour obtenir une explication sur l'ordre dans lequel les clients effectuent une mise à jour à partir de différentes sources.

Utilisation du déploiement automatique

Le déclenchement de la mise à jour automatique des clients et la configuration d'une mise à jour programmée sont un moyen simple et efficace d'assurer aux clients l'obtention permanente des composants les plus récents depuis le serveur.

Conseil : Trend Micro vous conseille de toujours utiliser le déploiement automatique. Cela allège le fardeau des mises à jour manuelle pour les clients et supprime tout risque de composants obsolètes sur des ordinateurs clients si ceux-ci n'ont pas effectué une mise à jour immédiate.

Lorsque le serveur OfficeScan est prêt à effectuer un déploiement automatique, il envoie des notifications de mise à jour aux clients, les informant de vérifier si le serveur dispose de composants mis à jour.

Remarque : Si le serveur OfficeScan est incapable d'envoyer avec succès une notification de mise à jour aux clients, il renvoie automatiquement la notification après un délai de 30 minutes. Le serveur continuera à envoyer de telles notifications jusqu'à huit fois maximum, jusqu'à ce que le client réponde.

Si la huitième tentative est un échec, le serveur peut supprimer le client de la file d'attente des notifications et l'avertir lorsqu'il redémarre et se connecte au serveur. Pour cela, vous devez d'abord cocher la case **Déployer vers les clients pour les clients OfficeScan uniquement et à l'exception des clients itinérants** à leur redémarrage sur l'écran **Déploiement automatique**(consultez la rubrique *Utilisation du déploiement automatique* à la page 2-29).

Le fait de programmer un déploiement permet aux clients de vérifier la présence de mises à jour sur le serveur en fonction de la programmation spécifiée. L'utilisation du déploiement automatique comporte deux étapes :

1. Accorder aux clients le privilège d'activer une mise à jour programmée
2. Configurer les paramètres de la Programmation du déploiement.

Pour mettre à jour les clients par déploiement automatique :

1. Dans la barre latérale, cliquez sur **Mises à jour > Déploiement du client > Déploiement automatique**. L'écran **Déploiement automatique** apparaît.
2. Sous **Déploiement déclenché par un événement**, sélectionnez à quel moment déployer les mises à jour et s'il faut scanner le client :
 - **Déployer vers les clients immédiatement après le téléchargement d'un nouveau composant sur le serveur OfficeScan** : le client OfficeScan initie cette mise à jour après le téléchargement des composants mis à jour (sélectionnés par défaut)
Sélectionnez également si le(s) client(s) itinérant(s) doit(vent) être inclus ou non.
 - **Déployer vers les clients pour les clients OfficeScan uniquement et à l'exception des clients itinérants à leur redémarrage** : le client OfficeScan (à l'exclusion des clients itinérants) initie cette mise à jour après son redémarrage et sa connexion au serveur OfficeScan (sélectionné par défaut)

Pour scanner le client après la mise à jour, cochez la case **Scanner l'ordinateur après la mise à jour** et cliquez sur l'une des options suivantes :

- **Exécuter un nettoyage immédiat ou un scan immédiat** : exécuter un nettoyage immédiat et un scan immédiat chez le client (sélectionné par défaut).
 - **Exécuter un nettoyage immédiat** : effectuer un nettoyage immédiat sur le client uniquement
3. Sous **Planification des déploiements**, sélectionnez à quelle fréquence effectuer le déploiement programmé. Choisissez l'une des options suivantes :
 - **Minutes** : pour un déploiement toutes les { } minutes. Sélectionnez le nombre de minutes.
 - **Heures** : pour un déploiement toutes les { } heures. Sélectionnez un nombre d'heures.
 - **Quotidien** : pour un déploiement quotidien. Sélectionnez l'heure de début et la durée du déploiement
 - **Hebdomadaire** : pour un déploiement hebdomadaire. Sélectionnez un jour.

Si vous sélectionnez **Minutes** ou **Heures**, la case **Mise à jour des configurations du client une seule fois par jour** apparaît.

Si vous ne cochez pas cette case, le client OfficeScan récupère aussi bien les

composants de protection contre les programmes espions/graywares mis à jour que les fichiers de configuration mis à jour disponibles sur le serveur à l'intervalle spécifié.

Si vous cochez cette case, OfficeScan ne met à jour que les composants à l'intervalle spécifié et les fichiers de configuration une fois par jour.

Conseil : Trend Micro réalise fréquemment des mises à jour des composants antivirus et anti-programmes espions ; cependant, vos paramètres de configuration d'OfficeScan changent probablement moins fréquemment. La mise à jour des fichiers de configuration avec les composants nécessite plus de bande passante et augmente le temps nécessaire à OfficeScan pour terminer la mise à jour. Trend Micro recommande de cocher la case **Mise à jour des configurations du client une seule fois par jour** pour limiter les mises à jour des fichiers de configuration.

4. Assurez-vous que vous avez accordé aux clients le privilège d'activer une mise à jour programmée (consultez la rubrique *Configuration des privilèges et paramètres clients* à la page 2-63).

Conseil : Trend Micro recommande de spécifier un programme de mise à jour. Si vous ne le faites pas, les clients seront uniquement mis à jour si vous effectuez un déploiement manuel depuis la console.


5. Cliquez sur **Enregistrer**.

Utilisation du déploiement manuel

Vous pouvez mettre à jour manuellement les clients en poussant les composants mis à jour sur le serveur vers les clients par la méthode de déploiement manuel.

Pour mettre à jour les clients par déploiement manuel :

1. Dans la barre latérale, cliquez sur **Mises à jour > Déploiement du client > Déploiement manuel**. L'écran **Déploiement manuel** apparaît et présente un récapitulatif des composants, des versions et de la date de leur dernière mise à jour effectuée par OfficeScan.
2. Sous **Cible de la mise à jour**, vous pouvez choisir de mettre à jour des clients spécifiques ou tous les clients dont les composants sont obsolètes :

- Pour mettre à jour tous les clients en ligne, y compris les clients itinérants possédant des connexions fonctionnelles avec le serveur, cliquez sur **Sélectionner les clients dotés de composants obsolètes** et cochez la case **Inclure le(s) client(s) itinérant(s)**.
 - Pour mettre à jour les clients spécifiques, cliquez sur **Sélectionner manuellement les clients** puis cliquez sur le bouton **Sélectionner** pour sélectionner des clients spécifiques. L'écran **Déploiement manuel** contient l'arborescence des clients. Cliquez sur les clients que vous souhaitez mettre à jour : cliquez sur l'icône de la racine  pour les sélectionner tous.
3. Après avoir sélectionné tous les clients à mettre à jour, cliquez sur **Notifier**. Le serveur demande alors à tous les clients de télécharger les mises à jour.

Utilisation de la mise à jour immédiate sur le client

Les utilisateurs peuvent mettre à jour les composants du client OfficeScan en utilisant la fonction de mise à jour immédiate sur leur ordinateur client.

Pour effectuer une mise à jour immédiate sur le client :

1. Cliquez à l'aide du bouton droit de la souris sur l'icône OfficeScan dans la barre des tâches de l'ordinateur client OfficeScan. Le menu de raccourcis OfficeScan apparaît.
2. Cliquez sur **Mettre à jour**. L'écran **Paramètres de mise à jour** apparaît.
3. Si votre réseau requiert l'utilisation d'un serveur proxy, cochez la case **Utiliser un serveur proxy** et entrez les paramètres du serveur proxy.
4. Cliquez sur **Mettre à jour**. Un écran d'état affichant la progression du téléchargement des composants apparaît.

Remarque : Si le téléchargement s'effectue directement depuis le serveur de mise à jour de Trend Micro, vous pouvez uniquement mettre à jour le fichier de signatures de virus, le moteur de scan, la signature Cleanup de scan des programmes espions/graywares, le modèle et le moteur des services Damage Cleanup.

Vérification de la mise à jour du client

Vérifiez les journaux de mise à jour du client pour contrôler qu'une mise à jour a été correctement déployée.

Pour afficher les journaux de mise à jour du client :

1. Dans la barre latérale, cliquez sur **Journaux > Journaux de mise à jour > Mise à jour du client**. L'écran **Journaux de mise à jour du client** apparaît.
2. Sélectionnez le nombre de résultats que vous voulez afficher par page dans la liste des **Résultats affichés par page**.
3. Pour trier le tableau, cliquez sur les titres des colonnes **Heure/Date** ou **Composants de la mise à jour**.
4. Pour afficher la progression d'une mise à jour particulière, cliquez sur **Afficher** dans la colonne **Progression**. L'écran **Progression de la mise à jour du client** apparaît, affichant le nombre de clients mis à jour pour chaque intervalle de 15 minutes, ainsi que le nombre total de clients mis à jour.
5. Pour afficher les détails d'une mise à jour particulière, cliquez sur **Afficher** dans la colonne **Détails**. L'écran **Détails de la mise à jour du client** apparaît.

Utilisation de la mise à jour programmée avec le mode NAT

Les problèmes suivants peuvent se poser si votre réseau utilise le mode Traduction d'adresses réseau (NAT) :

- Les clients apparaissent hors ligne sur la console Web
- Le serveur OfficeScan n'est pas en mesure d'avertir les clients des mises à jour et des modifications de la configuration.

Vous pouvez contourner ces problèmes en extrayant des composants et fichiers de configuration mis à jour du serveur pour les installer sur le client à l'aide d'une mise à jour programmée. Vous pouvez donner aux clients le privilège d'activer une mise à jour programmée, ce qui leur permet de mettre à jour automatiquement tant les fichiers de configuration que les composants antivirus conformément à une planification de Déploiement automatique que vous définissez (consultez la rubrique *[Configuration des privilèges et paramètres clients](#)* à la page 2-63 pour obtenir des informations sur l'activation d'une mise à jour programmée et la rubrique *[Utilisation du déploiement automatique](#)* à la page 2-29 pour obtenir des informations sur la configuration d'une mise à jour programmée).

Exécutez les opérations suivantes :

- Avant d'installer le client OfficeScan sur les ordinateurs clients, activez le déploiement programmé sur le serveur et donnez aux clients le privilège d'activer des mises à jour programmées.
Si vous le faites après l'installation du programme client OfficeScan, accordez aux clients le privilège d'effectuer une mise à jour immédiate et effectuez ensuite la mise à jour sur l'ordinateur client afin d'obtenir les paramètres de configuration mis à jour.

Lorsque des clients effectuent une mise à jour programmée, ils reçoivent à la fois les composants et les fichiers de configuration mis à jour.

Rétrogradation des composants

Rétrograder signifie revenir à une version précédente du fichier de signatures ou du moteur de scan. Si le fichier de signatures et/ou le moteur de scan que vous utilisez actuellement ne fonctionnent pas correctement, il est conseillé de revenir à leur ancienne version.

Remarque : Vous pouvez uniquement rétrograder le fichier de signatures de virus et le moteur de scan. Il n'est possible de revenir en arrière avec aucun autre composant.


OfficeScan utilise différents moteurs de scan pour chacun des clients suivants :

- Windows 95/98/Me
- Windows NT/2000/XP/Server 2003
- Windows XP/Server 2003 sur une architecture IA-64

Il est nécessaire de rétrograder ces types de moteurs séparément. Les procédures de rétrogradation sont identiques pour tous les types de moteurs.

Remarque : OfficeScan conserve uniquement la version actuelle et la version précédente du moteur de scan, ainsi que les cinq derniers fichiers de signatures.

Pour rétrograder le fichier de signatures ou le moteur de scan :

1. Dans la barre latérale, cliquez sur **Mises à jour > Rétrograder**. L'écran **Rétrograder** apparaît ; il affiche la version actuelle de votre fichier de signatures et de votre moteur de scan, ainsi que les versions précédentes de ces composants (si elles existent).
2. Cliquez sur **Synchroniser avec le serveur** dans la section appropriée. L'écran **Rétrograder** apparaît ; il affiche l'arborescence des domaines du client.
 Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine . Vous pouvez également rechercher des clients en appliquant des critères de sélection et changer l'affichage de l'arborescence client. Pour sélectionner plusieurs clients adjacents, cliquez sur le premier client, maintenez la touche MAJ enfoncée et cliquez sur le dernier client à sélectionner :
3. Cliquez sur **Notifier** pour rétrograder le fichier de signatures ou le moteur de scan sur les postes clients sélectionnés. Un écran de confirmation apparaît.
 Cliquez sur **Précédent** pour revenir à l'écran **Rétrograder** d'origine.
4. S'il existe sur le serveur une version plus ancienne du fichier de signatures, vous pouvez rétrograder non seulement le client, mais aussi le serveur. Pour cela, cliquez sur **Rétrograder le serveur et les clients**. L'écran **Rétrograder** apparaît.
5. Sélectionnez les clients à rétrograder.
6. Cliquez sur **Notifier** pour rétrograder le fichier de signatures sur les postes clients sélectionnés.
 Le serveur informe les clients sélectionnés qu'ils doivent rétrograder leur fichier de signatures afin d'être parfaitement synchronisés avec le serveur.

Vérification de la Connexion serveur-client

Dans OfficeScan, l'état de la connexion du client est représenté par des icônes dans l'arborescence du domaine. Cependant, dans certains cas, l'affichage de l'état correct de la connexion du client dans l'arborescence du domaine est impossible. Par exemple, si le câble réseau d'un client est accidentellement débranché, le client ne pourra pas informer le serveur qu'il se trouve hors ligne. Le client apparaîtra comme étant encore en ligne dans l'arborescence du domaine.

Vous pouvez vérifier la connexion client-serveur manuellement ou en la programmant à partir de la console Web.

Remarque : La vérification de la connexion ne permet pas de sélectionner des domaines ou clients spécifiques. Elle contrôle la connexion à tous les clients enregistrés sur le serveur OfficeScan.

Pour vérifier la connexion client-serveur :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez les domaines ou les clients auxquels vous souhaitez accorder des privilèges en cliquant sur leurs icônes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Vérifier la connexion** dans la barre latérale. L'écran **Vérifier la connexion** apparaît.
4. Vérifiez la connexion manuellement ou configurez une vérification programmée :
 - Pour vérifier manuellement la connexion client-serveur :
Cliquez sur **Vérifier maintenant** dans **Vérification manuelle**.
 - Pour vérifier automatiquement la connexion client-serveur :
- a. Cliquez sur l'onglet **Vérification programmée** et cochez la case **Activer la vérification programmée**.

- b. Sélectionnez l'une des options suivantes :

Une fois : sélectionnez cette option pour effectuer une seule vérification de la connexion

Horaire : sélectionnez cette option pour vérifier la connexion client-serveur toutes les heures

Quotidien(ne) : sélectionnez cette option pour vérifier la connexion client-serveur tous les jours

Hebdomadaire : sélectionnez cette option pour vérifier la connexion client-serveur toutes les semaines et sélectionnez un jour dans la liste

- c. Sélectionnez l'heure de début de la vérification dans **Heure de début**.

5. Cliquez sur **Enregistrer** pour enregistrer la programmation de vérification établie.
6. Vérifiez à nouveau l'arborescence client pour s'assurer que l'état du client a bien été modifié. Affichez également le journal de vérification de la connexion pour disposer du récapitulatif de la vérification de connexion effectuée. Consultez la rubrique *[Affichage des journaux de vérification de la connexion](#)* à la page 7-7 pour obtenir plus d'informations.

Configuration des alertes

Configurer divers messages d'alertes pour qu'OfficeScan vous notifie ainsi que les parties concernées lorsqu'il détecte des infections virales, des programmes espions, d'autres types de graywares et des épidémies. Vous pouvez également afficher des messages sur les ordinateurs clients pour les détections d'infections et les violations de pare-feu.

- **Message du moniteur d'alerte d'épidémie** : OfficeScan envoie ce message d'alerte lors de la détection d'un nombre excessif de sessions sur votre réseau. C'est le signal d'une possible épidémie (consultez la rubrique *Configuration du moniteur d'activité virale* à la page 5-11).
- **Message d'alerte pour la prévention des épidémies** : OfficeScan envoie ce message d'alerte lorsque vous activez manuellement la prévention des épidémies et que vous configurez la notification des clients en cas d'épidémies (consultez la rubrique *Configuration de la notification des clients en cas d'épidémies* à la page 5-9).
- **Message d'alerte standard** : OfficeScan envoie un message immédiatement après la détection du premier virus ou de la première application de graywares (consultez la rubrique *Configuration des alertes standards* à la page 2-40).
- **Message d'alerte d'épidémie** : OfficeScan envoie ce message d'alerte lors du scan et de la détection d'un nombre excessif de virus ou d'applications de graywares, qui est le signal d'une possible épidémie (consultez la rubrique *Configuration des alertes d'épidémies* à la page 2-42).
- **Message d'alerte émis par le moniteur d'activité du pare-feu** : OfficeScan envoie ce message d'alerte lorsque le pare-feu pour clients – version d'entreprise détecte un nombre excessif d'entrées journal liées au pare-feu, ce qui est le signal d'un éventuel virus réseau ou d'une intrusion sur votre réseau (consultez la rubrique *Configuration du moniteur d'activité virale du pare-feu* à la page 6-21).
- **messages d'alerte du client** : OfficeScan propose des messages d'alertes surgissant par défaut sur les ordinateurs clients lorsqu'il détecte une infection virale, une violation du pare-feu ou lorsqu'il détermine qu'un ordinateur client est à la source d'une épidémie. Vous pouvez modifier ces alertes pendant l'installation et par le biais de la console Web (consultez la rubrique *Modification des messages d'alerte du client* à la page 2-45).

Utilisation des variables de jetons avec les alertes standards et les alertes d'épidémie

Pour afficher des informations importantes au sein des alertes standards et des alertes d'épidémies envoyées par courrier électronique, vous pouvez utiliser les variables de jetons suivantes :

Variable	Description
Alertes standard	
%s	Nom de l'ordinateur infecté
%n	Nom de l'utilisateur connecté à l'ordinateur infecté
%m	Nom de domaine auquel appartient l'ordinateur infecté
%p	Chemin de l'ordinateur infecté
%v	Nom du virus
%y	Date et heure de la détection de virus
%a	Action prise contre le virus et réussite ou échec de cette action
Alertes d'épidémies	
%cv	Nombre total d'infections virales détectées
%cc	Nombre total de clients infectés
%g	Informations sur le GUID

Voici un exemple de message de notification comprenant des variables de jetons :

```
A %y, le virus suivant a été détecté par OfficeScan sur
l'ordinateur %m%s sur lequel l'utilisateur %n était connecté :
virus %v, emplacement : %p.
OfficeScan a effectué l'action suivante sur la machine
infectée : %a.
```

Configuration des alertes standards

Envoyer des alertes vers votre poste ou celui des autres administrateurs de votre entreprise dès qu'OfficeScan détecte un virus, un programme espion ou d'autres types de graywares sur l'un des clients. Les alertes standard vous informent des infections et des occurrences de graywares détectées sur votre réseau.

Les alertes en cas de détection de programmes espions et autres type de graywares sont activées par défaut.

Afin qu'OfficeScan n'envoie que des alertes d'épidémies, veuillez procéder comme suit :

1. Dans la barre latérale, cliquez sur **Administration > Alerte standard**.
2. Désactivez la case **Inclure les programmes espions/graywares**.
3. Cliquez sur **Enregistrer**.

OfficeScan propose plusieurs méthodes d'expédition des alertes, afin de garantir la réception des messages par les destinataires. Ainsi, les alertes standard peuvent être notifiées par :

- e-mail
- pageur
- déroutement SNMP
- Journal des événements Windows NT

OfficeScan inclut par défaut les informations suivantes dans tous les messages d'alerte, à l'exception des alertes sur pageur :

- Nom de l'ordinateur
- Utilisateur
- Nom de domaine
- Chemin du fichier infecté
- Nom du virus
- Date et heure de la détection
- Action de scan et résultat

Pour envoyer des alertes par courrier électronique :

1. Dans la barre latérale, cliquez sur **Administration > Alerte standard > Notification par e-mail**. L'écran **Notification par e-mail** apparaît.
2. Cochez la case **Activer la notification par e-mail** et remplissez les champs suivants :
 - **SMTP** : saisissez le nom de domaine du serveur de messagerie.
 - **Numéro de port** : saisissez le numéro de port utilisé par le serveur OfficeScan pour communiquer avec le serveur de messagerie (par défaut : port 25).
 - **À** : saisissez l'adresse du destinataire
 - **De** : saisissez le nom de l'expéditeur
 - **Objet** : saisissez l'objet de l'alerte
 - **Message** : saisissez le message d'alerte
3. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

Pour envoyer des alertes via un pageur :

1. Dans la barre latérale, cliquez sur **Administration > Alerte standard > Notification par pageur**. L'écran **Notification par pageur** apparaît.
2. Cochez la case **Activer la notification par pageur**.
3. Saisissez le numéro du pageur auquel vous souhaitez envoyer le message d'alerte, puis entrez le numéro du port COM (communication) auquel votre modem est connecté.
4. Entrez votre message dans la zone de texte **Message**. Vous devez inclure le signe dièse « # » avant le message.
5. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

Pour envoyer des alertes par déroutement SNMP :

1. Dans la barre latérale, cliquez sur **Administration > Alerte standard > Déroutement SNMP**. L'écran **Déroutement SNMP** apparaît.
2. Cochez la case **Activer la notification par déroutement SNMP**.
3. Saisissez l'adresse IP pour les notifications par déroutement SNMP, puis le nom de la communauté.
4. Entrez votre message dans la zone de texte **Message**.
5. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

Pour envoyer des alertes vers le journal des événements Windows NT :

1. Dans la barre latérale, cliquez sur **Administration > Alerte standard > Journal des événements NT**. L'écran **Journal des événements NT** apparaît.
2. Cochez la case **Activer la notification via le journal des événements NT**.
3. Entrez votre message dans la zone de texte **Message**.
4. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

Configuration des alertes d'épidémies

Une épidémie se manifeste par un accroissement soudain du nombre de virus ou de la détection de programmes espions et d'autres types de graywares sur le réseau. Vous pouvez définir vous-même les critères d'identification des épidémies ; autrement dit, préciser le nombre d'incidents viraux ou de détections de graywares sur une période donnée. Il est vital de réagir face à une épidémie. En l'absence de mesures correctives, une épidémie peut se répandre très rapidement à travers le réseau, voire au-delà.

Pour pouvoir réagir efficacement aux épidémies pouvant se développer sur votre réseau, envoyez des alertes sur votre poste et sur celui des autres administrateurs de votre entreprise dès que votre système atteint les critères d'épidémies définis (les alertes de détection de programmes espions et autres type de graywares sont activées par défaut). Pour obtenir plus d'informations sur la Prévention des épidémies, consultez la rubrique *Mise en œuvre de la prévention contre les épidémies virales* à la page 5-2.

Afin qu'OfficeScan n'envoie que des alertes d'épidémies, veuillez procéder comme suit :

1. Dans la barre latérale, cliquez sur **Administration > Alerte d'épidémie**.
2. Désactivez la case **Inclure les programmes espions/graywares**.
3. Cliquez sur **Enregistrer**.

Pour configurer les critères d'alertes de détections d'épidémies :

- Sous **Critères d'épidémies**, définissez le nombre à partir duquel les détections, sur une période donnée, devront être considérées comme une épidémie.

Remarque : OfficeScan envoie une alerte lorsque le nombre de détections de virus et de programmes graywares dépasse la valeur spécifiée. Par exemple, si vous indiquez 100, OfficeScan envoie une alerte lorsqu'il détecte la 101^e occurrence d'un virus ou d'un programme grayware.

Conseil : Trend Micro recommande donc de déclarer une épidémie lorsqu'OfficeScan détecte 100 virus en 24 heures (valeurs par défaut).

OfficeScan fournit les méthodes suivantes pour envoyer des alertes :

- e-mail
- pageur
- déroutement SNMP
- Journal des événements Windows NT

Pour envoyer des alertes par e-mail :

1. Dans la barre latérale, cliquez sur **Administration > Alerte d'épidémie > Notification par e-mail**. L'écran **Notification par e-mail** apparaît.
2. Cochez la case **Activer la notification par e-mail**.
3. Sous **Paramètres du message d'alerte**, remplissez les champs suivants :
 - **SMTP** : saisissez le nom de domaine du serveur de messagerie.
 - **Numéro de port** : saisissez le numéro de port utilisé par le serveur OfficeScan pour communiquer avec le serveur de messagerie (par défaut : port 25).
 - **À** : saisissez l'adresse du destinataire
 - **De** : saisissez le nom de l'expéditeur
 - **Objet** : saisissez l'objet de l'alerte
 - **Message** : saisissez le message d'alerte
4. Sous **Informations d'alerte à inclure**, sélectionnez les informations que vous souhaitez inclure dans le corps du message.
5. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

Pour envoyer des alertes via un pageur :

1. Dans la barre latérale, cliquez sur **Administration > Alerte d'épidémie > Notification par pageur**. L'écran **Notification par pageur** apparaît.
2. Cochez la case **Activer la notification par pageur**.
3. Saisissez le numéro du pageur auquel vous souhaitez envoyer le message d'alerte, puis entrez le numéro du port COM (communication) auquel votre modem est connecté.

4. Entrez votre message dans la zone de texte **Message**. Vous devez inclure le signe dièse « # » avant le message.
5. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

Pour envoyer des alertes par déroutement SNMP :

1. Dans la barre latérale, cliquez sur **Administration > Alerte d'épidémie > Déroutement SNMP**. L'écran **Déroutement SNMP** apparaît.
2. Cochez la case **Activer la notification par déroutement SNMP**.
3. Saisissez l'adresse IP de la station de gestion du réseau que vous utilisez pour les notifications par déroutement SNMP, puis entrez le nom de la communauté.
4. Entrez votre message dans la zone de texte **Message**.
5. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

Pour envoyer des alertes vers le journal des événements Windows NT :

1. Dans la barre latérale, cliquez sur **Administration > Alerte d'épidémie > Journal des événements NT**. L'écran **Journal des événements NT** apparaît.
2. Cochez la case **Activer la notification via le journal des événements NT**.
3. Entrez votre message dans la zone de texte **Message**.
4. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

Modification des messages d'alerte du client

OfficeScan peut afficher des messages d'alertes sur les postes clients pour informer les utilisateurs que les événements suivants se produisent sur leurs ordinateurs :

- **Infections virales** : apparaît sur les postes clients lorsqu'OfficeScan détecte un virus
- **Violations du pare-feu pour clients – version d'entreprise** : apparaît sur les postes clients lorsque vous activez les messages d'alerte de ce pare-feu (consultez la rubrique *Configuration des stratégies* à la page 6-13)
- **Détections des sources d'infection** : apparaît sur les postes clients lorsqu'OfficeScan détecte que le poste est la source de la propagation d'une infection virale

OfficeScan affiche un message par défaut pour chacun des événements et vous permet de les modifier pendant son installation (consultez le *Guide de déploiement et d'installation*). Vous pouvez également les modifier sur l'écran **Message d'alerte du client**.

Pour modifier le message d'alerte :

1. Dans la barre latérale, cliquez sur **Administration > Message d'alerte du client**. L'écran **Message d'alerte du client** apparaît.
2. Modifiez les messages par défaut.
3. Dans **Message d'alerte du client pour la source d'infection**, cochez la case **Afficher un avertissement avec une description de la source d'infection** pour afficher ce message d'avertissement sur le client.
4. OfficeScan affiche un message d'avertissement sur le client pour chaque virus provenant du client. S'il détecte plusieurs virus, il affiche plusieurs messages d'avertissement. Cependant, vous pouvez limiter le nombre de messages à afficher en paramétrant un intervalle de temps entre les messages. À côté de **Intervalle minimum**, sélectionnez le délai d'attente minimum (en minutes) avant qu'OfficeScan n'affiche un autre message d'avertissement (1 minute par défaut). Si OfficeScan détecte plusieurs virus provenant du client pendant cet intervalle, il n'affichera pas de message d'avertissement supplémentaire.
5. Cliquez sur **Enregistrer**.

Définition des options de scan

OfficeScan met à votre disposition trois types de scan différents, afin de garantir la protection de vos clients contre les menaces d'épidémies, de programmes espions et d'autres types de graywares :

- **Scan manuel** : s'effectue à la demande de l'utilisateur et scanne totalement tous les fichiers spécifiés. La durée de cette procédure dépend du nombre de fichiers à scanner et des ressources matérielles disponibles.
- **Scan en temps réel** : vous pouvez configurer OfficeScan pour qu'il scanne les fichiers en temps réel chaque fois qu'ils sont ouverts ou enregistrés. Si OfficeScan ne détecte aucun virus, l'utilisateur peut procéder à l'ouverture ou à l'enregistrement du fichier désiré. Si un virus est détecté, OfficeScan affiche un message d'alerte avec le nom du fichier infecté et le nom du virus.

La vitesse d'exécution du scan en temps réel dépend de ses paramètres de configuration. Ainsi, vous pouvez améliorer la performance des scans en temps réel en précisant uniquement les types de fichiers susceptibles de contenir un virus ou en limitant le nombre de couches de compression à scanner.

- **Scan programmé** : cette procédure permet de scanner l'ensemble des fichiers en respectant la date et la fréquence configurées. Utilisez les scans programmés pour automatiser les scans des routines de vos clients et améliorer l'efficacité de votre gestion antivirus.

Remarque : L'activation du scan pour la recherche de programmes espions et autres types de graywares peut générer un grand nombre de journaux d'alertes et d'incidents. OfficeScan peut détecter de manière régulière plusieurs applications fréquemment utilisées, comme Hotbar, et les interpréter comme des programmes espions/publicitaires. Pour empêcher OfficeScan de détecter des applications fréquemment utilisées, ajoutez les fichiers des applications à la liste d'exclusions pour tous les types de scans (consultez les rubriques *Définition des virus* à la page 1-6 et *Définition des programmes espions et autres types de graywares* à la page 1-7 pour obtenir plus d'informations sur les types de menaces qu'OfficeScan peut reconnaître et la rubrique *Fichiers et dossiers exclus des actions de scan* à la page 2-57 pour obtenir des instructions sur le mode de configuration des exclusions).

À propos de ActiveAction

À chaque type de virus correspond une action de scan différente. La personnalisation des actions en fonction des types de virus détectés exige des connaissances approfondies sur les virus informatiques et peut se révéler fastidieuse. C'est pour cette raison que Trend Micro a créé ActiveAction.

ActiveAction est un ensemble d'actions de scan pré-configurées, destinées à lutter contre les virus et contre tous les autres types de menaces comme les programmes espions et les graywares. L'action recommandée pour lutter efficacement contre les virus est le nettoyage ; la quarantaine peut être utilisée en tant qu'alternative. L'action recommandée pour lutter contre les chevaux de Troie et les canulars est la mise en quarantaine.

Si les actions de scan ne vous sont pas familières ou si vous ignorez quelle action est la mieux adaptée à tel ou tel type de virus, il est recommandé d'utiliser l'outil ActiveAction.

ActiveAction vous offre les avantages suivants :

- **Maintenance sans efforts** : ActiveAction utilise les actions de scan de Trend Micro. Vous ne perdez plus votre temps à les personnaliser vous-même.
- **Actions de scan actualisables** : les créateurs de virus modifient en permanence la manière dont leurs virus attaquent les ordinateurs.

Pour assurer une protection efficace de ses clients contre les menaces informatiques et les méthodes d'attaque les plus récentes, Trend Micro actualise les paramètres d'ActiveAction dans chaque nouveau fichier de signatures.

À propos de IntelliScan

IntelliScan est une nouvelle méthode d'identification des fichiers à scanner, plus efficace que l'option standard Scanner tous les fichiers. Pour les fichiers exécutables (comme par exemple les `.zip` et `.exe`), le véritable type du fichier est défini en fonction de son contenu. Pour les fichiers non exécutables (au format `.txt` par exemple), le véritable type du fichier est défini en fonction de son en-tête.

IntelliScan offre les avantages suivants :

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

Configuration du scan manuel

Suivez les instructions ci-dessous pour définir les paramètres de scan manuel pour le(s) client(s).

Pour configurer le scan manuel :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez les domaines ou les clients auxquels vous souhaitez accorder des privilèges en cliquant sur leurs icônes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Options de scan > Paramètres de scan manuel** dans la barre latérale. L'écran **Paramètres de scan manuel** apparaît.
4. Indiquez les fichiers à scanner sous **Cible du scan** :
 - **Tous les fichiers scannables** : cliquez ici pour scanner tous les fichiers que le client ouvre ou enregistre
 - **Utilisez IntelliScan – Identification du véritable type de fichier** : cliquez sur cette option si vous souhaitez utiliser IntelliScan, une méthode d'identification des fichiers à scanner, plus efficace que l'option standard **Scanner tous les fichiers**

- **Scanner les fichiers dotés des extensions suivantes** : cliquez ici si vous souhaitez spécifier manuellement les fichiers à scanner en fonction de leur extension.
Vous pouvez ajouter ou supprimer des extensions de la liste des extensions par défaut.
 - **Scanner les fichiers compressés** : sélectionnez cette option pour scanner les fichiers compressés et enregistrés sur le client. Dans la **liste Jusqu'à { } couche(s) de compression**, sélectionnez le nombre maximal de couches à scanner.
 - **Activer la liste d'exclusions** : sélectionnez les répertoires, les fichiers et les extensions à exclure du scan. Cliquez sur le lien **Activer la liste d'exclusions** pour passer à l'écran Liste d'exclusions, sur lequel vous pouvez configurer les paramètres d'exclusion.
 - **Scanner la mémoire (ne s'applique pas aux clients Windows NT/2000/XP/Server 2003)** : sélectionnez cette option pour scanner la mémoire vive (RAM) du client
 - **Scanner la zone d'amorçage** : sélectionnez cette option pour scanner le secteur d'amorçage du disque dur client
 - **Scanner les fichiers masqués** : sélectionnez cette option pour inclure les dossiers masqués dans tous les scans
 - **Rechercher les programmes espions/graywares** : sélectionnez cette option pour analyser les programmes espions et autres types de graywares
 - **Scanner les lecteurs mappés et les dossiers partagés du réseau** : cliquez sur cette option pour scanner tous les lecteurs mappés et les dossiers partagés du réseau
5. Spécifiez la méthode de traitement des virus détectés sous **Action de scan** :
- **Utiliser ActiveAction – actions recommandées selon le type de fichier** : cliquez ici si vous souhaitez utiliser ActiveAction, un ensemble d'actions de scan pré-configurées de Trend Micro
 - **Utiliser une action de scan personnalisée** : cliquez sur cette option pour spécifier manuellement la méthode de traitement des différents types de menaces et graywares lors de leur détection
Dans les listes **Action1** et **Action2**, sélectionnez l'action à exécuter sur les fichiers infectés. Vous avez le choix entre **Ignorer**, **Supprimer**, **Renommer**, **Mettre en quarantaine** et **Nettoyer**. L'action de scan recommandée est

Nettoyer. OfficeScan effectue l'action de scan 2 uniquement si l'action de scan 1 échoue. Vous pouvez sélectionner les actions pour les types de menace Internet suivants (l'action par défaut est indiquée ci-dessous) :

- **Canular** : mettre en quarantaine
- **Cheval de Troie** : mettre en quarantaine
- **Virus** : nettoyer
- **Virus de test** : ignorer
- **Programme espion/grayware** : ignorer
- **Autre** : nettoyer
- **Appliquer la même action pour tous les types** : cliquez sur cette option si vous souhaitez traiter tous les types de virus de façon identique

Trend Micro vous recommande de sauvegarder le fichier avant de le nettoyer. Pour sauvegarder une copie des fichiers avant le nettoyage, cochez la case **Sauvegarder les fichiers avant nettoyage**. Cette option enregistre une copie des fichiers infectés dans le répertoire suivant sur l'ordinateur client :

Client OfficeScan/Backup

- Dans la zone **Dossier de quarantaine**, saisissez un chemin d'accès URL (Uniform Resource Locator) ou UNC (Universal Naming Convention) pour le stockage des fichiers infectés. Si le dossier de quarantaine spécifié est invalide, OfficeScan utilise le dossier quarantaine par défaut du client :

Client OfficeScan/SUSPECT.

6. Sous Utilisation de la CPU, cliquez sur l'une des options suivantes :

- **Élevé** : scanner les fichiers les uns après les autres (sans interruption entre les scans)
- **Moyen** : légère interruption entre les scans de fichiers
- **Faible** : interruption plus importante entre les scans de fichiers

Remarque : L'exécution de scans nécessite d'importantes ressources CPU. Si vos ordinateurs clients font fonctionner des applications exigeantes en terme de CPU, réduisez le paramètre Utilisation de la CPU pour que les CPU clients soient moins sollicités par OfficeScan.

7. Cliquez sur **Enregistrer**.

Remarque : Si vous avez cliqué sur l'icône racine avant de définir les paramètres de scan, un autre bouton intitulé **Appliquer à tous** vous sera proposé à côté du bouton **Enregistrer**. Pour appliquer ces paramètres à tous les clients existants et futurs, cliquez sur **Appliquer à tous**.

Configuration du scan en temps réel

Suivez les instructions ci-dessous pour définir les paramètres de scan en temps réel pour le(s) client(s).

Pour configurer le scan en temps réel :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez les domaines ou les clients auxquels vous souhaitez accorder des privilèges en cliquant sur leurs icônes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Dans la barre latérale, cliquez sur **Options de scan > Scan en temps réel**. L'écran **Paramètres de scan en temps réel** apparaît.
4. Cochez la case **Activer le scan en temps réel**.
5. Sous **Cible du scan**, spécifiez les fichiers entrants ou sortants.
 - **Scanner les fichiers entrants** : sélectionnez cette option pour scanner uniquement les fichiers enregistrés par l'utilisateur
 - **Scanner les fichiers sortants** : sélectionnez cette option pour scanner uniquement les fichiers ouverts par l'utilisateur
 - **Scanner les fichiers entrants et sortants** : sélectionnez cette option pour scanner les fichiers entrants et sortants (les fichiers que l'utilisateur client enregistre et/ou ouvre)
 - **Tous les fichiers scannables** : cliquez ici pour scanner tous les fichiers que le client ouvre ou enregistre
 - **Utiliser IntelliScan – tous les types de fichiers essentiels** : cliquez ici pour utiliser IntelliScan

- **Scanner les fichiers dotés des extensions suivantes** : permet de désigner manuellement les fichiers à scanner, en fonction de leur extension

Vous pouvez ajouter ou supprimer des extensions dans la liste des extensions par défaut.

Conseil : Vous pouvez également utiliser ? et * comme caractère de substitution lors de la spécification des extensions. Par exemple, si vous souhaitez scanner tous les fichiers dont l'extension commence par D, vous pouvez saisir .D? ou .D*. OfficeScan scannera tous les fichiers dont l'extension commence par un D, y compris .DOC, .DOT et .DAT. Cette option est uniquement disponible pour le scan en temps réel.

- **Scanner les fichiers compressés** : sélectionnez cette option pour scanner les fichiers compressés enregistrés sur le client. Dans la liste **Jusqu'à { }** **couche(s) de compression**, sélectionnez le nombre maximal de couches à scanner.
- **Activer la liste d'exclusions** : sélectionnez cette option pour exclure du scan certains répertoires, fichiers et extensions. Cliquez sur le lien **Activer la liste d'exclusions** pour accéder à l'écran Liste d'exclusions et configurer les paramètres d'exclusion. Consultez la rubrique *Fichiers et dossiers exclus des actions de scan* à la page 2-57.
- **Scanner la zone d'amorçage (ne s'applique pas aux clients Windows NT/2000/XP/Server 2003)** : sélectionnez cette option pour scanner le secteur d'amorçage du disque dur client
- **Scanner la disquette pendant l'arrêt du système** : sélectionnez cette option pour exécuter un scan en temps réel à chaque arrêt du client
- **Rechercher programmes espions/graywares** : sélectionnez cette option pour analyser le logiciel qui installe les composants permettant d'enregistrer les habitudes de navigation sur le Web (inclut les logiciels publicitaires et espions, les enregistreurs de frappe et les compositeurs de numéros)
- **Scanner les lecteurs mappés et les dossiers partagés du réseau** : cliquez sur cette option pour scanner tous les lecteurs mappés et les dossiers partagés du réseau

6. Spécifiez comment traiter les menaces Internet détectées par OfficeScan, sous **Action de scan.**

- **Affichez un message d'alerte sur le client chaque fois qu'un virus est détecté** : sélectionnez cette option pour afficher un message d'alerte sur le client
- **Utiliser ActiveAction – actions recommandées selon le type de fichier** : cliquez pour utiliser l'outil ActiveAction
- **Utiliser une action de scan personnalisée** : cliquez sur cette option pour spécifier manuellement la méthode de traitement des différents types de menaces et graywares lors de leur détection

Dans les listes **Action1** et **Action2**, sélectionnez l'action à exécuter sur les fichiers infectés. Vous avez le choix entre **Ignorer**, **Supprimer**, **Renommer**, **Mettre en quarantaine** et **Nettoyer**. L'action de scan recommandée est **Nettoyer**. OfficeScan effectue l'action de scan 2 uniquement si l'action de scan 1 échoue. Vous pouvez sélectionner les actions pour les types de menace Internet suivants (l'action par défaut est indiquée ci-dessous) :

- **Canular** : mettre en quarantaine
- **Cheval de Troie** : mettre en quarantaine
- **Virus** : nettoyer
- **Virus de test** : ignorer
- **Programme espion/grayware** : ignorer
- **Autre** : nettoyer
- **Appliquer la même action pour tous les types** : cliquez sur cette option si vous souhaitez traiter tous les types de virus de façon identique

Trend Micro vous recommande de sauvegarder le fichier avant de le nettoyer. Pour sauvegarder une copie des fichiers avant le nettoyage, cochez la case **Sauvegarder les fichiers avant nettoyage**. Cette option enregistre une copie du fichier infecté dans le répertoire suivant sur l'ordinateur client :

Client OfficeScan/Backup

- Dans la zone **Dossier de quarantaine**, saisissez un chemin d'accès URL (Uniform Resource Locator) ou UNC (Universal Naming Convention) pour le stockage des fichiers infectés. Si le dossier de quarantaine spécifié est invalide, OfficeScan utilise le dossier quarantaine par défaut du client :

Client OfficeScan/SUSPECT.

7. Cliquez sur **Enregistrer**.

Remarque : Si vous avez cliqué sur l'icône racine avant de définir les paramètres de scan manuel, un autre bouton intitulé **Appliquer à tous** vous sera proposé à côté du bouton **Enregistrer**. Pour appliquer ces paramètres de scan manuel à tous les clients existants et futurs, cliquez sur **Appliquer à tous**.

Configuration du scan programmé

Suivez les instructions ci-dessous pour définir les paramètres de scan programmé pour le(s) client(s).

Pour configurer le scan programmé :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines **Client** apparaît.
2. Sélectionnez les domaines ou les clients auxquels vous souhaitez accorder des privilèges en cliquant sur leurs icônes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Dans la barre latérale, cliquez sur **Options de scan > Paramètres de scan programmé**. L'écran **Paramètres de scan programmé** apparaît.
4. Cochez la case **Activer le scan programmé**.
5. Sous **Programmation**, indiquez le moment auquel exécuter des scans programmés :
 - **Horaire** : cliquez ici pour exécuter un scan programmé tous les jours
 - **Hebdomadaire** : cliquez sur cette option pour réaliser un scan programmé une fois par semaine. Vous devez sélectionner un jour dans la liste
 - **Mensuel(le)** : cliquez sur cette option pour réaliser un scan programmé une fois par mois. Vous devez sélectionner une date dans la liste

Indépendamment de la fréquence sélectionnée **Quotidien**, **Hebdomadaire** ou **Mensuel**, vous devez indiquer un moment pour exécuter un scan programmé dans les zones **Heure de début**.

6. Spécifiez les fichiers à scanner sous **Cible de scan** en cochant les cases et en cliquant sur les options.
 - **Tous les fichiers scannables** : cliquez ici pour scanner tous les fichiers que le client ouvre ou enregistre
 - **Utiliser IntelliScan – tous les types de fichiers essentiels** : cliquez ici pour utiliser IntelliScan
 - **Scanner les fichiers dotés des extensions suivantes** : permet de désigner manuellement les fichiers à scanner, en fonction de leur extension.
Vous pouvez ajouter ou supprimer des extensions dans la liste des extensions par défaut.
 - **Scanner les fichiers compressés** : sélectionnez cette option pour scanner les fichiers compressés enregistrés sur le client. Dans la liste **Jusqu'à { }** **couche(s) de compression**, sélectionnez le nombre maximal de couches à scanner.
 - **Activer la liste d'exclusions** : sélectionnez cette option pour exclure du scan certains répertoires, fichiers et extensions. Cliquez sur le lien **Activer la liste d'exclusions** pour accéder à l'écran Liste d'exclusions et configurer les paramètres d'exclusion. Consultez la rubrique *Fichiers et dossiers exclus des actions de scan* à la page 2-57.
 - **Scanner la mémoire (ne s'applique pas aux clients Windows NT/2000/XP/Server 2003)** : sélectionnez cette option pour scanner la mémoire vive (RAM) du client
 - **Scanner la zone d'amorçage** : sélectionnez cette option pour scanner le secteur d'amorçage du disque dur du client
 - **Rechercher programmes espions/graywares** : sélectionnez cette option pour analyser le logiciel qui installe les composants permettant d'enregistrer les habitudes de navigation sur le Web (inclut les logiciels publicitaires et espions, les enregistreurs de frappe et les compositeurs de numéros)
7. Spécifiez comment traiter les menaces Internet détectées par OfficeScan, sous **Action de scan**.
 - **Affichez un message d'alerte sur le client chaque fois qu'un virus est détecté** : sélectionnez cette option pour afficher un message d'alerte sur le client

- **Utiliser une action de scan personnalisée** : cliquez sur cette option pour spécifier manuellement la méthode de traitement des différents types de menaces et graywares lors de leur détection
Dans les listes **Action1** et **Action2**, sélectionnez l'action à exécuter sur les fichiers infectés. Vous avez le choix entre **Ignorer**, **Supprimer**, **Renommer**, **Mettre en quarantaine** et **Nettoyer**. L'action de scan recommandée est **Nettoyer**. OfficeScan effectue l'action de scan 2 uniquement si l'action de scan 1 échoue. Vous pouvez sélectionner les actions pour les types de menace Internet suivants (l'action par défaut est indiquée ci-dessous) :
 - **Canular** : mettre en quarantaine
 - **Cheval de Troie** : mettre en quarantaine
 - **Virus** : nettoyer
 - **Virus de test** : ignorer
 - **Programme espion/grayware** : ignorer
 - **Autre** : nettoyer
- **Appliquer la même action pour tous les types** : cliquez sur cette option si vous souhaitez traiter tous les types de virus de façon identique
Trend Micro vous recommande de sauvegarder le fichier avant de le nettoyer. Pour sauvegarder une copie des fichiers avant le nettoyage, cochez la case **Sauvegarder les fichiers avant nettoyage**. Cette option enregistre une copie du fichier infecté dans le répertoire suivant sur l'ordinateur client :
Client OfficeScan/Backup
- Dans la zone **Dossier de quarantaine**, saisissez un chemin d'accès URL (Uniform Resource Locator) ou UNC (Universal Naming Convention) pour le stockage des fichiers infectés. Si le dossier de quarantaine spécifié est invalide, OfficeScan utilise le dossier quarantaine par défaut du client :
Client OfficeScan/SUSPECT.
- **Élevé** : scanner les fichiers les uns après les autres (sans interruption entre les scans)
- **Moyen** : légère interruption entre les scans de fichiers
- **Faible** : interruption plus importante entre les scans de fichiers

Remarque : L'exécution de scans nécessite d'importantes ressources CPU. Si vos ordinateurs clients font fonctionner des applications exigeantes en terme de CPU, réduisez le paramètre Utilisation de la CPU pour que les CPU clients soient moins sollicités par OfficeScan.

8. Cliquez sur **Enregistrer**.

Remarque : Si vous avez cliqué sur l'icône racine avant de définir les paramètres de scan manuel, un autre bouton intitulé **Appliquer à tous** vous sera proposé à côté du bouton **Enregistrer**. Pour appliquer ces paramètres de scan manuel à tous les clients existants et futurs, cliquez sur **Appliquer à tous**.

Fichiers et dossiers exclus des actions de scan

Afin d'améliorer la performance du scan et ignorer les fichiers provoquant de fausses alertes, vous pouvez exclure certains fichiers et certains dossiers des actions de scan. Les fichiers et les dossiers que vous ajoutez à la liste d'exclusion seront ignorés lors des opérations de scan manuel, en temps réel et de scan programmé.


Conseil : L'activation de la recherche de programmes espions/graywares peut générer un grand nombre de journaux d'alertes et d'incidents. OfficeScan peut détecter de manière régulière plusieurs applications fréquemment utilisées, comme Hotbar, et les interpréter comme des programmes espions/publicitaires. Pour éviter qu'OfficeScan ne détecte des applications couramment utilisées, ajoutez les fichiers d'application à la Liste d'exclusions pour tous les types de scans.

Pour définir les fichiers et les dossiers exclus des actions de scan :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez les domaines ou les clients pour lesquels vous souhaitez configurer les options de scan, en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Options de scan** dans la barre latérale. Cliquez ensuite sur le type de scan que vous souhaitez exécuter (manuel, temps réel, programmé). Son écran de paramétrage apparaît.
4. Dans cet écran, cochez la case **Activer la liste d'exclusions**. Cliquez ensuite sur le lien **Activer la liste d'exclusions**. L'écran **Liste d'exclusions** apparaît.
5. Pour exclure tous les dossiers contenant les composants et les produits Trend Micro, cochez la case **Exclure du scan les répertoires d'installation des produits Trend Micro**.

6. Pour exclure certains dossiers spécifiques, saisissez leur nom sous **Entrer le chemin d'accès du répertoire** (par ex. **c:\temp\ExcludeDir**) et cliquez sur **Ajouter**.
7. Pour exclure certains fichiers spécifiques, saisissez leur nom sous **Entrer le nom du fichier ou le nom du fichier accompagné du chemin d'accès complet** (par ex. **ExcludeDoc.hlp**; **c:\temp\excldir\ExcludeDoc.hlp**) et cliquez sur **Ajouter**.

Remarque : Tous les sous-dossiers contenus dans le chemin d'accès au répertoire spécifié sont également exclus.

8. Spécifiez les fichiers à exclure selon leur extension de nom de fichier.
Pour utiliser certaines extensions, sélectionnez celles que vous souhaitez protéger et cliquez sur .
Pour sélectionner une extension qui ne figure pas dans la liste proposée, saisissez simplement cette extension dans la zone de texte, puis cliquez sur **Ajouter**.

Remarque : Les caractères génériques tels que « * », ne sont pas autorisés pour les extensions de fichier.

9. Pour appliquer cette configuration à tous les clients qui appartiendront ultérieurement au domaine que vous avez sélectionné, cliquez sur **Enregistrer**.
 - Pour appliquer cette configuration à tous les clients (existants et futurs) qui appartiennent ou appartiendront au domaine que vous avez sélectionné, cliquez sur **Appliquer à tous**.
 - Si vous n'avez sélectionné que des clients à l'étape 1, seul le bouton **Enregistrer** vous est proposé.

Remarque : Si Microsoft Exchange Server est installé sur vos postes clients, Trend Micro vous recommande d'exclure tous les dossiers Microsoft Exchange Server.

Exécution du scan immédiat

La console Web permet d'exécuter à distance la fonction de scan immédiat sur vos clients. Trend Micro vous recommande d'exécuter un scan immédiat sur les ordinateurs susceptibles d'être infectés, en complément des scans en temps réel et des scans programmés préalablement configurés.

Remarque : Les procédures de scan immédiat et de scan manuel sont les mêmes types de scans. La seule différence réside dans le fait que le scan immédiat s'exécute à distance depuis la console Web, tandis que le scan manuel est exécuté en local par les utilisateurs.

Pour exécuter un scan immédiat :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines **Client** apparaît.
2. Sélectionnez les domaines ou les clients sur lesquels vous souhaitez exécuter un scan immédiat en cliquant sur les icônes correspondantes dans l'arborescence du domaine. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Scan immédiat** dans la barre latérale. L'écran **Scan immédiat** apparaît ; il affiche les clients ou les domaines sélectionnés.
4. Sous **Ordinateur**, sélectionnez les clients sur lesquels vous souhaitez exécuter le scan immédiat, puis cliquez sur **Démarrer la notification**. Le serveur envoie alors une requête aux clients afin qu'ils exécutent un scan immédiat à l'aide des paramètres prédéfinis.

Pour changer les paramètres de scan immédiat :

1. Cliquez sur **Paramètres de scan immédiat**. L'écran **Paramètres de scan immédiat** apparaît.
2. Indiquez les fichiers à scanner sous **Cible du scan** :
 - **Tous les fichiers scannables** : cliquez ici pour scanner tous les fichiers que le client ouvre ou enregistre
 - **Utiliser IntelliScan – tous les types de fichiers essentiels** : cliquez ici pour utiliser IntelliScan

- **Scanner les fichiers dotés des extensions suivantes** : cliquez pour désigner manuellement les fichiers à scanner, en fonction de leur extension.
Vous pouvez ajouter ou supprimer des extensions dans la liste des extensions par défaut.
 - **Activer la liste d'exclusions** : sélectionnez cette option pour exclure du scan certains répertoires, fichiers et extensions. Cliquez sur le lien **Activer la liste d'exclusions** pour accéder à l'écran Liste d'exclusions et configurer les paramètres d'exclusion. Consultez la rubrique *Fichiers et dossiers exclus des actions de scan* à la page 2-57.
 - **Scanner la mémoire (ne s'applique pas aux clients Windows NT/2000/XP/Server 2003)** : sélectionnez cette option pour scanner la mémoire vive (RAM) du client
 - **Scanner la zone d'amorçage** : sélectionnez cette option pour scanner le secteur d'amorçage du disque dur du client
 - **Rechercher programmes espions/graywares** : sélectionnez cette option pour analyser le logiciel qui installe les composants permettant d'enregistrer les habitudes de navigation sur le Web (inclut les logiciels publicitaires et espions, les enregistreurs de frappe et les composeurs de numéros)
 - **Scanner les fichiers compressés** : sélectionnez cette option pour scanner les fichiers compressés enregistrés sur le client. Dans la liste **Jusqu'à { }** **couche(s) de compression**, sélectionnez le nombre maximal de couches à scanner.
3. Spécifiez comment traiter les menaces Internet détectées par OfficeScan, sous **Action de scan**.
- **Utiliser ActiveAction – actions recommandées selon le type de fichier** : cliquez ici pour utiliser l'outil ActiveAction
4. Spécifiez comment traiter les menaces Internet détectées par OfficeScan, sous **Action de scan**.
- **Utiliser ActiveAction – actions recommandées selon le type de fichier** : cliquez pour utiliser l'outil ActiveAction
 - **Utiliser une action de scan personnalisée** : cliquez sur cette option pour spécifier manuellement la méthode de traitement des différents types de menaces et graywares lors de leur détection

Dans les listes **Action1** et **Action2**, sélectionnez l'action à exécuter sur les fichiers infectés. Vous avez le choix entre **Ignorer**, **Supprimer**, **Renommer**, **Mettre en quarantaine** et **Nettoyer**. L'action de scan recommandée est **Nettoyer**. OfficeScan effectue l'action de scan 2 uniquement si l'action de scan 1 échoue. Vous pouvez sélectionner les actions pour les types de menace Internet suivants (l'action par défaut est indiquée ci-dessous) :

- **Canular** : mettre en quarantaine
- **Cheval de Troie** : mettre en quarantaine
- **Virus** : nettoyer
- **Virus de test** : ignorer
- **Programme espion/grayware** : ignorer
- **Autre** : nettoyer
- **Appliquer la même action pour tous les types** : cliquez sur cette option si vous souhaitez traiter tous les types de virus de façon identique
Trend Micro vous recommande de sauvegarder le fichier avant de le nettoyer. Pour sauvegarder une copie des fichiers avant le nettoyage, cochez la case **Sauvegarder les fichiers avant nettoyage**. Cette option enregistre une copie du fichier infecté dans le répertoire suivant sur l'ordinateur client :
Client OfficeScan/Backup
- Dans la zone **Dossier de quarantaine**, saisissez un chemin d'accès URL (Uniform Resource Locator) ou UNC (Universal Naming Convention) pour le stockage des fichiers infectés. Si le dossier de quarantaine spécifié est invalide, OfficeScan utilise le dossier quarantaine par défaut du client :
Client OfficeScan/SUSPECT.
- **Élevé** : scanner les fichiers les uns après les autres (sans interruption entre les scans)
- **Moyen** : légère interruption entre les scans de fichiers
- **Faible** : interruption plus importante entre les scans de fichiers

Remarque : L'exécution de scans nécessite d'importantes ressources CPU. Si vos ordinateurs clients font fonctionner des applications exigeantes en terme de CPU, réduisez le paramètre Utilisation de la CPU pour que les CPU clients soient moins sollicités par OfficeScan.

5. Cliquez sur **Enregistrer**.

Remarque : Si vous avez cliqué sur l'icône racine avant de définir les paramètres de scan manuel, un autre bouton intitulé **Appliquer à tous** vous sera proposé à côté du bouton **Enregistrer**. Pour appliquer ces paramètres de scan manuel à tous les clients existants et futurs, cliquez sur **Appliquer à tous**.

Pour arrêter le scan immédiat :

1. Sélectionnez les clients sur lesquels vous souhaitez arrêter le scan immédiat.
2. Cliquez ensuite sur **Arrêter le scan**.

Pour stopper les notifications :

1. Sélectionnez les clients sur lesquels vous ne souhaitez plus exécuter le scan immédiat.
2. Cliquez ensuite sur **Arrêter la notification**. Les clients qui n'ont pas encore démarré le scan sont alors exclus de votre requête. En revanche, les clients qui ont déjà démarré le scan continuent leur procédure normalement. Pour arrêter le scan immédiat sur ces clients, cliquez sur **Arrêter le scan**.

Configuration des privilèges et paramètres clients

Tout en gardant le contrôle de votre réseau OfficeScan, vous pouvez accorder aux différents utilisateurs le privilège de modifier leurs paramètres individuels et de supprimer ou de décharger leur client. L'octroi de privilèges est une façon très simple de partager le contrôle des paramètres individuels des clients.

Toutefois, pour garantir l'uniformité de la stratégie antivirus appliquée dans l'entreprise, Trend Micro recommande d'accorder aux utilisateurs des privilèges limités. Cette limitation empêchera OfficeScan de modifier les paramètres de scan et de supprimer les clients sans votre permission.

Pour accorder des privilèges aux clients :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines **Client** apparaît.
2. Sélectionnez les domaines ou les clients auxquels vous souhaitez accorder des privilèges en cliquant sur leurs icônes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Privilèges/Paramètres Clients** dans la barre latérale. L'écran **Définir les privilèges et paramètres Clients** apparaît.
4. Sélectionnez les privilèges que vous souhaitez accorder aux utilisateurs. Configurez les zones suivantes :
 - **Antivirus** : cochez ces cases pour accorder les privilèges de scan aux utilisateurs et pour activer le mode itinérant.
 - **Pare-feu pour clients – version d'entreprise** : cochez ces cases pour permettre aux clients de consulter l'onglet de ce pare-feu, de l'activer ou de le désactiver, tout comme le système de détection d'intrusions

Remarque : Si vous autorisez les clients à activer ou à désactiver le pare-feu, le Système de détection d'intrusions et le message d'alerte, les paramètres s'affichent sous **Paramètres locaux du pare-feu** sur console client. Ces paramètres ne peuvent pas être modifiés à partir de la console Web OfficeScan. Si vous n'accordez pas aux clients ce privilège, les paramètres s'affichent sous **Liste des cartes réseau** sur la console client. Ces paramètres peuvent être modifiés à partir de la console Web du serveur d'OfficeScan. Les informations sous **Paramètres locaux du pare-feu** sur la console client reflètent toujours les paramètres configurés à partir de la console client, non de la console Web du serveur.

- **Scan du courrier** : cochez ces cases pour accorder les privilèges de scan du courrier aux utilisateurs.
- **Boîte à outils** : cochez ces cases pour accorder aux utilisateurs le privilège d'installer, de mettre à niveau/d'exécuter Wireless Protection Manager et d'installer le support Check Point SecureClient
- **Paramètres proxy** : cochez cette case pour autoriser le client à configurer les paramètres du proxy
- **Mettre à jour les privilèges** : cochez ces cases pour accorder aux utilisateurs les privilèges de mise à jour. Vous pouvez autoriser le client à **Exécuter une mise à jour immédiate !** et à **Activer la mise à jour programmée**. Cela permet aux utilisateurs clients de mettre à jour les composants à la demande depuis leur console client et d'activer ou de désactiver la mise à jour programmée.
- **Paramètres de mise à jour** : cochez les cases pour activer les paramètres de mise à jour : Télécharger depuis le serveur ActiveUpdate de Trend Micro, activer la mise à jour programmée, interdire la mise à jour du programme et le déploiement de correctifs (hot fixes) ou agir comme agent de mise à jour (pour obtenir de plus amples informations, consultez les rubriques Définition des agents de mise à jour et Description des agents de mise à jour) (consultez les rubriques *À propos des correctifs, corrections, et service packs* à la page 1-13 et *Utilisation d'un agent de mise à jour* à la page 2-21).

Remarque : **Activer la mise à jour programmée** peut s'exécuter uniquement si vous activez le déploiement programmé dans l'écran **Déploiement automatique**, accessible sous **Mises à jour > Déploiement du client** (consultez la rubrique *Utilisation du déploiement automatique* à la page 2-29 pour obtenir de plus amples informations).
Si vous sélectionnez des clients multiples, vous ne pouvez pas modifier le privilège **Faire office d'agent de mise à jour**. Pour modifier simultanément ce privilège chez plusieurs clients, créez et exportez une stratégie pour les paramètres du privilège client. Sélectionnez ensuite plusieurs clients et importez la stratégie. Les paramètres des privilèges clients, y compris le privilège Faire office d'agent de mise à jour, sont appliqués à tous les clients sélectionnés.

Lorsque les utilisateurs clients lancent une mise à jour, le poste client reçoit des mises à jour depuis la source de mise à jour indiquée sur l'écran Source de mise à jour. Si la mise à jour échoue, les postes clients essaient de procéder à la mise à jour du serveur OfficeScan. La sélection de **Télécharger des mises à jour à partir du serveur ActiveUpdate de Trend Micro** permet aux clients d'essayer d'effectuer des mises à jour à partir du serveur ActiveUpdate, si la mise à jour du serveur OfficeScan échoue.

La sélection de la case **Activer la mise à jour programmée** autorise le client à effectuer une mise à jour programmée.

- **Désinstallation** : pour autoriser les utilisateurs à supprimer leur client sans saisir aucun mot de passe, cliquez sur **Autoriser l'utilisateur client à désinstaller le client OfficeScan**. Pour admettre uniquement les utilisateurs qui connaissent le mot de passe de désinstallation, cliquez sur **Demander un mot de passe à l'utilisateur client lors de la désinstallation du client OfficeScan**, puis saisissez un mot de passe de désinstallation dans la zone de texte.
- **Déchargement** : pour autoriser les utilisateurs à télécharger (ou à désactiver) leur client sans saisir de mot de passe, cliquez sur **Autoriser l'utilisateur client à télécharger OfficeScan**. Pour admettre uniquement les utilisateurs qui connaissent le mot de passe de téléchargement, cliquez sur **Demander un mot de passe à l'utilisateur client lors du téléchargement du client OfficeScan**, puis saisissez un mot de passe de téléchargement dans la zone de texte.
- **Sécurité du client** : cliquez sur **Normal** pour autoriser les clients à accéder en lecture/écriture aux dossiers, fichiers et registres du client OfficeScan sur les ordinateurs clients. Pour limiter l'accès des clients aux dossiers, fichiers et registres du client OfficeScan, cliquez sur **Élevé**.

Remarque : Si vous sélectionnez **Élevé**, les paramètres de droits d'accès aux dossiers, fichiers et registres sont issus du fichier WINNT (pour les ordinateurs clients équipés de Windows NT) ou du dossier Programmes (pour les ordinateurs clients équipés de Windows 2000/XP/Server 2003).

Par conséquent, si les paramètres de droits d'accès (paramètres de **sécurité** sous Windows) du fichier WINNT ou du dossier Programmes sont définis pour autoriser un accès complet en lecture/écriture, la sélection de l'option **Élevé** permet encore aux clients d'accéder en lecture/écriture aux registres, fichiers et dossiers des clients OfficeScan.

5. Cliquez sur **Enregistrer**.

Remarque : Si vous avez cliqué sur l'icône racine avant d'accorder les privilèges, un autre bouton intitulé **Appliquer à tous** vous sera proposé à côté du bouton **Appliquer**. Pour accorder les mêmes privilèges à tous les clients existants et futurs, cliquez sur **Appliquer à tous**.

Configuration des paramètres généraux

OfficeScan propose plusieurs types de paramètres qui s'appliquent à tous les clients enregistrés sur le serveur. À partir de la console Web, vous pouvez configurer plusieurs types de paramètres généraux des clients.

Pour configurer les paramètres généraux :

1. Dans la barre latérale, cliquez sur **Clients > Paramètres généraux du client**.
2. Configurer les paramètres applicables à tous les clients :
 - Paramètres de scan

Configurer les paramètres de scan pour les gros fichiers

compressés : cochez cette case pour préciser les fichiers compressés qu'OfficeScan devra ignorer (sur la base de leur taille décompressée ou en fonction du nombre de fichiers contenus dans le fichier compressé).

Nettoyer les fichiers compressés : cochez cette case si vous souhaitez nettoyer les fichiers compressés.

Scanner jusqu'à { } couche(s) OLE : cochez cette case si vous souhaitez que vos clients puissent scanner les couches Object Linking and Embedding (OLE) ; indiquez ensuite le nombre de couches à scanner. OLE permet aux utilisateurs de créer des objets dans une application puis de les lier ou de les imbriquer dans une autre application.

Ajouter le scan manuel au menu des raccourcis Windows sur les clients : cochez cette case si vous souhaitez créer un lien vers OfficeScan dans le menu de raccourcis des postes clients. Ce lien vers OfficeScan permet aux utilisateurs de scanner des fichiers et des dossiers en cliquant du bouton droit de la souris sur le fichier ou le dossier souhaité sur le Bureau ou dans l'Explorateur de Windows, puis en cliquant sur **Scanner avec le client OfficeScan**.

Activer les services Damage Cleanup pour nettoyer les programmes espions/graywares (applications en cours d'exécution uniquement) : cochez cette case pour permettre aux clients d'éliminer les programmes espions, autres applications et processus de graywares avec les services Damage Cleanup (consultez la rubrique *Fonctionnement des services Damage Cleanup* à la page 3-6)

Activer Liste d'exclusion pour les programmes espions/graywares : cochez cette case pour permettre aux utilisateurs clients de configurer leur propre liste d'applications et de fichiers qu'OfficeScan peut considérer comme programmes espions ou autres types de graywares. OfficeScan scanne les fichiers de cette liste d'exclusion à la recherche de autres graywares.

Activer la liste d'exclusion critique des programmes espions/graywares : sélectionner cette case à cocher pour permettre aux utilisateurs clients de configurer leur propre liste d'application et de types de fichiers que Trend Micro considère potentiellement légitime et critique pour les opérations effectuées sur vos ordinateurs clients. Par défaut, tous ces éléments identifiés de cette manière par Trend Micro figurent dans la liste.

Exclure le dossier de la base de données du serveur OfficeScan du scan en temps réel : cochez cette case pour empêcher OfficeScan de scanner sa propre base de données lors de scans en temps réel uniquement

Remarque : OfficeScan ne scanne pas sa propre base de données par défaut. Trend Micro recommande de garder cette case cochée afin d'éviter toute corruption éventuelle de la base de données, susceptible de survenir lors du scan.

- Paramètres d'alerte

Afficher l'écran de bienvenue OfficeScan à chaque démarrage : cochez cette case si vous souhaitez afficher l'écran de bienvenue OfficeScan lorsque le client démarre son ordinateur.

Afficher l'icône d'alerte dans la barre des tâches Windows si le fichier de signatures de virus n'a pas été mis à jour après { } jours : cochez cette case si vous souhaitez que l'icône d'alerte s'affiche sur vos clients lorsque le fichier des signatures est obsolète et sélectionnez un numéro dans la liste

- Paramètres de nettoyage programmé
Cliquez sur **Activer le nettoyage programmé** pour activer le nettoyage automatique. Deux options vous sont alors proposées :
 - **Heures** : cliquez ici pour procéder à un nettoyage toutes les { } heure(s), puis choisissez un nombre dans la liste
 - **Jours** : cliquez ici pour procéder à un nettoyage tous les { } jour(s) puis choisissez un nombre dans la liste
- Paramètres Espace disque réservé et surveillance

Conseil : Trend Micro vous recommande d'activer le service de surveillance des clients pour vous assurer que le client OfficeScan protège correctement vos ordinateurs clients. Si le client OfficeScan se ferme de façon inattendue (ce qui peut arriver lorsque le client subit l'attaque d'un pirate informatique), le service de surveillance redémarre automatiquement le client OfficeScan.

Activer le service de surveillance des clients OfficeScan : cochez cette case pour que le service de surveillance puisse tenter de redémarrer votre programme client. Indiquez ensuite combien de fois le service de surveillance doit contrôler l'état du client et tenter de redémarrer le programme client.

Activer le mode anti-piratage : cochez cette case pour affecter un nom aléatoire au service de surveillance. Cette fonction empêche un virus ou tout autre type de menace d'identifier le service et de l'arrêter.

Réserver { } Mo d'espace disque pour les mises à jour : cochez cette case pour réserver une certaine quantité d'espace sur les disques durs des clients ; cet espace disque sera réservé aux correctifs (hot fixes), aux fichiers de signatures des virus, aux moteurs de scan et aux mises à jour des programmes. Par défaut, OfficeScan réserve 20 Mo d'espace disque.

- Paramètres de connexion
Connexion au serveur OfficeScan à l'aide de son nom de domaine complet (FQDN) : cochez cette case si vous souhaitez que vos clients Windows 95/98/Me utilisent le nom de domaine complet du serveur. Trend Micro vous recommande de cocher cette case si vos clients Windows 95/98/Me rencontrent des problèmes lorsqu'ils tentent de se connecter au serveur par l'intermédiaire de son nom d'hôte ou de domaine.


- Consolidation des journaux des virus de réseau
Cochez la case afin que les clients envoient leurs journaux de virus de réseau au serveur OfficeScan, lequel, en retour, les enverra à un serveur Control Manager enregistré quelconque. Utilisez ces informations dans Control Manager pour générer des rapports d'analyse de virus de réseau.
 - Paramètres de la bande passante du journal de virus
Cochez la case afin qu'OfficeScan consolide les entrées de virus lorsque de multiples infections sont détectées en cas de présence des mêmes virus ou programmes de graywares sur une courte période. OfficeScan peut détecter les mêmes virus ou programmes de graywares à plusieurs reprises, remplir alors rapidement le journal de virus et monopoliser la bande passante du réseau lorsque le client envoie les informations du journal de virus au serveur. L'activation de cette fonctionnalité permet de réduire à la fois le nombre d'entrées consignées dans le journal de virus et la bande passante du réseau que les clients utilisent lorsqu'ils soumettent au serveur des informations du journal de virus.
 - Règle de groupage
Sélectionnez le type de domaine pour regrouper les clients :
 - **NetBIOS**
 - **Active Directory**
 - **DNS**
3. Cliquez sur **Enregistrer**.

Importation et exportation des stratégies

Vous pouvez souhaiter que plusieurs clients OfficeScan aient les mêmes paramètres scan et/ou privilèges clients. OfficeScan vous permet d'enregistrer (exporter) les stratégies de scan et de privilèges client puis de les importer ultérieurement vers des clients multiples. Vous pouvez ainsi aisément configurer des paramètres identiques sur plusieurs clients.

Conseil : Si vous avez regroupé des clients avec les mêmes exigences de protection antivirus dans un domaine, Trend Micro vous recommande de configurer les paramètres d'un client, en exportant sa stratégie et en important le fichier de stratégies vers le reste des clients présents dans ce domaine (consultez la rubrique *Utilisation des domaines OfficeScan* à la page 2-10).

Pour exporter les paramètres d'un client dans un fichier de stratégies :


1. Dans la barre latérale, cliquez sur **Clients > Exporter/Importer**. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez le domaine ou le client dont vous souhaitez exporter les paramètres de scan et de privilèges en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner les paramètres du domaine racine, cliquez sur l'icône racine . Vous pouvez également rechercher des clients en appliquant des critères de sélection et changer l'affichage de l'arborescence client.

Remarque : Il est impossible d'exporter les paramètres de scan et de privilèges de clients multiples. Vous pouvez uniquement exporter les paramètres d'un client unique, d'un domaine ou de la racine.

3. Cliquez sur **Exporter les paramètres** dans la barre latérale. L'écran **Exporter les paramètres** apparaît.
4. Cliquez sur les liens pointant vers les paramètres de scan ou vers les paramètres de privilèges, afin d'afficher et de modifier les paramètres des clients ou des domaines sélectionnés.
5. Cliquez ensuite sur **Exporter** pour sauvegarder les paramètres en tant que stratégie (fichier .dat).

6. Cliquez sur **Enregistrer**, puis indiquez dans quel dossier le fichier .dat doit être déposé.
7. Cliquez une nouvelle fois sur **Enregistrer** pour sauvegarder le fichier.

Pour importer les stratégies d'un client :

1. Dans la barre latérale, cliquez sur **Clients > Exporter/Importer**. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez les domaines ou les clients dans lesquels vous souhaitez importer la stratégie en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine . Vous pouvez également rechercher des clients en appliquant des critères de sélection et changer l'affichage de l'arborescence client. Pour sélectionner plusieurs clients adjacents, cliquez sur le premier client, maintenez la touche MAJ enfoncée et cliquez sur le dernier client à sélectionner :
3. Cliquez sur **Importer la stratégie** dans la barre latérale. L'écran **Importer la stratégie** apparaît.
4. Cliquez sur **Parcourir** pour localiser le fichier de stratégies .dat sur votre ordinateur, puis cliquez sur **Importer**. L'écran **Importer la stratégie** apparaît ; il affiche un résumé des paramètres contenus dans la stratégie importée.
5. Cliquez sur les liens pointant vers les paramètres de scan ou vers les paramètres de privilège, afin d'afficher des informations détaillées sur ces paramètres. Si vous avez sélectionné un domaine entier dans l'arborescence, cochez la case **Appliquer aux sous-éléments** pour importer les stratégies vers tous les clients inclus dans ce domaine.
6. Cliquez sur **Appliquer à la cible** pour importer les fichiers de stratégies sélectionnés. Un écran de confirmation apparaît ; il vous informe que l'importation s'est déroulée avec succès.

Suppression des programmes espions, des autres types de graywares, et des menaces des chevaux de Troie

Ce chapitre vous explique comment configurer OfficeScan pour vous aider à éliminer les programmes espions, les autres types de graywares et les menaces des chevaux de Troie des ordinateurs clients de votre réseau.

Les rubriques présentées dans ce chapitre incluent :

- *Définition des programmes espions et autres types de graywares* à la page 3-2
- *Fonctionnement des services Damage Cleanup* à la page 3-6
- *Exécution du nettoyage immédiat* à la page 3-8
- *Configuration des paramètres anti-programmes espions* à la page 3-9
- *Protection contre les programmes espions* à la page 3-12

Définition des programmes espions et autres types de graywares

Vos ordinateurs courent d'autres menaces potentielles que les virus. Les graywares sont des applications ou des fichiers non répertoriés comme virus ou chevaux de Troie mais pouvant toutefois avoir un effet négatif sur les performances des ordinateurs de votre réseau. Ils font courir un risque significatif à la sécurité, à la confidentialité et à la légalité de votre entreprise. Les graywares réalisent souvent des actions variées non souhaitées et menaçantes qui irritent les utilisateurs avec des fenêtres pop-up, enregistrent les séquences de frappe des touches du clavier et exposent les failles de l'ordinateur à des attaques.

Types de graywares

OfficeScan est à même de détecter plusieurs types de graywares, y compris les suivants :

- **Programmes espions** : récoltent des données, telles que des noms d'utilisateur de compte, de mots de passe, des numéros de cartes de crédit et d'autres informations confidentielles pour les transmettre à des tiers
- **Programmes publicitaires** : affichent des publicités et récoltent des données utilisateurs, telles que des préférences de navigation, pouvant être utilisées à des fins publicitaires
- **Composeurs de numéros** : modifient les paramètres Internet et obligent un ordinateur à composer des numéros de téléphone préconfigurés à l'aide d'un modem. Ce sont souvent des numéros de services téléphoniques facturés à l'utilisation (pay-per-call) ou internationaux qui peuvent entraîner une dépense significative pour votre société.
- **Canulars** : entraîne un fonctionnement anormal d'un ordinateur, en faisant par exemple vibrer l'écran ou en modifiant l'apparence du curseur
- **Outils de piratage** : aident les pirates informatiques malveillants à s'infiltrer sur un ordinateur
- **Outils d'accès à distance** : aident les pirates informatiques malveillants à accéder à distance à un ordinateur et à le contrôler
- **Applications de piratage des mots de passe** : aident à déchiffrer des noms d'utilisateurs et des mots de passe
- **Autres** : autres types de programmes potentiellement malveillants

Le mode d'infiltration des programmes espions et autres graywares sur votre réseau

Les programmes espions et autres graywares pénètrent sur un réseau d'entreprise lorsque les utilisateurs téléchargent des programmes légitimes dont le module d'installation contient des applications de graywares. Les applications de graywares utilisent souvent des contrôles ActiveX (consultez la rubrique [À propos d'ActiveX](#) à la page 3-5).

La plupart des programmes proposent un contrat de licence d'utilisation que l'utilisateur est tenu d'accepter avant de lancer la procédure de téléchargement. Ce contrat de licence inclut des informations relatives à l'application supplémentaire de graywares et à sa fonction de collecte de données personnelles; toutefois, les utilisateurs font souvent fi de ces informations ou ne comprennent pas la terminologie juridique décrivant l'application.

Risques et menaces potentiels

Les programmes espions et les autres types de graywares sur votre réseau sont susceptibles de donner lieu à ce qui suit :

- **réduction des performances de l'ordinateur** : afin d'exécuter leurs tâches, les applications de graywares consomment souvent une grande partie des ressources du processeur et de la mémoire du système.
- **Augmentation du nombre des plantages liés au navigateur Web** : certains types de graywares tels que les programmes publicitaires, sont souvent conçus pour ouvrir des fenêtres contextuelles ou afficher des informations dans votre navigateur ou dans sa barre. Selon le mode d'interaction du code de ces applications avec les processus du système, les graywares peuvent parfois provoquer un plantage des navigateurs ou les bloquer; un redémarrage du système s'impose parfois.
- **Diminution de la rentabilité de l'utilisateur** : les graywares détournent inutilement les utilisateurs de leurs tâches et responsabilités principales en les obligeant à fermer fréquemment des publicités pop-up et à gérer les effets négatifs des canulars.
- **Dégradation de la bande passante du réseau** : Les graywares transmettent également souvent les données qu'ils collectent à d'autres applications présentes sur votre réseau ou à l'extérieur de celui-ci, utilisant ainsi la bande passante de votre réseau.

- **Perte d'informations personnelles et professionnelles** : les données que les programmes de graywares récoltent ne sont pas toutes aussi simples qu'une liste de sites Web visités par les utilisateurs. Les graywares peuvent également récupérer les noms d'utilisateur et les mots de passe permettant d'accéder aux comptes personnels, tels qu'un compte en banque et des comptes d'entreprise de votre réseau.
- **Risque accru de responsabilité juridique** : en cas de piratage des ressources informatiques de votre réseau, les pirates peuvent utiliser vos ordinateurs pour lancer des attaques ou installer des graywares sur des ordinateurs situés en dehors de votre réseau. L'utilisation des ressources de votre réseau pour des activités de ce genre peut rendre votre organisation responsable juridiquement des dommages occasionnés aux tierces parties.

La solution Trend Micro

Cette version de Trend Micro OfficeScan est en mesure de rechercher, détecter et supprimer une multitude de fichiers et d'applications liés aux programmes espions et autres graywares.

Pour obtenir des instructions sur la configuration des paramètres d'OfficeScan liés aux programmes espions/graywares, consultez *Configuration des paramètres anti-programmes espions* à la page 3-9.

Grayware inconnu

Vous pouvez envoyer vos virus, fichiers infectés, chevaux de Troie, vers suspects, logiciels espions et autres fichiers suspects à Trend Micro pour les évaluer. Pour cela, contactez l'assistance de votre fournisseur ou visitez l'URL de l'Assistant d'envoi de Trend Micro :

<http://www.trendmicro-europe.com/avservice/>

Consultez la rubrique *Contacter Trend Micro* à la page 9-20 pour obtenir plus d'informations.

À propos d'ActiveX

ActiveX est une technologie de Microsoft qui permet de gérer les interactions entre les navigateurs Web, les applications Microsoft ou d'autres applications tierces et le système d'exploitation de l'ordinateur. ActiveX utilise des contrôles ActiveX – des composants logiciels installés sur les ordinateurs qui ajoutent des fonctionnalités spécialisées aux pages Web, comme des programmes d'animation et des programmes interactifs.

Les créateurs de programmes espions et autres graywares masquent souvent leurs applications sous des aspects de contrôles ActiveX normaux. Lorsque vos utilisateurs affichent des sites Web requérant la fonctionnalité ActiveX, ils peuvent sciemment ou inconsciemment télécharger des contrôles ActiveX sur leurs ordinateurs et sans le savoir installer des applications de graywares.

Il existe deux possibilités de se prémunir des programmes espions et autres graywares masqués sous l'aspect de contrôles ActiveX :

- en configurant le navigateur Web client de façon qu'il demande une confirmation avant d'installer des applications ActiveX
- en apprenant à vos utilisateurs à se méfier des applications pouvant être des graywares lors du téléchargement de fichiers, contrôles ActiveX ou applications sur leur ordinateur

Fonctionnement des services Damage Cleanup

OfficeScan utilise des services Damage Cleanup (DCS) pour protéger vos ordinateurs Windows contre les chevaux de Troie et pour nettoyer vos clients des programmes espions et autres types de graywares éventuellement non désirés.

Chevaux de Troie

Un cheval de Troie est un programme malveillant dissimulé sous les apparences d'une application inoffensive. À la différence des virus, les chevaux de Troie ne se reproduisent pas mais n'en restent pas moins destructeurs. Comme leur nom l'indique, les chevaux de Troie sont des applications qui introduisent de nouveaux virus sur votre ordinateur, alors qu'ils prétendent éradiquer les virus détectés. Les solutions antivirus conventionnelles peuvent détecter et supprimer les virus mais pas les chevaux de Troie, notamment ceux qui ont déjà pénétré votre système.

Graywares

Le terme graywares désigne plusieurs types de fichiers et applications qui peuvent être secrètement installés sur les ordinateurs afin de suivre les habitudes de navigation Web, afficher des publicités, consigner des touches de clavier, modifier les paramètres Internet, déclencher un comportement anormal de l'ordinateur et même compromettre la sécurité du système (consultez la rubrique *Définition des programmes espions et autres types de graywares* à la page 3-2 pour obtenir plus d'explications sur les différents types de graywares). Consultez le *Manuel de l'administrateur* et l'aide en ligne du serveur OfficeScan pour obtenir des instructions relatives à la configuration d'OfficeScan pour protéger vos clients des graywares).

La solution Services Damage Cleanup

Pour traiter les menaces et les nuisances posées par les programmes espions et les graywares, DCS :

- détectent et suppriment les chevaux de Troie et les graywares actifs
- éliminent les processus que les programmes espions et les graywares créent
- réparent les fichiers système modifiés par les chevaux de Troie et les graywares
- éliminent les fichiers et les applications laissés par les programmes espions et les graywares

Pour mener à bien ces tâches, DCS emploie les composants suivants :

- **Moteur Damage Cleanup** : le moteur utilisé par les services Damage Cleanup pour rechercher et supprimer les chevaux de Troie et leurs processus
- **Modèle Damage Cleanup** : modèle utilisé par le moteur Damage Cleanup qui contribue à identifier les fichiers des chevaux de Troie et leurs processus, de manière à les éliminer
- **Signature pour le nettoyage des programmes espions/graywares** : fichier utilisé par le moteur Damage Cleanup pour aider à éliminer les fichiers espions/publicitaires et leurs processus

DCS s'exécute automatiquement sur les clients OfficeScan à ces occasions :


- les utilisateurs clients peuvent effectuer un nettoyage manuel depuis la console principale du client OfficeScan
- vous exécutez la fonction Nettoyage immédiat sur les clients à partir de la console Web du serveur OfficeScan
- les utilisateurs clients peuvent exécuter la fonction Scan manuel, Scan programmé ou Scan immédiat (et le nettoyage des programmes espions et graywares est sélectionné sur l'écran **Paramètres généraux** du client). Consultez l'aide en ligne du serveur OfficeScan pour obtenir plus d'informations.
- après un correctif (hot fix) ou le déploiement d'un correctif (consultez la rubrique *À propos des correctifs, corrections, et service packs* à la page 1-13 pour obtenir de plus amples informations)
- Lors du redémarrage du service OfficeScan (le service de surveillance du client OfficeScan doit être sélectionné pour relancer le client automatiquement si le programme client se ferme de façon inattendue. Activez cette fonction sur l'écran **Paramètres généraux du client**. Consultez la rubrique *Configuration des paramètres généraux* à la page 2-67 pour obtenir plus de détails.)

Étant donné que DCS s'exécute automatiquement, vous ne devez pas le configurer. Les utilisateurs ne remarquent même pas l'exécution du programme DCS, qui s'opère en arrière-plan pendant que le client OfficeScan est en service. Toutefois, OfficeScan peut parfois demander à l'utilisateur de redémarrer son ordinateur pour terminer la procédure de suppression des chevaux de Troie ou des graywares.

Exécution du nettoyage immédiat

La fonction de nettoyage immédiat permet d'exécuter Services Damage Cleanup à distance. Consultez la rubrique *Damage Cleanup Services de Trend Micro* à la page 1-19 pour obtenir de plus amples informations sur la façon dont fonctionne DCS.

Pour exécuter le nettoyage immédiat :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez les domaines ou les clients sur lesquels vous souhaitez effectuer un nettoyage immédiat, en cliquant sur leurs icônes dans l'arborescence des domaines. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine . Vous pouvez rechercher des clients en appliquant des critères de sélection tels que le nom de l'ordinateur, l'adresse IP ou la version du fichier de signatures ; vous pouvez également changer l'affichage de l'arborescence client.
3. Cliquez sur **Nettoyage immédiat** dans la barre latérale. L'écran **Nettoyage immédiat** apparaît ; il affiche les clients ou les domaines sélectionnés.
4. Dans **Ordinateur**, sélectionnez les clients sur lesquels vous souhaitez exécuter le nettoyage immédiat, puis cliquez sur **Démarrer la notification**. Le serveur demande alors aux clients d'exécuter la fonction de nettoyage immédiat en utilisant le dernier modèle Damage Cleanup que le serveur OfficeScan a reçu des laboratoires TrendLabs.

Cliquez sur **Sélectionner les ordinateurs non informés** pour sélectionner tous les clients qui n'ont pas encore été informés.

Pour localiser un ordinateur en particulier, saisissez son nom (complet ou partiel) dans le champ Nom d'ordinateur.

Pour stopper l'envoi des notifications aux clients qui n'ont pas encore démarré la fonction de nettoyage, procédez comme suit :

Pour stopper les notifications :

1. Choisissez les clients sur lesquels vous ne souhaitez plus effectuer un nettoyage immédiat.
2. Cliquez ensuite sur **Arrêter la notification**. Les clients qui n'ont pas encore démarré le nettoyage sont alors exclus de votre requête. En revanche, les clients qui ont déjà démarré le nettoyage continuent leur procédure normalement.

Configuration des paramètres anti-programmes espions

La configuration des paramètres anti programmes espions/graywares comporte deux étapes :

1. Configurez tous les types de scans (Scan manuel, Scan en temps réel, Scan programmé et Scan immédiat) pour rechercher des fichiers et applications de programmes espions et autres graywares et les supprimer.
2. Activez les services Damage Cleanup pour nettoyer les restes d'applications de programmes espions et autres graywares et mettre fin à tout processus susceptible d'avoir été exécuté par des applications du genre.

Pour rechercher et supprimer les programmes espions et d'autres types de graywares :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines **Client** apparaît.
2. Sélectionnez les domaines ou les clients auxquels vous souhaitez accorder des privilèges en cliquant sur leurs icônes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Options de scan** dans la barre latérale.
4. Cliquez sur les paramètres du type de scan à configurer. L'écran de paramétrage s'affiche pour ce type de scan.
5. Cochez la case **Rechercher les programmes espions/graywares**.
6. Cliquez sur **Enregistrer**.
7. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
8. Cliquez sur **Paramètres clients généraux**. L'écran Paramètres clients généraux s'affiche.
9. Cochez la case permettant d'**activer les services Damage Cleanup pour nettoyer les programmes espions/graywares (applications en cours d'exécution uniquement)** : Ceci permet aux ordinateurs clients d'exécuter DCS pour nettoyer les programmes espions et autres applications et processus de graywares en cours d'exécution. Ce paramètre s'applique à tous les clients enregistrés sur le serveur OfficeScan.

10. Si vous souhaitez éviter qu'OfficeScan analyse certains fichiers qu'il peut considérer comme étant des graywares, cliquez sur la case **Activer Liste d'exclusion pour les programmes espions/graywares** et cliquez sur le lien pour configurer la liste d'exclusion :

- a. A partir de la liste **Type**, sélectionnez un type de programme espion ou de grayware.

Remarque : Cliquez sur le lien **Encyclopédie des programmes espions/graywares** pour aller sur le site Web de Trend Micro. Vous pouvez y trouver des informations sur les différents types de graywares, ainsi que les différents types de virus et autres menaces potentielles.

- b. Cliquez sur le programme espion/graywares ou le fichier.
- c. Pour ajouter d'autres applications ou fichiers connus, cliquez sur **Rechercher** et repérez le fichier adéquat.
- d. Cliquez sur le bouton **AJOUTER**. L'application ou le fichier est ajouté à la liste d'exclusion.
- e. Cliquez sur **Enregistrer** pour fermer la fenêtre de la liste d'exclusion.

11. Si vous souhaitez éviter qu'OfficeScan ne scanne certains types de fichiers et d'applications que Trend Micro considère comme potentiellement légitimes et essentiels au fonctionnement de vos ordinateurs clients, cochez la case **Activer la liste d'exclusion critique de programmes espions/graywares**. Par défaut, tous ces éléments identifiés de cette manière par Trend Micro figurent dans la liste. Cliquez sur le lien pour les supprimer.

- a. Dans la **liste d'exclusion**, sélectionnez un type de programme espion ou de grayware.

Remarque : Cliquez sur le lien **Encyclopédie des programmes espions/graywares** pour accéder au site Web de Trend Micro. Vous y trouverez des informations sur les différents types de graywares, ainsi que les différents types de virus et autres menaces potentielles.

- b. Cliquez sur le bouton **Supprimer**. L'application ou le fichier est ajouté à la liste d'exclusion.

12. Cliquez sur **Enregistrer** pour fermer la fenêtre de la liste d'exclusion. Cliquez sur **Enregistrer** dans l'écran **Paramètres clients généraux**.
13. Pour analyser votre protection anti-programmes espions/graywares, affichez le journal de virus, qui est l'endroit où OfficeScan consigne les détections d'infections de ce type (consultez la rubrique *Affichage des journaux de virus* à la page 7-2).

Conseil : Maintenez à jour vos composants anti-programmes espions/graywares OfficeScan. Affichez l'écran Pourcentage de protection contre les programmes espions pour analyser l'état de vos composants de protection contre les programmes espions/graywares (consultez la rubrique *Affichage du Pourcentage de protection contre les programmes espions* à la page 3-11).

Remarque : Par défaut, OfficeScan inclut la détection de programmes espions et autres types de graywares lors de l'envoi d'alertes standard et d'alertes d'épidémies (consultez la rubrique *Configuration des alertes* à la page 2-38).

Affichage du Pourcentage de protection contre les programmes espions

Le pourcentage de protection contre les programmes espions correspond au nombre de clients dont les composants de protection contre les programmes espions/graywares sont mis à jour (moteur de nettoyage des dommages et signature Cleanup de programmes espions/graywares) par rapport au nombre total de clients en ligne. Ce pourcentage peut vous aider à déterminer le degré de mise à jour de vos fonctions de nettoyage de graywares/protection contre les programmes espions.

L'écran Pourcentage de protection contre les programmes espions affiche le nombre d'ordinateurs clients mis à jour ou non pour les clients en ligne, hors ligne et itinérants et pour le nombre total de clients.

Pour afficher le Pourcentage de protection contre les programmes espions :

1. Cliquez sur **Résumé** dans la barre latérale. L'écran **Résumé** apparaît.
2. Sous **Pourcentages de mise à jour de composants de clients**, cliquez sur le nombre à côté de **Pourcentage de protection contre les programmes espions**.

3. Cliquez sur **Afficher les clients obsolètes** pour accéder à l'arborescence client et afficher les clients disposant encore de composants anti-programmes espions/graywares obsolètes.
4. Cliquez sur **Actualiser** pour actualiser les informations présentes à l'écran.

Remarque : Les clients hors ligne ne sont pas repris dans le pourcentage et ne sont pas représentés sur le graphique.

Protection contre les programmes espions

Vous pouvez prendre de nombreuses mesures pour éviter l'installation de programmes espions et autres types de graywares sur vos ordinateurs clients. Trend Micro suggère de prendre les mesures standard suivantes comme initiatives anti-programmes espions/graywares pour votre société :

- Suivez les étapes de configuration de OfficeScan recommandées dans ce chapitre (consultez la rubrique *Configuration des paramètres anti-programmes espions* à la page 3-9)
- Formez les utilisateurs clients à effectuer les opérations suivantes :

Lisez le contrat de licence utilisateur final (CLUF) et la documentation intégrée aux applications téléchargées et installées sur les ordinateurs

Cliquez sur **Non** à tout message demandant l'autorisation de télécharger et installer des logiciels à moins que les utilisateurs clients ne soient certains que le créateur du logiciel et le site Web qu'ils utilisent sont de confiance.

Supprimez tout courrier électronique commercial non sollicité (spam), particulièrement si le spam demande au client de cliquer sur un bouton ou un lien hypertexte.
- Configurez les paramètres du navigateur Web afin d'assurer un niveau de sécurité strict Trend Micro recommande de configurer les navigateurs Web pour qu'ils demandent confirmation aux utilisateurs avant d'installer des contrôles ActiveX. Pour augmenter le niveau de sécurité d'Internet Explorer (IE), allez dans **Outils > Options Internet > Sécurité** et faites glisser le curseur vers un niveau plus élevé. Si ces paramètres posent problème avec des sites Web que vous souhaitez visiter, cliquez sur **Sites...**, puis ajoutez les sites que vous souhaitez visiter dans la liste des sites de confiance.

- En cas d'utilisation de Microsoft Outlook, configurez les paramètres de sécurité de façon qu'Outlook ne fasse pas de téléchargement automatique d'éléments HTML, tels que les images envoyées dans les messages de spam. Les images sont souvent utilisées par les créateurs de programmes espions et de graywares.
- N'autorisez pas l'utilisation de services peer-to-peer de partage de fichiers. Les applications de programmes espions ou autres graywares peuvent se cacher derrière d'autres types de fichiers que vos utilisateurs peuvent souhaiter télécharger tels que les fichiers musicaux MP3.
- Examinez régulièrement les logiciels installés sur vos ordinateurs clients et recherchez les applications pouvant être des programmes espions ou autres graywares. Si vous découvrez une application ou un fichier qu'OfficeScan ne peut pas détecter comme étant grayware mais que vous jugez comment en étant un, envoyez-le à Trend Micro : <http://www.trendmicro-europe.com/avservice/>.

Trend Labs analysera les fichiers et les applications que vous envoyez.

Consultez la rubrique *Contacteur Trend Micro* à la page 9-20 pour obtenir plus d'informations.

- Maintenez à jour votre système d'exploitation Windows avec les correctifs les plus récents de Microsoft. Consultez le site Web de Microsoft pour obtenir davantage de détails.

Exécution des tâches administratives supplémentaires

Pendant l'installation du serveur OfficeScan, vous avez configuré les paramètres pour le mot de passe de la console Web et l'adresse IP du serveur Web. Si besoin est, vous pouvez encore modifier à tout moment plusieurs de ces paramètres via la console Web.

Les rubriques présentées dans ce chapitre incluent :

- *Modification du mot de passe de la console Web* à la page 4-2
- *Définition du proxy intranet* à la page 4-3
- *Modification des informations du serveur Web OfficeScan* à la page 4-4
- *Suppression des clients inactifs* à la page 4-5
- *Configuration du gestionnaire de quarantaine* à la page 4-6
- *Participation au programme international de pistage des virus* à la page 4-7
- *Sauvegarde de la base de données OfficeScan* à la page 4-8

Modification du mot de passe de la console Web

Afin d'empêcher tout utilisateur non-autorisé de modifier vos paramètres ou de supprimer le programme client sur vos ordinateurs, la console Web d'OfficeScan est protégée par un mot de passe. Le programme principal d'installation OfficeScan nécessite un mot de passe pour la console Web. Vous pouvez toutefois modifier votre mot de passe à partir de la console Web.

Pour modifier le mot de passe de la console :

1. Dans la barre latérale, cliquez sur **Administration > Définir le mot de passe de la console**. L'écran **Définir le mot de passe de la console** apparaît.
2. Saisissez le mot de passe actuel dans la zone de texte **Ancien mot de passe**.
3. Saisissez ensuite le nouveau mot de passe (24 caractères maximum) dans le champ **Nouveau mot de passe**, et confirmez votre saisie dans le champ **Confirmer le mot de passe**.
4. Cliquez sur **Enregistrer**.

Remarque : Si vous avez oublié le mot de passe de votre console, contactez le service d'assistance technique de Trend Micro pour savoir comment accéder à votre console sans saisir de mot de passe. La seule alternative possible est la suppression et la réinstallation d'OfficeScan.

Définition du proxy intranet

La console Web utilise deux paramètres proxy : un pour la communication client-serveur sur l'intranet et un pour le serveur lorsqu'il se connecte à Internet pour télécharger des mises à jour sur le serveur de mise à jour de Trend Micro.

Normalement, les communications serveur-client sur l'intranet ne nécessitent pas de serveur proxy. Si toutefois votre réseau utilise un serveur proxy pour les communications internes, vous pouvez paramétrer OfficeScan de façon à ce qu'il utilise un proxy intranet.

Pour paramétrer le proxy Intranet :

1. Dans la barre latérale, cliquez sur **Administration > Proxy Intranet**. L'écran **Proxy Intranet** apparaît.
2. Cochez la case **Activer le proxy Intranet**.
3. Saisissez ensuite le nom du serveur proxy et son numéro de port. Si votre entreprise utilise SOCKS 4, cochez la case à côté de **Utiliser SOCKS 4**.
4. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, saisissez ces données dans les champs prévus à cet effet.
5. Cliquez sur **Enregistrer**.

Modification des informations du serveur Web OfficeScan

Le serveur Web permet d'utiliser la console Web pour exécuter des tâches administratives majeures relatives à OfficeScan. Pendant l'installation principale, le programme d'installation définit automatiquement un serveur Web. Dès que l'installation principale est terminée, vous pouvez commencer à utiliser la console Web pour configurer OfficeScan.

Toutefois, si vous modifiez les paramètres du serveur Web en externe (par exemple à partir de la console de gestion IIS), sachez que vous devez également apporter des modifications dans OfficeScan pour vous assurer qu'il maintient la communication serveur-client et que vous pouvez toujours accéder à la console Web. Si, par exemple, vous changez manuellement l'adresse IP du serveur ou si vous lui attribuez une adresse IP dynamique, vous devez reconfigurer les paramètres du serveur Web dans OfficeScan.

Conseil : Si votre serveur obtient une adresse IP dynamique, Trend Micro vous recommande d'utiliser le nom de domaine complet du serveur, au lieu de son adresse IP. Ainsi, vous serez certain que vos clients trouveront systématiquement le serveur, bien qu'il possède une adresse IP dynamique.

Pour configurer le serveur Web :

1. Dans la barre latérale, cliquez sur **Administration > Serveur Web**. L'écran **Serveur Web** apparaît.
2. Saisissez le nom de domaine ou l'adresse IP du serveur OfficeScan.
3. Saisissez ensuite le numéro du port utilisé par le serveur OfficeScan.
4. Cliquez sur **Enregistrer**.

Remarque : Ce port est le port sécurisé que le serveur OfficeScan et le client utilisent pour communiquer entre eux.

Suppression des clients inactifs

Lorsque vous utilisez le programme de désinstallation du client pour supprimer le client OfficeScan sur un ordinateur, le programme en informe automatiquement le serveur. Dès qu'il reçoit cette information, le serveur supprime le client dans l'arborescence des domaines, indiquant ainsi que le client n'existe plus.

En revanche, si le client est désinstallé d'une autre façon (reformatage du disque dur de l'ordinateur ou suppression manuelle des fichiers clients, par exemple), OfficeScan n'est pas informé de cette suppression et considère les clients comme « clients inactifs ». Lorsqu'un utilisateur décharge ou désactive le client sur une longue période, le serveur considère également ce client comme un « client inactif ».

Pour que l'arborescence des domaines affiche uniquement les clients actifs, vous devez configurer OfficeScan de telle sorte qu'il supprime automatiquement de l'arborescence tous les clients inactifs.

Pour supprimer automatiquement les clients inactifs :

1. Dans la barre latérale, cliquez sur **Administration > Clients inactifs**. L'écran **Clients inactifs** apparaît.
2. Cochez la case **Activer la suppression automatique des clients inactifs**.
3. Précisez ensuite combien de jours doivent se passer avant qu'OfficeScan considère un client comme inactif.
4. Cliquez sur **Enregistrer**.

Configuration du gestionnaire de quarantaine

Si un client détecte une menace Internet dans un fichier et si l'action de scan configurée pour ce type de menace est l'option Mise en quarantaine, le programme client OfficeScan encode automatiquement le fichier infecté, le place dans le répertoire Suspect du client Officescan et l'envoie vers le dossier de quarantaine du serveur. OfficeScan encode le fichier infecté afin d'éviter qu'il n'infecte d'autres fichiers.

L'emplacement par défaut du dossier Suspect du client OfficeScan est le suivant :

Program Files\Trend Micro\OfficeScan Client\SUSPECT

L'emplacement par défaut du dossier de quarantaine du serveur OfficeScan est le suivant :

OfficeScan\PCCSRV\Virus

Remarque : Si le client OfficeScan client n'est pas capable d'envoyer le fichier encodé au serveur OfficeScan pour une raison quelconque, tel qu'un problème de connexion réseau, le fichier encodé reste dans le répertoire Suspect du client. Le client essaie d'envoyer à nouveau le fichier lorsqu'il se reconnecte au serveur OfficeScan.

Pour obtenir davantage d'informations sur la configuration des paramètres de scan et pour savoir comment changer l'emplacement du dossier de quarantaine, consultez la rubrique *Définition des options de scan* à la page 2-46 et sélectionnez un type de scan.

À partir de l'écran Gestionnaire de quarantaine, vous pouvez configurer la capacité globale du dossier de quarantaine et la taille maximale autorisée pour chaque fichier individuel infecté déposé dans le dossier de quarantaine.

Pour configurer le dossier de quarantaine :

1. Dans la barre latérale, cliquez sur **Administration > Gestionnaire de quarantaine**. L'écran **Gestionnaire de quarantaine** apparaît.
2. Pour définir la capacité globale du dossier de quarantaine, saisissez une nouvelle valeur (en Mo) dans le champ **Capacité du dossier Quarantaine**. La capacité par défaut est fixée à 10 240 Mo.

3. Pour définir la taille maximale de chaque fichier infecté pouvant être déposé dans le dossier de quarantaine, saisissez une nouvelle valeur (en Mo) dans le champ **Taille maximale d'un fichier unique**. La taille par défaut est fixée à 64 Mo.
4. Cliquez sur **Enregistrer**.
Pour supprimer tous les fichiers stockés dans le dossier de quarantaine, cliquez sur **Supprimer tous les fichiers en quarantaine**.

Participation au programme international de pistage des virus

Vous pouvez envoyer les résultats de scan depuis votre installation OfficeScan vers le programme international de pistage des virus afin de mieux suivre les tendances des épidémies. Votre participation à ce programme peut contribuer aux tentatives de compréhension du développement et de la diffusion des infections virales.

Lorsque vous installez OfficeScan, le programme d'installation OfficeScan vous demande si vous voulez participer à ce programme, mais vous pouvez changer ce paramètre à tout moment.

Pour enregistrer les paramètres de participation au programme de pistage des virus :

1. Dans la barre latérale, cliquez sur **Administration > Pistage international des virus**. L'écran **Programme international de pistage des virus** apparaît.
2. Lisez l'avis de non-responsabilité et cliquez sur **Oui** pour participer au programme international de pistage des virus ou sur **Non** pour ne pas y participer.
3. Cliquez sur **Enregistrer**.
Pour afficher la carte des virus actuelle Trend Micro, cliquez sur Virus Map ou saisissez l'adresse suivante sur votre navigateur Web :

`http://fr.trendmicro-europe.com/enterprise/security_info/virus_flash_map.php`

Sauvegarde de la base de données OfficeScan

La base de données du serveur contient tous les paramètres OfficeScan, y compris les paramètres de scan et les privilèges. En cas d'endommagement de votre base de données serveur, vous pouvez facilement la restaurer si vous disposez d'une copie de sauvegarde. Vous pouvez créer une sauvegarde de la base de données manuellement ou configurer un programme de sauvegarde automatique.

Lorsque vous sauvegardez la base de données, OfficeScan vous aide automatiquement à la défragmenter et répare éventuellement toute corruption du fichier d'index.

Conseil : Trend Micro recommande de configurer un programme de sauvegarde automatique. Sauvegardez la base de données durant les heures creuses lorsque les demandes sur le serveur sont faibles.

AVERTISSEMENT ! *Afin de garantir une sauvegarde correcte de la base de données, ne l'effectuez à l'aide d'aucun autre outil ou programme. Configurez la sauvegarde de la base de données uniquement à partir de la console Web d'OfficeScan.*

Pour programmer la sauvegarde de la base de données :

1. Dans la barre latérale, cliquez sur **Administration > Sauvegarde de la base de données**. L'écran **Sauvegarde de la base de données** s'affiche ; il résume les résultats de la dernière sauvegarde.
2. Pour configurer le programme de sauvegarde automatique, procédez comme suit :
 - a. Cochez la case **Activer la sauvegarde de la base de données programmée**.
 - b. Cliquez sur l'une des options sous le menu **Fréquence** :
 - **Quotidienne** : pour une sauvegarde quotidienne
 - **Hebdomadaire** : pour une sauvegarde hebdomadaire. Sélectionnez un jour.
 - **Mensuelle** : pour une sauvegarde mensuelle. Sélectionnez un jour du mois.

- c. Indépendamment de la fréquence sélectionnée dans **Quotidienne**, **Hebdomadaire** ou **Mensuelle**, vous devez spécifier l'heure d'exécution de la sauvegarde d'une base de données dans les zones **Heure de début**.
- d. Spécifiez le répertoire où vous souhaitez sauvegarder la base de données et n'existe pas. Précisez le lecteur et le chemin d'accès complet du répertoire (à savoir `c:\OfficeScan\DatabaseBackup`).
- a. Par défaut, OfficeScan copie la sauvegarde dans le répertoire suivant :
`c:\Program Files\Trend Micro\OfficeScan\backup\`
 OfficeScan permet de créer un sous-dossier sous le chemin de sauvegarde. Le nom du dossier repose sur l'heure de la sauvegarde et possède le format suivant : AAAAMMJJ_HHMMSS. OfficeScan conserve les sept dossiers de sauvegarde les plus récents et supprime le(s) dossier(s) antérieur(s).
 Si le chemin de sauvegarde désigne un ordinateur distant (en utilisant un chemin UNC), saisissez un nom de compte adapté et le mot de passe correspondant afin d'avoir un accès en écriture.
- b. Cliquez sur **Enregistrer**.

Pour sauvegarder la base de données manuellement :

1. Dans la barre latérale, cliquez sur **Administration > Sauvegarde de la base de données**. L'écran **Sauvegarde de la base de données** s'affiche ; il résume les résultats de la dernière sauvegarde.
2. Spécifiez le répertoire où vous souhaitez sauvegarder la base de données et cochez la case **Créer dossier** afin qu'OfficeScan crée le répertoire s'il n'existe pas. Précisez le lecteur et le chemin d'accès complet du répertoire (à savoir `c:\OfficeScan\DatabaseBackup`). Par défaut, OfficeScan copie la sauvegarde dans le répertoire suivant :
`c:\Program Files\Trend Micro\OfficeScan\backup\`
 OfficeScan permet de créer un sous-dossier sous le chemin de sauvegarde. Le nom du dossier repose sur l'heure de la sauvegarde et possède le format suivant : AAAAMMJJ_HHMMSS. OfficeScan conserve les sept dossiers de sauvegarde les plus récents et supprime le(s) dossier(s) antérieur(s).
 Si le chemin de sauvegarde désigne un ordinateur distant (en utilisant un chemin UNC), saisissez un nom de compte adapté et le mot de passe correspondant afin d'avoir un accès en écriture.
3. Pour sauvegarder une base de données manuellement, cliquez sur **Sauvegarder maintenant**

Pour restaurer les fichiers de sauvegarde de la base de données :

1. arrêtez le service principal OfficeScan.
2. Remplacez les fichiers de la base de données dans \PCCSRV\HTTPDB par les fichiers de sauvegarde.
3. Redémarrez le service principal OfficeScan.

Gestion des épidémies

OfficeScan fournit plusieurs méthodes pour gérer les épidémies sur votre réseau. Celles-ci incluent l'activation d'OfficeScan pour surveiller le réseau à la recherche de toute activité suspecte, en bloquant les dossiers et les ports importants des ordinateurs clients, en envoyant aux clients des messages d'alerte d'épidémie virale et en nettoyant les machines infectées.

Les rubriques présentées dans ce chapitre incluent :

- *Mise en œuvre de la prévention contre les épidémies virales* à la page 5-2
- *Configuration du moniteur d'activité virale* à la page 5-11

Mise en œuvre de la prévention contre les épidémies virales

Utilisez l'option Prévention des épidémies pour bloquer des ports de dossiers partagés spécifiques et pour interdire l'accès en écriture à des dossiers et des fichiers spécifiés sur les clients sélectionnés. Configurez également un message d'alerte qui s'affiche sur les ordinateurs clients OfficeScan.

AVERTISSEMENT ! *La fonction de prévention des épidémies ne doit être activée qu'en présence d'une épidémie virale. Configurez alors les paramètres de prévention avec soin. Une mauvaise configuration peut entraîner des problèmes de réseau imprévus.*

Une fois que vous avez activé la Prévention d'épidémies, vérifiez qu'une coche verte apparaît dans la colonne **OPP** des clients sélectionnés dans l'arborescence client.

Une fois que vous avez désactivé la prévention d'épidémies, Trend Micro vous recommande d'exécuter un scan immédiat pour vous aider à éradiquer les chevaux de Troie de vos clients ainsi que tous les processus qui leur sont liés ainsi qu'aux programmes espions et aux autres types de graywares (consultez la rubrique *Exécution du nettoyage immédiat* à la page 3-8).

Blocage des dossiers partagés

Pendant les épidémies virales, vous pouvez bloquer les dossiers partagés sur le réseau afin d'empêcher les virus de se répandre par leur intermédiaire. Certains virus sont en effet capables d'accéder aux ordinateurs par l'intermédiaire des dossiers partagés.

Pour bloquer les dossiers partagés :

1. Cliquez sur **Prévention des épidémies** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Cliquez sur les domaines ou les clients pour lesquels vous souhaitez activer la prévention, en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine. Vous pouvez également rechercher des clients en appliquant des critères de sélection et changer l'affichage de l'arborescence client.

3. Cliquez sur **Déployer maintenant** dans la barre latérale. L'écran **Paramètres de prévention des épidémies** apparaît.
4. Dans **Paramètres de prévention des épidémies**, sélectionnez **Bloquer les dossiers partagés**.
5. Pour configurer les paramètres de blocage des dossiers partagés, cliquez sur **Paramètres**. L'écran **Blocage des dossiers partagés** apparaît.
6. Sous **Paramètres de blocage des dossiers partagés**, indiquez le droit d'accès aux dossiers partagés lorsque vous activez la prévention des épidémies. Choisissez l'une des options suivantes :
 - **Accès en lecture seule**
 - **Aucun accès en lecture et en écriture**
7. Cliquez sur **Enregistrer** pour sauvegarder vos paramètres.
8. Cliquez sur **OK**.
9. Cliquez sur **Précédent** pour revenir à l'écran **Paramètres de prévention des épidémies**.
10. Cliquez sur **Activer les paramètres** pour activer la fonction de prévention dans les domaines ou les clients sélectionnés. L'écran **Prévention des épidémies** apparaît ; il affiche les paramètres de prévention actuels.

Blocage des ports

Pendant les épidémies virales, vous pouvez bloquer les ports vulnérables que les virus et les chevaux de Troie pourraient exploiter pour accéder aux clients.

AVERTISSEMENT ! *Configurez alors les paramètres de prévention avec soin. Le blocage des ports utilisés rendra indisponibles les services réseau qui dépendent de ces ports. Si vous bloquez le port sécurisé, OfficeScan ne peut pas communiquer avec le client pendant la durée de l'épidémie virale.*

Le port sécurisé, configuré durant l'installation du serveur OfficeScan, permet la communication entre le serveur OfficeScan et les clients. Bloquez-le uniquement si c'est nécessaire.

Pour bloquer des ports :

1. Cliquez sur **Prévention des épidémies** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Cliquez sur les domaines ou les clients pour lesquels vous souhaitez activer la prévention, en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Déployer maintenant** dans la barre latérale. L'écran **Paramètres de prévention des épidémies** apparaît.
4. Sous **Paramètres de prévention des épidémies**, cochez la case **Bloquer les ports**.
5. Pour configurer les paramètres de blocage des ports, cliquez sur **Paramètres**. L'écran **Blocage des ports** apparaît.
6. Pour bloquer le port sécurisé, que le serveur et le client utilisent pour communiquer, sélectionnez l'option **Bloquer le port sécurisé**.
7. Pour ajouter d'autres ports à bloquer, cliquez sur **Ajouter des ports**. L'écran **Ajouter des ports à bloquer** apparaît.

8. Spécifiez les ports que vous voulez bloquer. Choisissez l'une des options suivantes :

- **Bloquer tous les ports (y compris ICMP)** : cliquez ici pour bloquer tous les ports, y compris les ports chargés des communications du protocole ICMP (Internet Control Message Protocol).

Remarque : En activant l'option **Bloquer tous les ports (y compris ICMP)**, vous bloquez tous les ports à l'exception du port sécurisé. Pour bloquer également le port sécurisé, cochez la case **Bloquer les ports sécurisés** sur l'écran **Blocage des ports**.

- **Bloquer des ports définis** : cliquez pour spécifier les ports à bloquer. Choisissez l'une des options suivantes :
 - **Ports fréquemment utilisés** : cliquez pour bloquer les numéros de ports communément utilisés pour les services Internet les plus fréquents ; par exemple, le port 80 pour le Web (HTTP) et le port 25 pour les envois de courriers électroniques (SMTP). Si vous cliquez sur **Ports fréquemment utilisés**, sélectionnez ensuite un numéro de port (ou plusieurs) pour qu'OfficeScan sauvegarde vos paramètres de blocage des ports.
 - **Tous les ports des chevaux de Troie** : cliquez pour bloquer tous les ports connus pour être vulnérables aux attaques des chevaux de Troie
 - **Indiquez un numéro ou une plage de ports comprise entre 1 et 65 535** : cliquez pour préciser dans quelle direction le trafic doit être bloqué et une plage de numéros de ports (ou des numéros de ports séparés)

Pour bloquer le trafic entrant, sélectionnez **Trafic entrant**.

Pour bloquer le trafic sortant, sélectionnez **Trafic sortant**

Cliquez sur **Plage de ports** ou sur **Numéro(s) de ports**. Si vous cliquez sur **Intervalle de ports**, utilisez ensuite les champs pour définir un intervalle de numéros de port compris entre 1 et 65 535. Si vous cliquez sur **Numéro(s) de port**, utilisez ensuite les champs numériques pour entrer les numéros des ports que vous souhaitez bloquer. Séparez les entrées par des virgules.

À partir de la liste de **Protocoles**, sélectionnez le protocole de communication que vous souhaitez bloquer (liste déroulante). Sélectionnez Transmission Control Protocol (TCP), User Datagram Protocol (UDP) ou les deux.

Dans **Commentaires**, saisissez des informations complémentaires, par exemple, les raisons pour lesquelles vous bloquez les ports désignés.

- **Protocole de ping (Rejeter ICMP)** : cliquez pour bloquer les paquets ICMP, comme le ping

9. Cliquez sur **OK**. Un écran de confirmation apparaît.
10. Cliquez sur **OK**. L'écran **Blocage des ports** apparaît ; il affiche un résumé de vos paramètres de blocage des ports, avec les ports bloqués, le protocole de communication, les commentaires et la direction du trafic.
11. Cliquez sur **Précédent** pour revenir à l'écran **Prévention des épidémies**.
12. Cliquez sur **Activer les paramètres** pour activer la fonction de prévention dans les domaines ou les clients sélectionnés. L'écran **Prévention des épidémies** apparaît ; il affiche les paramètres de prévention actuels.

Pour modifier les paramètres de blocage des ports existants, consultez la rubrique suivante *[Changement des paramètres de blocage des ports](#)* à la page 5-6.


Changement des paramètres de blocage des ports

Dans la liste des **Paramètres de blocage des ports**, vous pouvez modifier les paramètres des entrées qui suivent :

- Direction du trafic : bloquez le trafic entrant et/ou sortant
- Numéro de port : modifiez le numéro d'un port ou entrez une plage de ports pour chaque entrée dans la liste
- Protocole de trafic : spécifiez TCP, UDP ou les deux
- Commentaire : ajoutez des commentaires pour décrire l'entrée dans la liste

Pour modifier les paramètres d'un port individuel à partir de l'écran Blocage de ports :

1. Cliquez sur **Prévention des épidémies** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Cliquez sur les domaines ou les clients pour lesquels vous souhaitez activer la prévention, en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.

3. Cliquez sur **Déployer maintenant** dans la barre latérale. L'écran **Paramètres de prévention des épidémies** apparaît.
4. Sous **Paramètres de prévention des épidémies**, cochez la case **Bloquer les ports**.
5. Pour configurer les paramètres de blocage des ports, cliquez sur **Paramètres**. L'écran **Blocage des ports** apparaît.
6. Cliquez sur l'icône  dans la colonne **Modifier** pour l'entrée de port que vous voulez modifier. L'écran **Paramètres de blocage des ports** apparaît.
7. Précisez si vous souhaitez bloquer le trafic entrant et/ou sortant ou non.
8. Cliquez sur **Intervalle de ports** et définissez une plage à l'intérieur de laquelle tous les ports seront bloqués ; ou cliquez sur **Numéro(s) de port** et saisissez un ou plusieurs numéros de port individuel à bloquer.
9. Modifiez le protocole de communication utilisé par le(s) port(s) en sélectionnant **TCP**, **UDP** ou **TCP/UDP** dans le menu **Protocole**.
10. Saisissez une description dans le champ **Commentaires** de chaque port, qui contient généralement le nom descriptif du port concerné.
11. Cliquez sur **OK**. Un écran de confirmation apparaît.
12. Cliquez à nouveau sur **OK** pour revenir à l'écran **Blocage des ports**.

Accès en écriture interdit aux fichiers et aux dossiers

Les virus peuvent modifier ou supprimer les fichiers et les dossiers stockés sur les ordinateurs infectés. Heureusement, vous pouvez configurer OfficeScan de telle sorte que les virus ne puissent plus modifier ni supprimer les fichiers et les dossiers de vos postes clients pendant une épidémie virale.

Pour interdire l'accès en écriture dans les fichiers et les dossiers :

1. Cliquez sur **Prévention des épidémies** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Cliquez sur les domaines ou les clients pour lesquels vous souhaitez activer la prévention, en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Déployer maintenant** dans la barre latérale. L'écran **Paramètres de prévention des épidémies** apparaît.


4. Dans **Paramètres de prévention des épidémies**, sélectionnez **Interdire l'accès en écriture aux fichiers et aux dossiers**.
5. Pour configurer les paramètres de blocage des dossiers partagés, cliquez sur **Paramètres**. L'écran **Paramètres d'interdiction en écriture** apparaît.
6. Pour protéger les répertoires et fichiers portant une extension spécifique, indiquez le chemin du répertoire à protéger dans le champ **Chemin d'accès au répertoire**. À titre d'exemple, vous pouvez saisir le chemin
C:\Windows\System32. Vous devez saisir le chemin d'accès absolu, et pas le chemin d'accès virtuel. Si vous saisissez plusieurs chemins d'accès, séparez les entrées à l'aide d'un point-virgule (;).

Lorsque vous aurez saisi le chemin d'accès au dossier que vous souhaitez protéger, cliquez sur **Ajouter**. Le chemin apparaît alors sous **Répertoires protégés**. Avant de continuer, assurez-vous que tous les dossiers à protéger sont bien affichés sous **Répertoires protégés**.

Remarque : OfficeScan protège également tous les sous-dossiers contenus dans le dossier spécifié.

Précisez ensuite les fichiers à protéger dans la liste **Répertoires protégés** ; pour cela, vous devez utiliser leur extension. Choisissez l'une des options suivantes :

- **Tous les fichiers dans les répertoires protégés**
- **Fichiers dotés des extensions suivantes dans les répertoires protégés**

Pour utiliser certaines extensions, sélectionnez les extensions à protéger dans la **liste des extensions** et cliquez sur .

Pour sélectionner une extension qui ne figure pas dans la liste proposée, saisissez simplement cette extension dans la zone de texte, puis cliquez sur **Ajouter**. Si vous saisissez plusieurs extensions, séparez les entrées à l'aide d'un point-virgule (;).

Pour protéger certains fichiers spécifiques, saisissez leurs noms complets dans le champ **Fichiers à protéger**.

7. Cliquez sur **Enregistrer** pour sauvegarder les paramètres. Un écran de confirmation apparaît.

8. Cliquez sur **OK**. Le chemin d'accès au répertoire que vous souhaitez protéger est visible sous **Répertoires protégés** dans l'écran **Paramètres d'interdiction en écriture**.
9. Cliquez sur **Précédent** pour revenir à l'écran **Paramètres de prévention des épidémies**.
10. Cliquez sur **Activer les paramètres** pour activer la fonction de prévention dans les domaines ou les clients sélectionnés. L'écran **Prévention des épidémies** apparaît ; il affiche les paramètres de prévention actuels.

Configuration de la notification des clients en cas d'épidémies

Pour informer les utilisateurs que la fonction de prévention des épidémies est active, vous pouvez faire apparaître des notifications d'épidémies sur les postes des clients.

Pour afficher une notification d'épidémie sur un poste client :

1. Cliquez sur **Prévention des épidémies** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Cliquez sur les domaines ou les clients pour lesquels vous souhaitez activer la prévention, en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Déployer maintenant** dans la barre latérale. L'écran **Paramètres de prévention des épidémies** apparaît.
4. Cochez la case **Lorsque la stratégie de prévention des épidémies est activée, afficher le message suivant sur les clients OfficeScan**.
5. Acceptez le message par défaut ou saisissez un nouveau message dans la zone de texte.
6. Cliquez sur **Appliquer les paramètres** pour enregistrer vos paramètres.

Remarque : Vous pouvez également configurer des alertes d'épidémies pour les envoyer vers votre poste ou vers les administrateurs OfficeScan par e-mail, pageur, déroutement SNMP ou par le journal des événements de Windows NT *Configuration des alertes d'épidémies* à la page 2-42).

Désactivation de la prévention des épidémies

Si vous êtes absolument certain que l'épidémie détectée a été contenue et que tous les fichiers infectés ont été nettoyés ou mis en quarantaine, vous pouvez rétablir les valeurs normales de vos paramètres réseau en désactivant la fonction de prévention des épidémies.

Pour désactiver la prévention des épidémies :

1. Cliquez sur **Prévention des épidémies** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Cliquez sur les domaines ou les clients pour lesquels vous souhaitez activer la prévention, en cliquant sur les icônes correspondantes dans l'arborescence. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Restaurer** dans la barre latérale. L'écran **Restaurer les paramètres de prévention des épidémies** apparaît.
4. Si vous souhaitez informer les utilisateurs que l'épidémie est enrayée, cochez la case **Message d'alerte – Prévention des épidémies désactivée**. Vous pouvez accepter le message par défaut ou saisir un nouveau message dans la zone de texte Message d'alerte.
5. Cliquez sur **Rétablir**.
6. L'écran **Prévention des épidémies** apparaît ; il affiche un message indiquant que la prévention des épidémies est désactivée au niveau des domaines et des ordinateurs sélectionnés.

Pour être certain que la fonction de prévention est bien désactivée, vérifiez que la coche verte n'apparaît plus dans la colonne **OPP** des clients sélectionnés dans l'arborescence client.

Remarque : Si vous ne restaurez pas les paramètres réseau manuellement, ils seront restaurés automatiquement par OfficeScan après expiration du nombre d'heures spécifié dans **Restaurer automatiquement les paramètres initiaux du réseau après { } heures**, sur l'écran **Paramètres de prévention des épidémies**. La valeur par défaut est fixée à 48 heures.

Configuration du moniteur d'activité virale

Les clients OfficeScan peuvent surveiller le réseau à la recherche de toute activité suspecte pouvant signaler une infection. Un nombre excessif de sessions ouvertes simultanément sur le réseau peut indiquer que les clients en réseau sont infectés ou attaqués. Dans ce cas, il est possible de configurer un message d'alerte qui sera envoyé par OfficeScan.

Pour configurer le moniteur d'activité virale :

1. Cliquez sur **Moniteur d'activité virale** dans la barre latérale. L'écran **Moniteur d'activité virale** apparaît.
2. Cochez la case **Activer le moniteur d'activité virale**.
3. Sous **Critères d'alerte pour le moniteur d'activité virale**, entrez le nombre minimum de sessions réseau et la durée (en minutes) pendant laquelle elles sont détectées. Ces critères détermineront à quel moment le message d'alerte sera envoyé.

Conseil : Lors de la définition du nombre de sessions de réseau, Trend Micro propose de prendre le nombre de clients divisés par 10 ((#clients)/10) pour chaque tranche horaire de trois minutes.

4. Pour envoyer un message d'alerte, cochez la case **Envoyer une notification par e-mail si les critères d'alerte sont remplis**.
5. Si vous activez un message d'alerte, remplissez les champs suivants dans **Paramètres du message d'alerte** :
 - **SMTP** : saisissez le nom de domaine du serveur de messagerie.
 - **Numéro de port** : saisissez le numéro de port utilisé par le serveur OfficeScan pour communiquer avec le serveur de messagerie (par défaut : port 25).
 - **À** : saisissez l'adresse du destinataire
 - **De** : saisissez le nom de l'expéditeur
 - **Objet** : saisissez l'objet de l'alerte
 - **Message** : saisissez le message d'alerte
6. Cliquez sur **Enregistrer** pour sauvegarder les paramètres.

Pour afficher et sauvegarder les enregistrements du moniteur :

1. Cliquez sur le lien affichant le nombre de sessions réseau enregistrées, sous **État actuel**. L'écran **Enregistrements du moniteur d'activité virale** apparaît.
2. Pour sauvegarder le journal en tant que fichier CSV (séparateur : point-virgule), cliquez sur Exporter vers fichier CSV. Un écran de confirmation apparaît.
3. Cliquez sur **Ouvrir** pour afficher le fichier dans votre tableur, sans l'enregistrer.
4. Cliquez sur **Enregistrer**, puis définissez le dossier dans lequel doit être déposé le fichier CSV.

Remarque : Utilisez un tableur pour afficher les fichiers de données CSV.

Configuration du Pare-feu pour clients – version d’entreprise

Ce chapitre décrit comment configurer les paramètres du Pare-feu pour clients – version d’entreprise pour protéger vos clients contre les piratages et les virus réseau.

Les rubriques présentées dans ce chapitre incluent :

- *Définition du Pare-feu pour clients – version d’entreprise* à la page 6-2
- *Pare-feu par défaut* à la page 6-5
- *Moniteur d'activité virale du pare-feu* à la page 6-8
- *Configuration du Pare-feu pour clients – version d’entreprise* à la page 6-13
- *Désactivation du pare-feu* à la page 6-23

Définition du Pare-feu pour clients – version d'entreprise

Les étapes suivantes sont nécessaires pour réussir le déploiement et utiliser le Pare-feu pour clients – version d'entreprise :

1. **Créer une stratégie** : la stratégie vous permet de sélectionner un niveau de sécurité qui bloque ou autorise le trafic de tous les clients et active les fonctions du pare-feu
2. **Ajouter des exceptions à la stratégie** : les exceptions permettent aux clients de dévier d'une stratégie. Grâce aux exceptions, vous pouvez spécifier des clients et autoriser ou bloquer certains types de trafic des clients, malgré le paramètre de niveau de sécurité dans la stratégie. Par exemple, vous pouvez bloquer tout le trafic pour un ensemble de clients dans une stratégie et créer une exception qui autorise le trafic HTTP pour que les clients puissent accéder à un serveur Web.
3. **Créer un profil** : le profil vous permet de choisir une stratégie (qui inclut des exceptions) à associer au profil, de spécifier les clients qui reçoivent le profil et de définir les privilèges client qui autorisent ou interdisent aux utilisateurs de modifier les paramètres du pare-feu
4. **Sélectionner des profils et les déployer vers les clients** : sélectionnez les profils que vous souhaitez utiliser et déployez-les vers les clients spécifiés dans le profil.

Conseil : Trend Micro recommande de désinstaller les autres pare-feu des logiciels sur les clients OfficeScan avant de déployer et d'activer le Pare-feu pour clients – version d'entreprise. Plusieurs installations de pare-feu sur le même ordinateur peuvent produire des résultats inattendus.

Pour obtenir les toutes dernières informations concernant les problèmes de compatibilité avec des pare-feu tiers, consultez la Base de connaissances Solution ID 20473. Elle est disponible sur le site Web suivant :

http://fr.trendmicro-europe.com/enterprise/support/knowledge_base_detail.php?searchSolutionID=20437

Définition des stratégies, des exceptions et des profils

Le pare-feu pour clients – version d'entreprise fait appel à des stratégies, des exceptions et des profils afin d'organiser et de personnaliser des méthodes de protection des clients sur le réseau.

Stratégies

Les stratégies sont incluses dans l'une des options suivantes :

- **Niveau de sécurité** : un paramètre général qui bloque ou autorise l'ensemble du trafic entrant et / ou sortant
- **Paramètres du Pare-feu pour clients – version d'entreprise** : activer ou désactiver le Pare-feu pour clients – version d'entreprise, le système de détection d'intrusion et le message d'alerte
- **Une liste d'exceptions** : une liste configurable d'exceptions qui permet de bloquer ou d'accepter les divers types de trafic réseau

Exceptions

Les exceptions sont des paramètres plus spécifiques qui permettent d'autoriser ou de bloquer les divers types de trafic réseau à partir du (des) numéro(s) de port(s) de l'ordinateur client et de (des) adresse(s) IP. Vous pouvez configurer une liste d'exception que vous associez à chaque stratégie. Les exceptions contenues dans la liste écrasent le paramètre de **Niveau de sécurité** dans une stratégie.

Les paramètres d'exception incluent :

- **Action** : bloquer ou autoriser tout le trafic qui répond aux critères des exceptions
- **Direction** : trafic réseau entrant ou sortant vers/depuis le client
- **Protocole** : le type de trafic : TCP, UDP, ICMP
- **Port(s)** : les ports sur l'ordinateur client sur lesquels vous souhaitez exécuter l'action
- **Ordinateurs** : les ordinateurs du réseau auxquels le critère de trafic ci-dessus s'applique

Configuration des exceptions : un exemple

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

Profils

OfficeScan utilise des profils pour définir les clients auxquels la stratégie associée est appliquée et pour configurer les privilèges du pare-feu des clients. Vous pouvez regrouper logiquement les paramètres de scan et de mise à jour par domaine OfficeScan ou par une sélection individuelle des clients. Les profils offrent une flexibilité en vous permettant de sélectionner les critères qu'un client ou un groupe de client doivent respecter avant d'appliquer une stratégie. Les profils sont inclus dans l'une des options suivantes :

- **Une stratégie associée** : chaque profil utilise une seule stratégie
- **Critères du client** : la stratégie est appliquée aux clients qui répondent aux critères suivants :
 - Adresse IP** : un client qui a une certaine adresse IP, des clients qui correspondent à une plage d'adresses IP ou des clients dont l'adresse IP appartient à un sous-réseau spécifié
 - Domaine** : des clients qui appartiennent à un domaine OfficeScan déterminé
 - Nom de l'ordinateur** : des clients qui ont les noms de poste spécifiés
 - Plate-forme** : des clients qui fonctionnent soit avec Windows Server (NT/2000/Server 2003) ou Windows Workstation (NT/2000/XP)
 - Nom de connexion** : des clients auxquels des utilisateurs spécifiques se sont connectés
 - Etat du client** : si des clients sont en ligne ou hors-ligneSélectionnez une combinaison de critères client pour spécifier les postes clients
- **Privilèges utilisateur** : permet ou empêche les utilisateurs du client d'effectuer les opérations suivantes :
 - Modifier le niveau de sécurité spécifié dans une stratégie
 - Modifier la liste des exceptions associée à une stratégie

Remarque : OfficeScan applique les profils du Pare-feu pour clients – version d'entreprise aux clients, dans l'ordre de leur apparition dans la liste des profils. Par exemple, si un client correspond au premier profil, OfficeScan applique au client les actions configurées pour ce profil. Les autres profils qui sont également configurés pour ce client sont ignorés.

Pare-feu par défaut

Le Pare-feu pour clients – version d'entreprise fournit des stratégies, des exceptions et des profils par défaut pour vous donner une base afin d'initier votre stratégie de protection de pare-feu des clients. Les stratégies, les exceptions et les profils par défaut sont présumés inclure des conditions communes qui peuvent être présentes chez vos clients comme les installations pour Cisco NAC Trust Agent et la nécessité d'accéder à la console Web ScanMail pour Microsoft Exchange.

Nom de la stratégie par défaut	Niveau de sécurité	Paramètres client	Exceptions	Utilisation recommandée
Tous les accès	Bas	Activer le pare-feu	Aucune	Utiliser pour permettre aux clients un accès illimité au réseau
Cisco Trust Agent pour Cisco NAC	Bas	Activer le pare-feu	Autoriser le trafic UDP entrant/sortant via le port 21862	Utiliser lorsque les clients ont une installation Cisco Trust Agent (CTA)
Ports de communication pour TCM	Bas	Activer le pare-feu	Autoriser tout le trafic TCP/UDP entrant/sortant via les ports 80 et 10319	Utiliser lorsque les clients ont une installation d'agent Control Manager
Console ScanMail pour Microsoft Exchange (SMEX)	Bas	Activer le pare-feu	Autoriser tout le trafic TCP entrant/sortant via le port 16372	Utiliser lorsque les clients veulent accéder à la console SMEX
Console InterScan Messaging Security Suite (IMSS)	Bas	Activer le pare-feu	Autoriser tout le trafic TCP entrant/sortant via le port 80	Utiliser lorsque les clients veulent accéder à la console IMSS

Nom de l'exception par défaut	Action	Protocole	Port	Direction
DNS	Autoriser	TCP/UDP	53	Entrant et sortant
NetBIOS	Autoriser	TCP/UDP	137,138,139,445	Entrant et sortant
HTTPS	Autoriser	TCP	443	Entrant et sortant

Nom de l'exception par défaut	Action	Protocole	Port	Direction
HTTP	Autoriser	TCP	80	Entrant et sortant
Telnet	Autoriser	TCP	23	Entrant et sortant
SMTP	Autoriser	TCP	25	Entrant et sortant
FTP	Autoriser	TCP	21	Entrant et sortant
POP3	Autoriser	TCP	110	Entrant et sortant

Remarque : Aucune des exceptions par défaut ne spécifie les clients. Si vous utilisez toutes les exceptions par défaut, indiquez les clients auxquels vous voulez appliquer les exceptions.

Nom du profil par défaut	Stratégie utilisée	Appliquée aux clients
Tous les profils clients	Tous les accès	non spécifié

Fonctions du Pare-feu pour clients – version d'entreprise

Le pare-feu pour clients – version d'entreprise contribue à protéger les clients OfficeScan, équipés de Windows NT/2000/XP/Server 2003, des attaques de pirates et des virus réseau, en créant une barrière entre eux et le réseau.

Filtrage du trafic

Le Pare-feu pour clients – version d'entreprise filtre l'ensemble du trafic entrant et sortant, permettant ainsi de bloquer certains types de trafic sur la base des critères suivants :

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

Recherche de virus réseau

Le Pare-feu pour clients – version d'entreprise examine également chaque paquet afin de déterminer s'il est infecté par un virus réseau (consultez la rubrique [Virus de réseau](#) à la page 1-7 pour obtenir plus d'informations).

Profils et stratégies personnalisés

Le Pare-feu pour clients – version d'entreprise vous permet de configurer des stratégies destinées à bloquer ou à autoriser certains types de trafic réseau. Attribuez une stratégie à un ou plusieurs profils que vous pouvez ensuite déployer à des clients OfficeScan. Vous disposez ainsi d'une méthode d'organisation et de configuration personnalisée des paramètres du Pare-feu pour clients – version d'entreprise pour vos clients

Stateful Inspection

Le Pare-feu pour clients – version d'entreprise est un pare-feu stateful inspection ; il contrôle toutes les connexions au client et rappelle tous les états de connexion. Il peut identifier les conditions spécifiques de toute connexion, prédire les actions qui doivent être prises et détecter tout viol des conditions normales. Les décisions de filtrage reposent dès lors non seulement sur les profils et stratégies, mais aussi sur le contexte défini par l'analyse des connexions et par le filtrage des paquets qui sont déjà passés par le pare-feu.

Système de détection d'intrusion

Le pare-feu pour clients – version d'entreprise contient également un Système de détection des intrusions (IDS). Lorsqu'il est activé, IDS peut contribuer à identifier des signatures dans les paquets réseau indiquant une attaque du client. Le pare-feu pour clients – version d'entreprise peut empêcher les intrusions bien connues suivantes :

Fragment trop important, Ping of Death, ARP conflictuel, flux SYN, Fragment de chevauchement, Teardrop, attaque par fragment minuscule, IGMP fragmenté, attaque terrestre

Moniteur d'activité virale du pare-feu

Le Moniteur d'activité virale du pare-feu envoie un message d'alerte à des destinataires spécifiés lorsque le nombre d'entrées dans le journal excède un seuil déterminé, ce qui peut constituer un signal d'attaque.

Privilèges du pare-feu clients

Donne aux clients le privilège de consulter l'onglet du pare-feu pour clients – version d'entreprise sur le programme client OfficeScan. L'onglet du pare-feu pour clients – version d'entreprise affiche les paramètres de ce pare-feu pour ce client. Accorde également aux utilisateurs le privilège d'activer ou de désactiver le pare-feu, le système de détection d'intrusion et le message d'alerte du Pare-feu pour clients – version d'entreprise (consultez la rubrique *Configuration des privilèges et paramètres clients* à la page 2-63).

Remarque : Vous pouvez installer, configurer et utiliser le Pare-feu pour clients – version d'entreprise de Trend Micro sur les ordinateurs Windows XP ayant également un Internet Connection Firewall™ (pare-feu de connexion Internet) activé. Cependant, vous devez gérer attentivement vos stratégies pour éviter de créer des stratégies de pare-feu conflictuelles et de produire des résultats inattendus. Par exemple, si vous configurez un pare-feu pour autoriser le trafic à partir d'un certain port mais que l'autre pare-feu bloque le trafic depuis le même port, le trafic sera bloqué. Consultez votre documentation Microsoft pour obtenir des détails sur le pare-feu Internet Connection Firewall.

Déploiement du pare-feu

Cette section fournit les étapes nécessaires pour le déploiement réussi du Pare-feu pour clients – version d'entreprise.

Pour déployer le pare-feu :

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise > Liste des stratégies**. L'écran **Liste des stratégies** apparaît.
2. Sélectionnez une stratégie par défaut en cochant la case située près du nom de la stratégie. Si vous voulez créer une nouvelle stratégie, cliquez sur **Ajouter**. L'écran **Editeur de stratégies** apparaît.
3. Entrez un nom pour la stratégie.
4. Cliquez sur un **Niveau de sécurité** pour autoriser ou bloquer le trafic entrant/sortant.
5. Cochez la case **Activer le pare-feu**. Vous pouvez également activer le système de détection d'intrusion et/ou un message d'alerte qui s'affichera sur le client s'il bloque un paquet sortant.

Remarque : Si vous autorisez les clients à activer ou désactiver le pare-feu, le Système de détection d'intrusion et le message d'alerte, les paramètres s'affichent sous **Paramètres locaux du pare-feu** sur la console client. Ces paramètres ne peuvent pas être modifiés à partir de la console Web OfficeScan.

Si vous n'accordez pas aux clients ce privilège, les paramètres s'affichent sous **Liste des cartes réseau** sur la console client. Ces paramètres peuvent être modifiés à partir de la console Web du serveur d'OfficeScan.

Les informations sous **Paramètres locaux du pare-feu** sur la console client reflètent toujours les paramètres configurés à partir de la console de celui-ci et non de la console Web du serveur.

6. Sous **Exception**, cochez les cases correspondant aux exceptions par défaut que vous souhaitez inclure dans cette stratégie.
Si vous voulez créer de nouvelles exceptions, procédez comme suit :
 - a. Cliquez sur **Ajouter**. L'écran **Modifier une exception** apparaît.
 - b. Entrez un nom pour l'exception.

- c. Près de **Action**, choisissez si vous autorisez ou si vous interdisez le trafic réseau pour cette exception
- d. A côté de **Direction**, cliquez sur **Entrant** ou **Sortant** pour sélectionner le type de trafic auquel les paramètres de cette exception s'appliquent.
- e. Dans la liste **Protocole**, sélectionnez le protocole utilisé par le trafic réseau que vous autorisez ou que vous interdisez :
 - **Tous**
 - **TCP/UDP (par défaut)**
 - **TCP**
 - **UDP**
 - **ICMP**
- f. Cliquez sur l'une des options suivantes pour spécifier les ports clients :
 - **Tous les ports** (par défaut)
 - **Plage** : saisissez une plage de ports
 - **Spécifique** : spécifiez des ports individuels. Utilisez une virgule (,) pour séparer les numéros de port.
- g. Sous **Ordinateurs**, sélectionnez les adresses IP à inclure dans les exceptions. Par exemple, si vous sélectionnez **Refuser tout le trafic réseau (Entrant et Sortant)** et que vous saisissez l'adresse IP d'un ordinateur unique sur le réseau, chaque client dont la stratégie contient cette exception ne pourra pas envoyer ou recevoir de données vers cette adresse IP ou à partir de celle-ci.
Choisissez l'une des options suivantes :
 - **Toutes les adresses IP** (par défaut)
 - **IP unique** : saisissez le nom de l'hôte ou l'adresse IP d'un client. Pour résoudre le nom de l'hôte du client vers une adresse IP, cliquez sur **Résoudre**.
 - **Plage IP** : entrez une plage d'adresses IP
 - **Masque de sous-réseau** : entrez une adresse IP et un masque de sous-réseau
- h. Cliquez sur **Enregistrer**. L'écran **Editeur de stratégies** apparaît avec la nouvelle exception dans la liste des exceptions.

7. Cochez les cases correspondant aux exceptions que vous voulez inclure dans le profil.
8. Cliquez sur **Enregistrer**. L'écran **Liste des stratégies** apparaît avec la nouvelle stratégie que vous avez créée.
9. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise > Liste des profils**. L'écran **Liste des profils** apparaît.
10. Pour créer un nouveau profil, cliquez sur **Ajouter**. L'écran **Editeur des profils** apparaît.
11. Cliquez sur **Activer ce profil** pour que le serveur OfficeScan puisse déployer ce profil vers les clients OfficeScan.
12. Saisissez un nom d'identification du profil, ainsi qu'une description facultative.
13. Dans la liste à côté de **Utiliser la stratégie suivante**, sélectionnez la stratégie que vous avez créée pour ce profil.
14. Sélectionnez les clients auxquels vous souhaitez appliquer la stratégie. Sélectionnez l'un des critères suivants :
 - **Adresse IP** : (les) l'adresse(s) IP du (des) client(s). Choisissez l'une des options suivantes :
 - **IP unique** : saisissez une adresse IP client valide.
 - **Plage** : saisissez une plage d'adresses IP dans les champs de texte **De** et **A**.
 - **Sous-réseau** : saisissez une adresse IP du sous-réseau et le masque de sous-réseau. OfficeScan utilise ces données pour calculer l'adresse réseau.
 - **Domaine** : le nom de domaine du (des) client(s). Cliquez sur **Afficher la console client** pour sélectionner des clients dans l'arborescence du domaine.
 - **Nom d'ordinateur** : le nom du (des) client(s). Cliquez sur **Afficher la console client** pour sélectionner des clients dans l'arborescence du domaine.
 - **Plate-forme** : le nom du système d'exploitation du (des) client(s). Sélectionnez l'un des systèmes suivants :
 - Serveur Windows (NT/2000/Server 2003)
 - Poste de travail Windows (NT/2003/XP)
 - **Nom de connexion** : l'ID des utilisateurs connectés en tant que client(s). Si vous saisissez plusieurs entrées, séparez-les à l'aide d'une virgule (,).

- **État du client** : si l'application OfficeScan Client est en ligne ou hors ligne. Choisissez l'une des options suivantes :
 - **En ligne**
 - **Hors-ligne**
15. Sous **Privilèges utilisateur**, choisissez parmi les options suivantes :
 - **Autoriser l'utilisateur à modifier le niveau de sécurité** : les clients peuvent modifier le niveau de sécurité de la stratégie du Pare-feu pour clients – version d'entreprise
 - **Autoriser l'utilisateur à modifier la liste d'exceptions du trafic** : les clients peuvent modifier une liste configurable d'exceptions, de manière à permettre des types de trafic spécifiés
 16. Cliquez sur **Enregistrer**. L'écran **Liste des profils** apparaît.
 17. Cliquez sur **Déployer vers les clients** pour déployer le profil, qui inclut la stratégie associée et sa liste d'exceptions.

Vérification du déploiement

Pour vérifier que vous avez réussi à déployer le Pare-feu pour clients – version d'entreprise vers les clients sélectionnés, affichez le client dans l'arborescence des domaines OfficeScan.

Pour vérifier le déploiement :

1. Cliquez sur **Clients** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Cliquez sur le domaine auquel le client appartient.
3. Sélectionnez **Affichage du pare-feu** dans la liste **Affichage de l'arborescence client**.
4. Vérifiez qu'il y a une coche verte dans la colonne **Pare-feu** de l'arborescence client. Si vous avez activé le **Système de détection d'intrusion** pour ce client, vérifiez qu'il y a également une coche verte dans la colonne **IDS**.
5. Vérifiez que la bonne stratégie de pare-feu a été appliquée au client. La stratégie apparaît sous la colonne **Stratégie en vigueur** dans l'arborescence client.

Configuration du Pare-feu pour clients – version d'entreprise

Cette section explique comment configurer les paramètres du pare-feu après le déploiement. Pour obtenir plus d'explications détaillées sur les divers champs et sélections, consultez la rubrique *Moniteur d'activité virale du pare-feu* à la page 6-8.

Configuration des stratégies

La liste des stratégies du Pare-feu pour clients – version d'entreprise donne un résumé de toutes les stratégies. Vous pouvez gérer la liste des stratégies à partir de cet écran. Et modifier le modèle des exceptions du pare-feu pour clients – version d'entreprise.

Pour ajouter ou modifier une stratégie :

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise > Liste des stratégies**. L'écran **Liste des stratégies** apparaît.
2. Pour créer une nouvelle stratégie, cliquez sur **Ajouter**.
Pour modifier une stratégie existante, cochez la case à côté de la stratégie à modifier, puis cliquez sur **Modifier**.
3. Entrez un nom pour la stratégie.
4. Cliquez sur un **Niveau de sécurité** pour autoriser ou bloquer le trafic entrant/sortant :
 - **Élevé** : bloque tout le trafic entrant et sortant à l'exception du trafic autorisé dans la liste des exceptions.
 - **Moyen** : bloque tout le trafic entrant et autorise tout le trafic sortant, à l'exception du trafic autorisé ou bloqué dans la liste des exceptions.
 - **Faible** : autorise tout le trafic entrant et sortant à l'exception du trafic bloqué dans la liste des exceptions.
5. Cochez les cases près des fonctions du Pare-feu pour clients – version d'entreprise pour :
 - **Activer le pare-feu**
 - **Activer le système de détection d'intrusion**

- **Activer le message d'alerte** : le message d'alerte client du Pare-feu pour clients – version d'entreprise apparaît lorsque le pare-feu bloque un paquet sortant (consultez la rubrique [Modification des messages d'alerte du client](#) à la page 2-45 pour obtenir des informations sur la modification du message d'alerte du Pare-feu pour clients – version d'entreprise)

Remarque : Si vous autorisez les clients à activer ou désactiver le pare-feu, le Système de détection d'intrusion et le message d'alerte, les paramètres s'affichent sous **Paramètres locaux du pare-feu** sur la console client. Ces paramètres ne peuvent pas être modifiés à partir de la console Web OfficeScan.

Si vous n'accordez pas aux clients ce privilège, les paramètres s'affichent sous **Liste des cartes réseau** sur la console client. Ces paramètres peuvent être modifiés à partir de la console Web du serveur d'OfficeScan.

Les informations sous **Paramètres locaux du pare-feu** sur la console client reflètent toujours les paramètres configurés à partir de la console de celui-ci et non de la console Web du serveur.

6. Sous **Exception**, cochez les cases correspondant aux exceptions du Pare-feu pour clients – version d'entreprise que vous souhaitez inclure dans cette stratégie.
7. Cliquez sur **Enregistrer** pour sauvegarder la stratégie.

Configuration des exceptions

La liste des exceptions sur le pare-feu pour clients – version d'entreprise contient des entrées que vous pouvez configurer de manière à autoriser ou à bloquer divers types de trafic réseau à partir du (des) numéro(s) de port de l'ordinateur client et de (des) adresse(s) IP. Les exceptions sont appliquées aux stratégies. Lorsque vous avez créé une exception, modifiez les stratégies auxquelles elle s'applique.

Choisissez le type d'exception que vous voulez utiliser. Il existe deux types d'exceptions :

- **Restrictive** : ces exceptions bloquent uniquement les types spécifiés de trafic réseau et s'appliquent aux stratégies qui autorisent tout le trafic réseau. Un exemple d'utilisation d'une exception restrictive est le blocage des ports de clients qui sont généralement vulnérables aux attaques, tels que les ports souvent utilisés par les chevaux de Troie (consultez l'aide OfficeScan pour obtenir des informations sur les ports des chevaux de Troie).

- **Permissive** : ces exceptions autorisent uniquement les types spécifiés de trafic réseau et s'appliquent aux stratégies qui bloquent tout le trafic réseau. Par exemple, vous souhaitez autoriser des clients à accéder uniquement au serveur OfficeScan et à un serveur Web. Pour cela, autorisez le trafic depuis le port sécurisé (utilisé pour communiquer avec le serveur OfficeScan) et le port que le client utilise pour la communication HTTP.

Pour afficher le port d'écoute (sécurisé) client sur la console Web d'OfficeScan, cliquez sur **Clients > Afficher l'état > Développer tout**. Le numéro situé à côté de l'étiquette du **port** est le port d'écoute (sécurisé) client.

Pour afficher le port d'écoute (sécurisé) du serveur sur la console Web d'OfficeScan, cliquez sur **Administration > Serveur Web**. Le numéro du **champ Port** est le port d'écoute (sécurisé) du serveur ou le port Web.

Remarque : Vous pouvez modifier les exceptions dans l'Éditeur de modèle d'exception et appliquer toutes les stratégies existantes ou modifier les exceptions s'appliquant à une stratégie particulière sur l'écran Éditeur de stratégie (consultez la rubrique *Configuration des stratégies* à la page 6-13).

Pour ajouter une entrée :

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise > Liste des stratégies**. L'écran **Liste des stratégies** apparaît.
2. Cliquez sur **Modifier le modèle d'exception**. L'écran **Éditeur de modèle d'exception** s'affiche, il présente une liste des exceptions existantes.
3. Cliquez sur **Ajouter**.
4. Entrez un nom pour l'exception.
5. A côté de **Action**, cliquez sur l'une des options suivantes :
 - **Autoriser tout le trafic du réseau**
 - **Refuser tout le trafic du réseau**
6. A côté de **Direction**, cliquez sur **Entrant** ou **Sortant** pour sélectionner le type de trafic auquel les paramètres de cette exception s'appliquent.

7. Sélectionnez le type de protocole réseau dans la liste des **Protocoles** :
 - **Tous**
 - **TCP/UDP (par défaut)**
 - **TCP**
 - **UDP**
 - **ICMP**
8. Cliquez sur l'une des options suivantes pour spécifier les ports clients :
 - **Tous les ports** (par défaut)
 - **Plage** : saisissez une plage de ports
 - **Spécifique** : spécifiez des ports individuels. Utilisez une virgule (,) pour séparer les numéros de port.
9. Sous **Ordinateurs**, sélectionnez les adresses IP à inclure dans les exceptions. Par exemple, si vous sélectionnez **Refuser tout le trafic réseau (Entrant et Sortant)** et que vous saisissez l'adresse IP d'un ordinateur unique sur le réseau, chaque client dont la stratégie contient cette exception ne pourra pas envoyer ou recevoir de données vers cette adresse IP ou à partir de celle-ci.
Choisissez l'une des options suivantes :
 - **Toutes les adresses IP** (par défaut)
 - **IP unique** : saisissez le nom de l'hôte ou l'adresse IP d'un client. Pour résoudre le nom de l'hôte du client vers une adresse IP, cliquez sur **Résoudre**.
 - **Plage IP** : entrez une plage d'adresses IP
 - **Masque de sous-réseau** : entrez une adresse IP et un masque de sous-réseau
10. Cliquez sur **Enregistrer**.

Pour supprimer une entrée :

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise > Liste des stratégies**. L'écran **Liste des stratégies** apparaît.
2. Cliquez sur **Modifier le modèle d'exception**. L'écran **Éditeur de modèle d'exception** s'affiche, il présente une liste des exceptions existantes.
3. Cochez les cases qui se trouvent à côté de l'exception (des exceptions) à supprimer.
4. Cliquez sur **Supprimer**. OfficeScan supprime (les) l'exception(s) de la liste.

Saisissez l'ordre des exceptions dans la liste :

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise > Liste des stratégies**. L'écran **Liste des stratégies** apparaît.
2. Cliquez sur **Modifier le modèle d'exception**. L'écran **Éditeur de modèle d'exception** s'affiche, il présente une liste des exceptions existantes.
3. Cochez la case qui se trouve à côté de l'exception à déplacer.
4. Cliquez sur **Monter** ou **Descendre**. Le numéro ID de l'exception change pour refléter cette nouvelle position.

Pour enregistrer les paramètres de la liste des exceptions :

Cliquez sur l'une des options d'enregistrement suivantes :

- **Enregistrez en tant que modèle** : enregistrez la liste des exceptions avec les entrées actuelles. Les politiques existantes qui utilisent les exceptions que vous avez modifiées ne sont pas mises à jour, mais le modèle par contre sera automatiquement appliqué aux stratégies que vous créerez à l'avenir.
- **Enregistrez et appliquez à toutes les stratégies existantes** : enregistrez la liste des exceptions avec les entrées actuelles. Les politiques existantes qui utilisent les exceptions que vous avez modifiées sont mises à jour et le modèle est automatiquement appliqué aux stratégies que vous créerez à l'avenir.

Configuration des profils

La Liste des profils du pare-feu pour clients – version d'entreprise résume tous les profils, y compris le nom du profil, la stratégie utilisée par chaque profil et l'état actuel du profil. Vous pouvez gérer la liste des profils à partir de cet écran. Vous pouvez aussi sélectionner des profils et les déployer sur les clients OfficeScan, afin de mettre à jour les paramètres du pare-feu pour clients – version d'entreprise.

Remarque : OfficeScan applique les profils du Pare-feu pour clients – version d'entreprise aux clients, dans l'ordre de leur apparition dans la liste des profils. Par exemple, si un client correspond au premier profil, OfficeScan applique au client les actions configurées pour ce profil. Les autres profils qui sont également configurés pour ce client sont ignorés.

Conseil : Placez les stratégies les plus exclusives au sommet de la liste. Placez par exemple les stratégies que vous créez pour un client unique au sommet de la liste, puis les stratégies qui concernent une gamme de clients, un domaine réseau, puis enfin celles qui concernent tous les clients.

Pour ajouter ou modifier un profil :

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise > Liste des profils**. L'écran **Liste des profils** apparaît.
2. Pour créer un nouveau profil, cliquez sur **Ajouter**.
Pour modifier un profil existant, cochez la case à côté du profil à modifier, puis cliquez sur **Modifier**.
3. Cliquez sur **Activer ce profil** pour que le serveur OfficeScan puisse déployer ce profil vers les clients OfficeScan.
4. Saisissez un nom d'identification du profil, ainsi qu'une description facultative.
5. Dans la liste à côté de **Utiliser la stratégie suivante**, sélectionnez une stratégie existante pour ce profil.

6. Sélectionnez les clients auxquels vous souhaitez appliquer la stratégie en procédant comme suit :
 - **Adresse IP** : (les) l'adresse(s) IP du (des) client(s). Choisissez l'une des options suivantes :
 - **IP unique** : saisissez une adresse IP client valide.
 - **Plage** : saisissez une plage d'adresses IP dans les champs de texte **De** et **A**.
 - **Sous-réseau** : saisissez une adresse IP du sous-réseau et le masque de sous-réseau. OfficeScan utilise ces données pour calculer l'adresse réseau.
 - **Domaine** : le nom de domaine du (des) client(s). Cliquez sur **Afficher la console client** pour sélectionner des clients dans l'arborescence du domaine.
 - **Nom d'ordinateur** : le nom du (des) client(s). Cliquez sur **Afficher la console client** pour sélectionner des clients dans l'arborescence du domaine.
 - **Plate-forme** : le nom du système d'exploitation du (des) client(s). Sélectionnez l'un des systèmes suivants :
 - Serveur Windows (NT/2000/Server 2003)
 - Poste de travail Windows (NT/2003/XP)
 - **Nom de connexion** : l'ID des utilisateurs connectés en tant que client(s). Si vous saisissez plusieurs entrées, séparez-les à l'aide d'une virgule (,).
 - **État du client** : si l'application OfficeScan Client est en ligne ou hors ligne. Choisissez l'une des options suivantes :
 - **En ligne**
 - **Hors-ligne**
7. Sous **Privilèges utilisateur**, choisissez parmi les options suivantes :
 - **Autoriser l'utilisateur à modifier le niveau de sécurité** : les clients peuvent modifier le niveau de sécurité de la stratégie du Pare-feu pour clients – version d'entreprise
 - **Autoriser l'utilisateur à modifier la liste d'exceptions du trafic** : les clients peuvent modifier une liste configurable d'exceptions, de manière à permettre des types de trafic spécifiés
8. Cliquez sur **Enregistrer**.

Pour modifier l'ordre des profils dans la liste :

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d’entreprise > Liste des profils**. L’écran **Liste des profils** apparaît.
2. Cochez la case qui se trouve à côté du profil à déplacer.
3. Cliquez sur **Monter** ou **Descendre**.

Pour déployer des profils vers les clients

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d’entreprise > Liste des profils**. L’écran **Liste des profils** apparaît.
2. Pour écraser le niveau de sécurité actuel et la liste des exceptions du (des) client(s), cochez la case **Ecraser le niveau de sécurité/la liste des exceptions du client**.

Remarque : Si vous avez accordé aux clients le **privilège** de modifier les paramètres du pare-feu, les utilisateurs peuvent avoir modifié leur niveau de sécurité et/ou leur liste d'exceptions (consultez la rubrique Étape 7 à la page 6-19 sous **Pour ajouter ou modifier un profil :**).

En cochant la case **Ecraser le niveau de sécurité/la liste des exceptions du client**, vous pouvez vérifier que le niveau de sécurité et la liste des exceptions que vous avez configurés pour la stratégie soient appliqués à tous les clients sélectionnés.

3. Cliquez sur **Déployer vers les clients**.

Remarque : Lorsque vous cliquez sur **Déployer vers les clients**, OfficeScan déploie tous les profils de la Liste des profils vers les clients qui correspondent aux critères définis dans le(s) profil(s).

Configuration du moniteur d'activité virale du pare-feu

Un nombre excessif d'entrées dans le journal peut indiquer une épidémie virale. Active le moniteur d'activité virale du pare-feu pour clients – version d'entreprise pour qu'OfficeScan signale une alerte d'épidémies sur le pare-feu si le nombre d'entrées dans le journal excède un seuil déterminé. Active aussi et configure un message d'alerte pour qu'OfficeScan notifie automatiquement les parties concernées de l'éventuelle épidémie.

Pour activer le moniteur d'activité virale du pare-feu :

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise > Moniteur d'activité virale du pare-feu**.
2. Cochez la case **Activer le moniteur d'activité virale du pare-feu**.
3. Sous **Critères d'alerte pour le moniteur d'activité virale du pare-feu** définissez le seuil du nombre d'entrées du journal pour lequel une alerte est déclenchée pour les types de journaux suivants :
 - **Journaux IDS**
 - **Journaux du pare-feu**
 - **Journaux de virus du réseau**
4. Saisissez le nombre d'heures dans lequel OfficeScan doit détecter le nombre spécifié d'entrées dans le journal.
5. Pour activer et configurer un message d'alerte facultatif, procédez de la manière suivante :
 - a. Cochez la case **Envoyer une notification par e-mail si les critères d'alerte sont remplis**.
 - b. Sous **Paramètres du message d'alerte**, saisissez les données suivantes :
 - **SMTP** : le nom de l'hôte ou l'adresse IP du serveur de messagerie Simple Mail Transfer Protocol (SMTP)
 - **Numéro de port** : numéro de port du serveur SMTP (par défaut 25)
 - **À** : adresses électroniques des destinataires. Séparer les adresses par un point-virgule « ; ».
 - **De** : le nom ou l'adresse de messagerie de l'expéditeur (par défaut il s'agit de « OfficeScan »)

- **Objet** : saisissez un objet (par défaut « Alerte issue par le moniteur de l'activité du pare-feu »)
- **Message** : saisissez un message (le message par défaut inclut les alertes déclenchées et le nombre total d'entrées dans le journal dans le nombre d'heures spécifiés précédemment)

6. Cliquez sur **Enregistrer**.

Test du pare-feu

Afin de garantir que le déploiement de votre pare-feu pour clients – version d'entreprise se passe correctement, effectuez un test sur un client ou un groupe de clients.

AVERTISSEMENT ! Testez les paramètres du client OfficeScan dans un environnement sous contrôle uniquement. N'effectuez aucun test sur des ordinateurs clients connectés à votre réseau ou à Internet. Vous risquez d'exposer ceux-ci à des virus, des attaques de pirates ou autres.

Pour tester le pare-feu pour clients – version d'entreprise :

1. Créez et enregistrez une stratégie de test (consultez la rubrique [Configuration des stratégies](#) à la page 6-13 pour obtenir des instructions). Configurez les paramètres pour bloquer les types de trafic que vous souhaitez tester. Par exemple, pour empêcher le client d'accéder à Internet uniquement, procédez comme suit :
 - a. Cliquez sur **Tout le trafic faible entrant/sortant est autorisé** pour le **niveau de sécurité par défaut**.
 - b. Sélectionnez **Activer le pare-feu** et **Activer le message d'alerte** sous **Paramètres du pare-feu client**.
 - c. Créez une exception bloquant le trafic HTTP (ou HTTPS).
2. Créez et enregistrez un profil de test sélectionnant les clients dont vous souhaitez tester le pare-feu. Associez la stratégie de test au profil de test (consultez la rubrique [Configuration des profils](#) à la page 6-18 pour obtenir des instructions).
3. Cliquez sur **Déployer vers les clients** pour déployer la stratégie de test.

4. Contrôlez le déploiement (consultez la rubrique *Moniteur d'activité virale du pare-feu* à la page 6-8 pour obtenir des instructions)
5. Testez le pare-feu sur l'ordinateur client en essayant d'envoyer ou de recevoir le type de trafic que vous avez configuré dans la stratégie.
Pour tester une stratégie configurée pour empêcher le client d'accéder à Internet, ouvrez un navigateur Web sur l'ordinateur client. Si vous avez activé le message d'alerte pour le pare-feu, il s'affiche sur la machine client (consultez la rubrique *Modification des messages d'alerte du client* à la page 2-45).

Désactivation du pare-feu

Pour désactiver le Pare-feu pour clients – version d'entreprise sur les postes clients à partir de la console Web OfficeScan, créez une nouvelle stratégie qui n'active pas le pare-feu et appliquez la stratégie aux clients.

Pour désactiver le pare-feu avec une nouvelle stratégie :

1. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise** > **Liste des stratégies**. L'écran **Liste des stratégies** apparaît.
2. Pour créer une nouvelle stratégie, cliquez sur **Ajouter**.
3. Entrez un nom pour la stratégie.
4. Décochez la case **Activer le pare-feu**.
5. Cliquez sur **Enregistrer** pour sauvegarder la stratégie.
6. Dans la barre latérale, cliquez sur **Pare-feu pour clients – version d'entreprise** > **Liste des profils**. L'écran **Liste des profils** apparaît.
7. Pour créer un nouveau profil, cliquez sur **Ajouter**.
8. Cliquez sur **Activer ce profil** pour que le serveur OfficeScan puisse déployer ce profil vers les clients OfficeScan.
9. Saisissez un nom d'identification du profil, ainsi qu'une description facultative.
10. Dans la liste à côté de **Utiliser la stratégie suivante**, sélectionnez la stratégie que vous avez créée.
11. Sélectionnez les clients pour lesquels vous voulez désactiver le pare-feu.
12. Cliquez sur **Enregistrer**.
13. Cliquez sur **Déployer vers les clients** pour déployer le profil, ce qui désactive le pare-feu.

Vous pouvez également désactiver le pare-feu pour tous les clients en le désinstallant dans l'écran **Licence du produit**.

Pour désactiver le pare-feu :

1. Dans la barre latérale, cliquez sur **Administration > Licence produit**. L'écran **Licence produit** s'affiche.
2. Décochez la case **Installer le pare-feu pour clients – version d'entreprise** sous Informations licence.
3. Cliquez sur **Appliquer**.

Affichage et interprétation des journaux

Ce chapitre décrit comment utiliser les journaux OfficeScan pour surveiller votre système et analyser la protection de votre réseau.

Les rubriques présentées dans ce chapitre incluent :

- *Affichage et interprétation des journaux* à la page 7-2
- *Affichage des journaux de virus* à la page 7-2
- *Suppression des journaux de virus* à la page 7-4
- *Affichage des journaux de mise à jour du serveur* à la page 7-5
- *Affichage des journaux de mise à jour du client* à la page 7-5
- *Affichage des journaux des événements du système* à la page 7-6
- *Affichage des journaux de vérification de la connexion* à la page 7-7
- *Affichage des journaux du pare-feu pour clients – version d'entreprise* à la page 7-8

Affichage et interprétation des journaux

OfficeScan met à votre disposition des journaux complets concernant les incidents viraux, les événements et les mises à jour. Vous pouvez utiliser ces journaux pour évaluer l'efficacité des stratégies antivirus de votre entreprise et pour identifier les clients présentant le plus fort risque d'infection. Vous pouvez également utiliser les journaux pour vérifier la connexion client-serveur et pour vous assurer que les mises à jour ont été déployées avec succès.

Remarque : Utilisez un tableur tel que Microsoft Excel pour ouvrir les fichiers journaux CSV.

OfficeScan maintient les journaux suivants :

- Journaux de virus
- Journaux de mise à jour du serveur
- Journaux de mise à jour du client
- Journaux des événements du système
- Journaux de vérification de la connexion
- Journaux de pare-feu des clients de l'entreprise

Affichage des journaux de virus

OfficeScan enregistre les entrées de journaux pour les virus détectés sur vos clients. Les journaux de virus comprennent les informations suivantes :

- **Date et Heure :** l'heure à laquelle OfficeScan a créé l'entrée de journal
- **Nom de l'ordinateur :** le nom du client OfficeScan
- **Nom du virus :** le(s) virus détecté(s) par OfficeScan
- **Source de l'infection :** le client à l'origine du virus
- **Fichier infecté :** le(s) fichier(s) infecté(s) par le(s) virus
- **Type de scan :** le type de scan effectué par OfficeScan lorsqu'il détecte le virus (Manuel, Temps réel, Programmé)
- **Résultat du scan :** l'action effectuée par OfficeScan après le scan

Pour afficher les journaux de virus :

1. Dans la barre latérale, cliquez sur **Journaux > Journaux de virus**. L'écran **Clients** apparaît.
2. Cliquez sur les icônes des clients ou des domaines dans l'arborescence pour afficher les journaux de virus correspondants. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Clients OfficeScan** dans la barre latérale. L'écran **Afficher les journaux de virus** apparaît.
4. Cliquez sur **Sélectionner une période** dans **Heure** et faites votre choix dans la liste ou cliquez sur **Spécifier une plage** et entrez une plage de dates.
5. Sous **Types de scan**, sélectionnez les types de journaux à afficher en cochant les cases correspondantes.
6. Sous **Classer par**, cliquez sur une option pour indiquer comment classer les journaux. Les options sont :
 - Date et Heure
 - Nom de l'ordinateur
 - Nom du virus
 - Type de scan
 - Résultat du scan
7. Pour afficher les journaux, cliquez sur **Afficher journaux**.
8. Pour sauvegarder le journal en tant que fichier CSV (séparateur : point-virgule), cliquez sur **Exporter vers fichier CSV**. Utilisez un tableur pour afficher les fichiers de données CSV.

Suppression des journaux de virus

Pour libérer de l'espace disque sur le serveur, supprimez les journaux de virus manuellement.

Pour supprimer les journaux de virus :

1. Dans la barre latérale, cliquez sur **Journaux > Journaux de virus**. L'écran **Clients** apparaît.
2. Cliquez sur les icônes des clients ou des domaines dans l'arborescence pour afficher les journaux de virus correspondants. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine.
3. Cliquez sur **Suppression de journaux** dans la barre latérale. L'écran **Supprimer des journaux** apparaît.
4. Sous **Sélectionner des types de journaux**, choisissez les types de journaux à supprimer (types définis selon la nature du scan réalisé par OfficeScan).
5. Sous **Suppression**, indiquez les journaux à supprimer. Les options sont :
 - **Supprimer tout le contenu des types de journaux sélectionnés**
 - **Supprimer tous les journaux antérieurs à { } jours**

Si vous cliquez sur **Supprimer les journaux antérieurs à { } jours**, saisissez une valeur pour le nombre de jours. Si, par exemple, vous entrez la valeur 20, OfficeScan supprimera tous les journaux créés il y a 20 jours et plus.
6. Cliquez sur **Appliquer** pour supprimer les journaux.

Affichage des journaux de mise à jour du serveur

OfficeScan tient des journaux des mises à jour du serveur. Ceci vous permet de garder un suivi de l'historique des mises à jour du serveur et des méthodes utilisées.

Pour afficher les journaux de mise à jour du serveur :

1. Cliquez sur **Journaux > Journaux de mise à jour > Mise à jour du serveur** dans la barre latérale. L'écran **Journaux de mise à jour du serveur** apparaît, contenant les informations suivantes :
 - l'heure et la date de la mise à jour
 - le résultat de la mise à jour
 - les composants de mise à jour
 - la méthode de mise à jour
2. Pour sauvegarder le journal en tant que fichier CSV (séparateur : point-virgule), cliquez sur **Exporter vers fichier CSV**. Utilisez un tableur pour afficher les fichiers de données CSV.

Affichage des journaux de mise à jour du client

OfficeScan fournit également des journaux de mise à jour du client. Utilisez ces journaux pour vérifier le déploiement des mises à jour.

Pour afficher les journaux de mise à jour du client :

1. Cliquez sur **Journaux > Journaux de mise à jour > Mise à jour du client** dans la barre latérale. L'écran **Journaux de mise à jour du client** apparaît, contenant les informations suivantes :
 - la date et l'heure de la mise à jour
 - Mettre à jour les composants
 - En cours
 - Détails
2. Sélectionnez le nombre de résultats que vous voulez afficher par page dans la liste des **Résultats affichés par page**.
3. Cliquez sur les en-têtes de colonnes **Heure/Date** ou **Composants de mise à jour** pour classer le tableau.

Pour afficher le nombre de clients mis à jour dans un déploiement de mise à jour donné :

1. Cliquez sur **Afficher** dans la colonne **Progression**. L'écran **Progression de la mise à jour du client** apparaît.
2. Sont affichés dans cet écran le nombre de clients mis à jour par intervalles de 15 minutes, ainsi que le nombre total de clients mis à jour.

Pour afficher les clients qui ont été mis à jour dans un déploiement de mise à jour donné :

1. Cliquez sur **Afficher** dans la colonne **Détails**. L'écran **Détails de la mise à jour du client** apparaît, indiquant les noms des clients mis à jour par OfficeScan et les détails de leur mise à jour.
2. Vous pouvez classer le tableau en cliquant sur les en-têtes des colonnes : **Nom de l'ordinateur**, **Notification envoyée**, **Notification reçue**, **Mise à jour terminée** ou **Source de mise à jour**.
3. Pour sauvegarder le journal en tant que fichier CSV (séparateur : point-virgule), cliquez sur **Exporter vers fichier CSV**. Utilisez un tableur pour afficher les fichiers de données CSV.

Affichage des journaux des événements du système

OfficeScan enregistre également les événements liés au programme serveur, tels que les arrêts et les démarrages. Utilisez ces journaux pour vérifier si le serveur fonctionne sans problème et si les services permettant à OfficeScan de fonctionner en réseau s'exécutent correctement.

Pour afficher les journaux des événements du système :

1. Cliquez sur **Journaux > Journaux des événements du système** dans la barre latérale. L'écran **Journaux des événements du système** apparaît et affiche les récents événements sur le serveur.
2. Sélectionnez le nombre de résultats que vous voulez afficher par page dans la liste des **Résultats affichés par page**.
3. Vous pouvez classer le tableau en cliquant sur les en-têtes des colonnes : **Heure/Date** ou **Nom de l'ordinateur** ou **Description de l'événement**.
4. Pour sauvegarder le journal en tant que fichier CSV (séparateur : point-virgule), cliquez sur **Exporter vers fichier CSV**. Utilisez un tableur pour afficher les fichiers de données CSV.

Affichage des journaux de vérification de la connexion

OfficeScan tient des journaux de vérification de la connexion pour vous permettre de déterminer l'état de connexion entre le serveur et les clients.


Pour afficher les journaux de vérification de la connexion :

1. Cliquez sur **Journaux > Journaux de vérification de la connexion** dans la barre latérale. L'écran **Journaux de vérification de la connexion** apparaît, indiquant les date et heure du journal, les noms des ordinateurs des clients, les domaines, les adresses IP et l'état de connexion.
2. Sélectionnez le nombre de résultats que vous voulez afficher par page dans la liste des **Résultats affichés par page**.
3. Vous pouvez classer le tableau en cliquant sur les en-têtes des colonnes : **Heure/Date, Nom de l'ordinateur, Domaine, Adresse IP** ou **État**.
4. Pour sauvegarder le journal en tant que fichier CSV (séparateur : point-virgule), cliquez sur Exporter vers fichier CSV. Un écran de confirmation apparaît.
 - Cliquez sur Ouvrir pour afficher le fichier dans votre tableur, sans l'enregistrer.
 - Cliquez sur **Enregistrer**, puis définissez le dossier dans lequel doit être déposé le fichier CSV.
5. Cliquez sur **Enregistrer**.

Affichage des journaux du pare-feu pour clients – version d'entreprise

Les clients OfficeScan, dont le pare-feu pour clients – version d'entreprise est activé, stockent les événements du pare-feu dans un journal sur l'ordinateur du client. Affichez ces journaux pour analyser la manière dont le pare-feu pour clients – version d'entreprise protège vos clients des attaques. Pour afficher les derniers journaux du pare-feu pour clients – version d'entreprise, vous devez d'abord indiquer aux clients d'envoyer leurs journaux sur le serveur OfficeScan.

Pour notifier aux clients d'envoyer les journaux du pare-feu pour clients – version d'entreprise sur le serveur OfficeScan :

1. Cliquez sur **Journaux** > **Journaux de pare-feu** dans la barre latérale. L'arborescence des domaines pour l'écran **Clients** apparaît.
2. Sélectionnez les domaines ou les clients auxquels envoyer des journaux de pare-feu pour clients – version d'entreprise en cliquant sur leurs icônes respectives dans l'arborescence du domaine. Pour sélectionner tous les domaines et les clients, cliquez sur l'icône racine . Vous pouvez rechercher des clients en appliquant des critères de sélection tels que le nom de l'ordinateur, l'adresse IP ou la version du fichier de signatures ; vous pouvez également changer l'affichage de l'arborescence client.
3. Cliquez sur **Notification client** dans la barre latérale. L'écran **Notification client pour journaux de pare-feu** apparaît.
4. Cliquez ensuite sur **Notifier**.

Pour afficher des journaux de pare-feu pour clients – version d'entreprise :

1. Cliquez sur **Journaux** > **Journaux de pare-feu** > **Afficher les journaux** dans la barre latérale. L'écran **Journaux de pare-feu pour clients – version d'entreprise** apparaît, contenant les informations suivantes :
 - l'heure et la date de l'entrée dans le journal
 - L'ordinateur qui a mis l'entrée dans le journal
 - L'hôte distant
 - l'hôte local
 - Le protocole
 - Une description de l'entrée dans le journal
 - Le port de destination
 - Détails de l'entrée dans le journal

2. Sélectionnez le nombre de résultats que vous voulez afficher par page dans la liste des **Résultats affichés par page**.
3. Vous pouvez classer le tableau en cliquant sur les en-têtes des colonnes.
4. Pour sauvegarder le journal en tant que fichier CSV (séparateur : point-virgule), cliquez sur Exporter vers fichier CSV. Un écran de confirmation apparaît.
 - Cliquez sur **Ouvrir** pour afficher le fichier dans votre tableur, sans l'enregistrer.
 - Cliquez sur **Enregistrer**, puis définissez le dossier dans lequel doit être déposé le fichier CSV.

Gestion des journaux

Gérez les journaux en effectuant une maintenance programmée des journaux pour éviter que leur taille n'occupe trop d'espace sur votre disque dur. Vous pouvez configurer OfficeScan pour une suppression programmée automatique des journaux.

Pour exécuter la maintenance programmée des journaux :

1. Dans la barre latérale, cliquez sur **Journaux > Maintenance des journaux**. L'écran **Maintenance des journaux** apparaît.
2. Cochez la case **Activer la suppression programmée des journaux** pour activer la fonction de maintenance planifiée.
3. Dans **Type(s) de journaux à supprimer**, sélectionnez les types de journaux à supprimer automatiquement.
4. Dans **Critères de suppression des entrées de journaux**, indiquez les journaux à supprimer. Les options sont :
 - **Supprimer tout le contenu des types de journaux sélectionnés**
 - **Supprimer tous les journaux antérieurs à { } jours**

Si vous cliquez sur **Supprimer tous les journaux antérieurs à { } jours**, saisissez ensuite la valeur désirée dans la zone de texte.
5. Sous **Planification**, indiquez la fréquence à laquelle s'exécutera la maintenance programmée des journaux :
 - **Quotidien**
 - **Hebdomadaire, tous les { }**
 - **Mensuel, le { }**

Si vous cliquez sur **Hebdomadaire**, sélectionnez ensuite un jour de la semaine dans la liste proposée.

Si vous cliquez sur **Mensuelle**, sélectionnez ensuite une date dans la liste proposée.

Quelle que soit la fréquence choisie, utilisez le champ **Heure de début** pour indiquer l'heure à laquelle doit démarrer la maintenance programmée.

6. Cliquez sur **Enregistrer** pour sauvegarder vos paramètres.

Utilisation des outils administrateurs et clients

OfficeScan comprend un ensemble d'outils permettant d'accomplir différentes tâches OfficeScan, parmi lesquelles la configuration du serveur et la gestion des clients.

Ces outils sont classés en deux catégories :

- **Outils administrateurs** : conçus pour vous aider à configurer le serveur et à gérer les clients (consultez la rubrique *Outils administrateurs* à la page 8-3)
- **Outils clients** : conçus pour améliorer les performances du programme client (consultez la rubrique *Outils clients* à la page 8-10)

Plusieurs outils des versions antérieures d'OfficeScan ont été intégrés à cette version (consultez la rubrique *Outils intégrés* à la page 8-19).

Résumé des outils

Reportez-vous au Tableau 8-1 pour connaître la liste complète des outils inclus dans cette version OfficeScan

Remarque : Certains outils disponibles dans les versions précédentes d'OfficeScan ne sont pas disponibles dans cette version. Si vous devez utiliser ces outils, contactez le support technique. Consultez la rubrique *Outils intégrés* à la page 8-19 pour connaître la liste des outils dont les fonctions sont intégrées à cette version OfficeScan.

Outils administrateurs	Outils clients
Configuration du script de connexion : automatise l'installation des clients OfficeScan (consultez la rubrique page 8-3)	Client Packager : crée un fichier auto-extractible contenant le programme client OfficeScan client et ses composants (consultez la rubrique page 8-10)
Vulnerability Scanner (Scanner de failles) : recherche les ordinateurs non protégés sur votre réseau (consultez la rubrique page 8-3)	Utilitaire de création d'image : permet de créer l'image d'un client OfficeScan et de la reproduire (consultez la rubrique page 8-10)
Server Tuner : optimise les performances du serveur OfficeScan (consultez la rubrique page 8-9)	Décodeur de fichiers : ouvre les fichiers infectés codés par OfficeScan (consultez la rubrique page 8-11)
	Client Mover I : transfère des clients d'un serveur OfficeScan vers un autre (consultez la rubrique page 8-13)
	Outil Touch : modifie la marque horaire sur un correctif (hot fix) pour le redéployer automatiquement (consultez la rubrique page 8-15)
	Outil de migration pour ServerProtect Normal Server : Migration d'ordinateurs exécutant ServerProtect Normal Server vers le client OfficeScan (consultez la rubrique page 8-16)

TABLEAU 8-1 Outils OfficeScan

Remarque : Ces outils ne peuvent pas s'exécuter à partir de la console Web OfficeScan. Pour obtenir des instructions sur le fonctionnement de ces outils, consultez les sections correspondantes ci-dessous.

Outils administrateurs

Cette section contient des informations sur les outils administrateurs OfficeScan suivants :

Configuration du script de connexion

L'outil Configuration du script de connexion permet d'automatiser l'installation du client OfficeScan sur les ordinateurs non protégés lorsque ceux-ci se connectent au réseau. L'outil ajoute un programme appelé `autopcc.exe` au script de connexion du serveur. Le programme `autopcc.exe` exécute les fonctions suivantes :

- Il détecte le système d'exploitation de l'ordinateur non protégé et installe la version appropriée du client OfficeScan
- Il met à jour le fichier de signatures des virus et les fichiers du programme

Pour obtenir des instructions sur l'installation des clients, consultez le *Guide de déploiement et d'installation* et l'aide en ligne du serveur OfficeScan.

Vulnerability Scanner

Vulnerability Scanner sert à détecter les solutions antivirus installées et recherche les ordinateurs non protégés sur votre réseau. Pour déterminer si les ordinateurs sont protégés, Vulnerability Scanner envoie une requête ping aux ports normalement utilisés par les solutions antivirus.

Vulnerability Scanner peut effectuer les actions suivantes :

- Exécuter un scan DHCP pour surveiller le réseau pour y trouver des demandes DHCP, de sorte que lorsque les ordinateurs sont connectés pour la première fois au réseau, Vulnerability Scan puisse déterminer leur état
- Envoyer une requête ping aux ordinateurs de votre réseau pour vérifier leur état et récupérer leurs noms d'ordinateur, versions de plate-forme et descriptions
- Déterminer si des solutions antivirus sont installées sur le réseau. Il peut détecter les produits Trend Micro (y compris OfficeScan, ServerProtect pour Windows NT et Linux, ScanMail pour Microsoft Exchange, InterScan Messaging Security Suite et PortalProtect) et les solutions antivirus tierces (y compris Norton AntiVirus ainsi que Corporate Edition v7.5 et v7.6 et McAfee VirusScan ePolicy Orchestrator).

- Afficher le nom du serveur et la version du fichier de signatures, du moteur de scan et du programme pour OfficeScan et ServerProtect pour Windows NT
- Envoyer les résultats de scan par courrier électronique
- S'exécuter en mode silencieux (mode d'invite de commande)
- Installer à distance le client OfficeScan sur les ordinateurs équipés de Windows NT/2000/XP (Professionnel uniquement)/Server 2003

Vous pouvez également automatiser Vulnerability Scanner en créant des tâches programmées. Pour obtenir des informations sur l'automatisation de Vulnerability Scanner, consultez l'aide en ligne TMVS.

Pour exécuter Vulnerability Scanner sur un ordinateur différent du serveur, copiez le dossier TMVS contenu dans le dossier \PCCSRV\Admin\Utility du serveur sur l'ordinateur souhaité.

Remarque : Vous pouvez utiliser Vulnerability Scanner sur les ordinateurs équipés de Windows 2000 et Server 2003, mais ces derniers ne peuvent pas exécuter Terminal Server.

Vous ne pouvez pas installer de clients OfficeScan avec Vulnerability Scanner si une installation serveur OfficeScan est présente sur le même ordinateur.

L'outil Vulnerability Scanner n'installe pas les clients OfficeScan sur un ordinateur exploitant déjà le serveur OfficeScan.

Pour exécuter Vulnerability Scanner sur un ordinateur différent du serveur, copiez le dossier TMVS contenu dans le dossier \PCCSRV\Admin\Utility du serveur sur l'ordinateur souhaité.

Pour configurer Vulnerability Scanner :

1. Ouvrez les répertoires suivants sur le lecteur d'installation du serveur OfficeScan : **OfficeScan > PCCSRV > Admin > Utility > TMVS**. Double-cliquez sur **TMVS.exe**. La console Vulnerability Scanner apparaît.
2. Cliquez sur **Paramètres**. L'écran **Paramètres** apparaît.

3. Sélectionnez les produits à rechercher sur le réseau dans la zone **Recherche Produits**. Sélectionnez la **recherche de tous les produits Trend Micro** pour sélectionner tous les produits.
Si Trend Micro InterScan et Norton AntiVirus Corporate Edition sont installés sur votre réseau, cliquez sur **Settings** à côté du nom du produit pour vérifier le numéro de port à contrôler par Vulnerability Scanner.
4. Cliquez sur la méthode de récupération de votre choix sous **Description Retrieval Settings**. L'option « Récupération normale » est plus précise, mais dure plus longtemps.
Si vous cliquez sur **Normal retrieval**, vous pouvez cocher la case **Retrieve computer description when available** afin de paramétrer Vulnerability Scanner de sorte qu'il tente de récupérer les descriptions des ordinateurs, si elles sont disponibles.
5. Pour envoyer automatiquement les résultats sur votre poste ou sur les postes des administrateurs, sous **Alert Settings** cochez la case **Email results to the system administrator**, puis cliquez sur **Configure** pour spécifier vos paramètres de courrier électronique.
 - Saisissez l'adresse électronique du destinataire dans **A**.
 - Saisissez votre adresse électronique dans **De**. Ainsi, le destinataire saura qui lui a envoyé le message, si vous ne l'envoyez pas uniquement sur votre poste.
 - Saisissez l'adresse de votre serveur SMTP dans le champ **SMTP server**. Saisissez, par exemple, smtp.société.com. Les informations relatives au serveur SMTP sont requises.
 - Sous **Objet**, entrez un nouvel objet pour le message ou acceptez l'objet par défaut.
 Cliquez sur **OK** pour enregistrer vos paramètres.
6. Pour afficher une alerte sur les ordinateurs non protégés, cochez la case **Display alert on unprotected computers**. Cliquez ensuite sur **Personnaliser** pour définir le message d'alerte. L'écran **Message d'alerte** apparaît. Vous pouvez saisir le nouveau message d'alerte ou acceptez le message par défaut. Cliquez sur **OK**.
7. Pour enregistrer les résultats dans un fichier de données au format CSV, cochez la case **Automatically save the results to a CSV file**. Les fichiers de données CSV sont enregistrés par défaut dans le dossier TMVS. Si vous voulez modifier le dossier CSV par défaut, cliquez sur **Parcourir**. L'écran **Parcourir le dossier** apparaît. Recherchez le dossier cible sur votre ordinateur ou sur le réseau, puis cliquez sur **OK**.

8. Vous pouvez autoriser Vulnerability Scanner à envoyer une requête ping aux ordinateurs en réseau afin d'obtenir leur état. Sous **Paramètres de ping**, spécifiez la méthode appliquée par Vulnerability Scanner pour l'envoi de paquets vers les ordinateurs et attendez les réponses. Acceptez les paramètres par défaut ou entrez les nouvelles valeurs dans les champs **Taille des paquets** et **Expiration**.
9. Pour installer à distance un client OfficeScan et envoyer un journal au serveur, entrez le nom et le numéro de port du serveur OfficeScan. Si vous voulez automatiquement installer à distance le client OfficeScan, cochez la case **Installation automatique du client OfficeScan sur les ordinateurs non protégés**.
10. Cliquez sur **Installer Compte** pour configurer le compte. L'écran **Informations sur le compte** apparaît. Entrez le nom d'utilisateur et le mot de passe permettant l'installation. Cliquez sur **OK**.
11. Si vous voulez envoyer le journal au serveur, cochez la case **Envoyer journal au serveur OfficeScan**.
12. Cliquez sur **OK** pour enregistrer vos paramètres. La console **Vulnerability Scanner de Trend Micro** apparaît.

Pour exécuter un scan de faille sur une plage d'adresses IP :

1. Dans **Plage IP à vérifier**, entrez la plage d'adresses IP pour laquelle vous voulez vérifier les solutions antivirus installées et rechercher les ordinateurs non protégés. Notez que le Vulnerability Scanner prend uniquement en charge les adresses IP de classe B.
2. Cliquez sur **Démarrer** pour commencer la vérification des ordinateurs de votre réseau. Les résultats s'affichent dans le tableau **Résultats**.

Pour exécuter Vulnerability Scanner sur des ordinateurs qui demandent des adresses IP à partir d'un serveur DHCP :

1. Cliquez sur l'onglet **Scan DHCP** dans la case **Résultats**. L'icône **Démarrer DHCP** apparaît.
2. Cliquez sur **Démarrer DHCP**. Vulnerability scanner commence à écouter les demandes DHCP puis exécute des contrôles de faille sur les ordinateurs lorsqu'ils sont connectés au réseau.

Pour créer des tâches programmées

1. Cliquez sur **Ajouter/Modifier** sous **Tâches programmées**. L'écran **Tâches programmées** apparaît.
2. Saisissez un nom pour la tâche que vous créez sous **Nom de la tâche**.
3. Dans **Plage adresses IP**, entrez la plage d'adresses IP pour laquelle vous voulez vérifier les solutions antivirus installées et rechercher les ordinateurs non protégés.
4. Cliquez sur la fréquence de la tâche que vous créez sous **Programmation Tâche**. Vous pouvez définir la tâche pour une exécution **Quotidienne**, **Hebdomadaire** ou **Mensuelle**. Si vous cliquez sur **Hebdomadaire**, vous devez sélectionner un jour dans la liste. Si vous cliquez sur **Mensuelle**, sélectionnez ensuite une date dans la liste.
5. Entrez ou sélectionnez l'heure d'exécution de la tâche dans la liste **Start time**. Utilisez le format 24 heures.
6. Dans **Settings**, cliquez sur **Use current settings** pour utiliser les paramètres existants ou cliquez sur **Modify settings**.
Si vous cliquez sur **Modify settings**, cliquez sur **Settings** pour modifier la configuration. Pour obtenir des informations sur la configuration de vos paramètres, reportez-vous aux étapes 4 et 5 de la procédure « Pour configurer Vulnerability Scanner : ».
7. Cliquez sur **OK** pour enregistrer vos paramètres. La tâche que vous avez créée apparaît dans **Scheduled Tasks**.

Autres paramètres

Pour configurer les paramètres suivants, vous devez modifier `TMVS.ini` :

- **Debug** : activer ou désactiver le journal de débogage
- **EchoNum** : définir le nombre d'ordinateurs auquel Vulnerability Scanner envoie simultanément une requête ping
- **ThreadNumManual** : définir le nombre d'ordinateurs que Vulnerability Scanner vérifie simultanément à la recherche d'un logiciel antivirus
- **ThreadNumSchedule** : définir le nombre d'ordinateurs que Vulnerability Scanner vérifie simultanément à la recherche d'un logiciel antivirus lors de l'exécution d'une tâche programmée

Pour modifier ces paramètres :

1. Ouvrez le dossier TMVS et localisez le fichier `TMVS.ini`.
2. Ouvrez le fichier `TMVS.ini` à l'aide du Bloc-notes ou de tout autre éditeur de texte.
3. Pour activer le journal de débogage, remplacez la valeur `Debug=0` par `Debug=1`.
4. Pour définir le nombre d'ordinateurs auquel Vulnerability Scanner envoie simultanément une requête ping, modifiez la valeur `EchoNum`. Indiquez une valeur comprise entre 1 et 64.

Saisissez par exemple `EchoNum=60` pour que Vulnerability Scanner envoie une requête ping à 60 ordinateurs en même temps.

5. Pour définir le nombre d'ordinateurs que Vulnerability Scanner vérifie simultanément à la recherche d'un logiciel antivirus, modifiez la valeur `ThreadNumManual`. Indiquez une valeur comprise entre 8 et 64.

Par exemple, saisissez `ThreadNumManual=60` pour rechercher un logiciel antivirus simultanément sur 60 ordinateurs.

6. Pour définir le nombre d'ordinateurs simultanément vérifiés par Vulnerability Scanner pour la recherche de logiciel antivirus, lors de l'exécution de tâches programmées, modifiez la valeur `ThreadNumSchedule`. Indiquez une valeur comprise entre 8 et 64.

Par exemple, saisissez `ThreadNumSchedule=60` pour rechercher simultanément le logiciel antivirus sur 60 ordinateurs chaque fois que Vulnerability Scanner exécute une tâche programmée.

7. Enregistrez le fichier `TMVS.ini`.

Server Tuner

Utilisez Server Tuner pour améliorer les performances de votre serveur.

Remarque : Vous ne pouvez utiliser cet outils qu'avec les versions OfficeScan 3.54 et supérieures.

Serveur Tuner utilise le fichier suivant :

- Fichier principal : `SvrTune.exe`

Pour utiliser Server Tuner :

1. Sur le serveur, ouvrez l'Explorateur de Windows et allez dans le dossier \PCCSRV\Admin\Utility\SvrTune d'OfficeScan.
2. Double-cliquez sur le fichier `SvrTune.exe` pour démarrer Server Tuner. La console **Server Tuner** s'ouvre.
3. Sous **Download**, modifiez les paramètres suivants selon le trafic de votre réseau :
 - **Délai**
 - **Délai pour la mise à jour**
 - **Réessayer le décompte**
 - **Réessayer l'intervalle**
4. Sous **Mémoire tampon**, modifiez les paramètres suivants selon le trafic de votre réseau :
 - **Mémoire tampon des événements** : utilisée pour rapporter l'état des clients
 - **Mémoire tampon journal** : utilisée pour rapporter les virus détectés
5. Sous **Contrôle du trafic réseau**, modifiez les paramètres suivants selon le trafic de votre réseau :
 - **Heures normales**
 - **Heures creuses**
 - **Heures de pointe**

Remarque : Si le nombre de clients qui communiquent avec votre serveur est important, vous pouvez augmenter la taille de la mémoire tampon. Une mémoire tampon de grande taille signifie toutefois une plus grande utilisation de la mémoire du serveur.

Outils clients

Cette section contient des informations sur les outils clients OfficeScan suivants :

Client Packager

Client Packager est un outil qui compresse les fichiers d'installation et de mise à jour dans un fichier auto-extractible afin de simplifier la distribution par e-mail, CD-ROM ou support similaire. Il inclut également une fonction de courrier électronique qui peut accéder au carnet d'adresses Microsoft Outlook et qui vous permet ainsi d'envoyer le fichier à extraction automatique depuis la console de l'outil.

Pour exécuter Client Packager, double-cliquez sur le fichier. Les clients OfficeScan installés à l'aide de Client Packager communiquent avec le serveur sur lequel a été créée la compression d'installation.

Pour obtenir des instructions sur l'utilisation de Client Packager, consultez le *Guide de déploiement et d'installation* et l'aide en ligne du serveur OfficeScan.

Utilitaire de création d'image

La technologie des images disques permet de créer l'image d'un client OfficeScan et de la cloner sur les autres ordinateurs du réseau.

Chaque installation client requiert un identificateur global unique (GUID), si bien que le serveur peut identifier vos clients individuellement. Utilisez le programme OfficeScan appelé `imgsetup.exe` pour créer un GUID différent pour chaque clone.

L'utilitaire de création d'image vous permet d'utiliser la technologie des images disques pour déployer le programme client OfficeScan.

Pour obtenir des instructions sur l'utilitaire de création d'image, consultez le *Guide de déploiement et d'installation* et l'aide en ligne du serveur OfficeScan.

Décodeur de fichiers

Chaque fois qu'OfficeScan détecte un fichier infecté, il encode ce fichier et le dépose dans le dossier Suspect du client, qui se trouve généralement à l'emplacement C:\Programmes\Trend Micro\OfficeScan Client\SUSPECT. Le fichier infecté est encodé pour empêcher les utilisateurs de l'ouvrir et de diffuser le virus dans d'autres fichiers de l'ordinateur.

Dans certaines situations, vous pouvez être amené à devoir ouvrir le fichier que vous savez être infecté. Par exemple, un document important a été infecté et vous devez extraire les informations du document ; vous devez décoder le fichier infecté pour extraire vos informations.

Vous pouvez utiliser le Décodeur de fichiers infectés pour décoder les fichiers infectés que vous voulez ouvrir.

Remarque : Pour éviter qu'OfficeScan ne détecte à nouveau le virus lorsque vous utilisez le Décodeur de fichiers infectés, excluez le dossier vers lequel vous décidez le fichier à partir du Scan en temps réel.

AVERTISSEMENT ! Lorsque vous décidez un fichier infecté, le virus qu'il contient peut se propager vers d'autres fichiers.

Le Décodeur de fichiers infectés requiert les fichiers suivants :

- Fichier principal : VSEncode.exe
- Fichier DLL requis : Vsapi32.dll

Pour décodés les fichiers stockés dans le dossier Suspect :

1. Sur le client où vous voulez décoder un fichier infecté, ouvrez Windows Explorer et accédez au dossier \PCCSRV\Admin\Utility\VSEncrypt d'OfficeScan.
2. Copiez l'intégralité du dossier VSEncrypt sur l'ordinateur client.

Remarque : Ne copiez pas le dossier VSEncrypt dans le dossier OfficeScan. Le fichier Vsapi32.dll du Décodeur de fichiers infectés entrerait alors en conflit avec le fichier original Vsapi32.dll.

3. Ouvrez une fenêtre d'invite et atteignez l'emplacement auquel vous avez copié le dossier VSEncrypt.
4. Exécutez le Décodeur de fichiers infectés à l'aide des paramètres suivants :
 - aucun paramètre: encoder les fichiers stockés dans le dossier Suspect
 - -d: décoder les fichiers stockés dans le dossier Suspect
 - -debug: créer un journal de débogage et le déposer dans le dossier racine du client
 - /o: écraser le fichier encodé ou décodé s'il existe déjà
 - /f: {nom du fichier}: encoder ou décoder un seul fichier
 - /nr: ne pas restaurer le nom de fichier original

À titre d'exemple, vous pouvez saisir la commande `VSEncode [-d] [-debug]` pour encoder les fichiers du dossier Suspect et créer un journal de débogage. Lorsque vous décidez ou encodez un fichier, le fichier décodé ou encodé est créé dans le même dossier que le fichier source.

Remarque : Il est possible que vous ne puissiez pas encoder ou décoder les fichiers verrouillés.

Le Décodeur de fichiers infectés crée les journaux suivants :

- `VSEncrypt.log` : contient les détails de l'encodage ou du décodage. Ce fichier est créé automatiquement dans le dossier temporaire de l'utilisateur connecté au poste (normalement, sur le lecteur C:).
- `VSEncDbg.log` : contient les détails du débogage. Ce fichier est créé automatiquement dans le dossier temporaire de l'utilisateur connecté au poste (normalement, sur le lecteur C:). si vous exécutez `VSEncode.exe` en utilisant le paramètre `-debug`.

Pour encoder ou décoder les fichiers stockés dans d'autres dossiers :

1. Créez un fichier texte, puis saisissez le chemin d'accès complet aux fichiers que vous souhaitez encoder ou décoder.

Par exemple, si vous voulez encoder ou décoder des fichiers dans le chemin d'accès `C:\Mes documents\Reports`, saisissez `C:\My Documents\Reports*. *` dans le fichier texte. Enregistrez ensuite le fichier texte au format INI ou TXT, par exemple, `ForEncryption.ini` et déposez-le sur le lecteur C:.

2. Dans une fenêtre d'invite, exécutez le Décodeur de fichiers infectés en saisissant la commande `VSEncode.exe -d -i {emplacement du fichier texte INI ou TXT}`, où {emplacement du fichier texte INI ou TXT} contient le chemin d'accès au fichier INI ou TXT que vous venez de créer (par exemple, `C:\ForEncryption.ini`).

Client Mover I

Si vous disposez de plusieurs serveurs OfficeScan sur le réseau, vous pouvez utiliser l'outil Client Mover pour transférer des clients d'un serveur OfficeScan vers un autre. Cet outil est particulièrement utile lorsque vous ajoutez un nouveau serveur OfficeScan au réseau pour transférer des clients OfficeScan existants vers ce nouveau serveur.

Remarque : Les deux serveurs doivent posséder une version dans la même langue.

En cas d'utilisation de Client Mover I pour déplacer un client OfficeScan 5.58 ou 6.5 enregistré sur un serveur OfficeScan 5.58 ou 6.5 vers un serveur de la version actuelle, le client sera mis à jour automatiquement et le client de la version actuelle sera installé.

Pour utiliser Client Mover I :

1. Sur le serveur OfficeScan, accédez au répertoire suivant :
`\PCCSRV\Admin\Utility\IpXfer`
2. Copiez le fichier `IpXfer.exe` vers le client à transférer.
3. Sur le client, ouvrez une invite de commande, puis accédez au dossier vers lequel vous avez copié le fichier.
4. Exécutez Client Mover en utilisant la commande suivante :

```
IpXfer.exe -s <server_name> -p <server_listening_port> -m  
1 -c <client_listening_port>
```

où :

`<server_name>` = le nom du serveur OfficeScan de destination (le serveur sur lequel le client sera transféré)

<server_listening_port> = le port d'écoute (sécurisé) du serveur OfficeScan de destination. Pour afficher le port d'écoute (sécurisé) du serveur sur la console Web d'OfficeScan, cliquez sur **Administration > Serveur Web**. Le numéro du **champ Port** est le port d'écoute (sécurisé) du serveur ou le port Web.

1 = le serveur HTTP (vous devez utiliser le numéro « 1 » après « -m »)

<port_écoute_client> = numéro par l'intermédiaire duquel le serveur communique avec les clients configurés pendant l'installation. Pour afficher le port d'écoute (sécurisé) client sur la console Web d'OfficeScan, cliquez sur **Clients > Afficher l'état > Développer tout**. Le numéro situé à côté de l'étiquette du port est le port d'écoute (sécurisé) client.

5. Pour confirmer que le client communique désormais avec l'autre serveur, procédez comme suit :
 - a. Sur le client, cliquez du bouton droit de la souris sur l'icône du programme client OfficeScan dans la barre d'état système.
 - b. Sélectionnez la **Page principale OfficeScan**.
 - c. Cliquez sur **Aide** dans le menu et sélectionnez **A propos de**.
 - d. Vérifiez le serveur OfficeScan auquel se rapporte le client sous **Informations de communication, Nom/port du serveur**.

Remarque : si le client ne s'affiche pas dans l'arborescence des domaines du nouveau serveur OfficeScan sur lequel il est enregistré, redémarrez le service principal du nouveau serveur (ofservice.exe).

Outil Touch

L'outil Touch synchronise l'horodatage d'un fichier grâce à celui d'un autre fichier ou de l'horloge système de l'ordinateur. Si vous ne parvenez pas à déployer un correctif (une mise à jour ou un correctif publié par Trend Micro) sur le serveur OfficeScan, utilisez l'outil Touch pour changer l'horodatage du correctif. OfficeScan considère alors qu'il s'agit d'un nouveau correctif, ce qui amène le serveur à tenter de nouveau de déployer le correctif automatiquement

Pour exécuter Touch Tool :

1. Sur le serveur OfficeScan, accédez au répertoire suivant :

```
\PCCSRV\Admin\Utility\Touch
```

2. Copiez le fichier TMTouch.exe vers le dossier contenant le fichier à changer. Si vous synchronisez l'horodatage d'un fichier grâce à celui d'un autre fichier, placez les deux fichiers dans l'emplacement de l'outil Touch.
3. Ouvrez une invite de commande et accédez à l'emplacement de l'outil Touch.
4. Entrez :

```
TmTouch.exe <destination_filename> <source_filename>
```

où :

<destination_filename> = le nom du fichier (le correctif, par exemple) pour lequel vous voulez modifier l'horodatage

<source_filename> = le nom du fichier pour lequel vous voulez répliquer l'horodatage

Si vous ne définissez pas un nom de fichier source, l'outil utilise l'heure du système comme horodatage du fichier de destination.

Remarque : Vous pouvez utiliser la troncature « * » dans le champ du nom du fichier de destination, mais pas dans le champ du nom du fichier source.

5. Pour vérifier que l'horodatage a bien été modifié, saisissez `dir` dans l'invite de commande ou cliquez à l'aide du bouton droit de la souris sur le fichier dans Windows Explorer et sélectionnez **Propriétés**.

Outil ServerProtect Normal Server Migration

L'outil ServerProtect Normal Server Migration est un outil Windows qui vous aide à faire migrer vers le client OfficeScan les ordinateurs exécutant ServerProtect Normal Server.

Configuration système requise

L'outil ServerProtect Normal Server Migration possède les mêmes spécifications logicielle et matérielle que le serveur OfficeScan. Exécutez l'outil sur les ordinateur équipés de Windows NT/2000/XP/Server 2003.

Lorsque la désinstallation du serveur ServerProtect Normal a bien réussi, l'installation du client OfficeScan a lieu. Toutefois, l'outil ne permet pas de conserver ni de faire migrer les paramètres du serveur ServerProtect Normal vers ceux du client OfficeScan.

Installation de l'outil Server Protect Normal Server Migration

- Copiez les fichiers `SPNSXfr.exe` et `SPNSX.ini` dans le dossier `PCCSRV\Admin` sur le serveur OfficeScan.

Utilisez le compte administrateur local/domaine pour accéder à l'ordinateur client. Si vous vous connectez aux ordinateurs distants avec des privilèges insuffisants, en tant qu'invité ou utilisateur normal par exemple, vous ne pourrez pas réaliser l'installation.

Pour effectuer la migration avec l'outil Server Protect Normal Server Migration :

1. Double-cliquez sur le fichier `SPNSXfr.exe` pour ouvrir l'outil. La console de l'outil Server Protect Normal Server Migration s'ouvre.
2. Sous le serveur **OfficeScan**, sélectionnez le serveur OfficeScan sur lequel vous exécutez l'outil. Le chemin du serveur OfficeScan s'affiche sous le chemin du serveur OfficeScan. S'il est incorrect, cliquez sur **Parcourir** et sélectionnez le dossier `PCCSRV` du répertoire dans lequel vous avez installé OfficeScan.
Pour permettre à l'outil de retrouver le serveur OfficeScan lors de la prochaine ouverture de l'outil, cochez la case **Détection automatique du serveur OfficeScan** (cochée par défaut).

3. Sélectionnez les ordinateurs exécutant ServerProtect Normal Server sur lesquels effectuer la migration en cliquant l'une des options suivantes sous l'**ordinateur cible** :
 - **Arbre du réseau Windows** : affiche une arborescence des domaines de votre réseau. Pour sélectionner des ordinateurs par cette méthode, cliquez sur les domaines sur lesquels rechercher des ordinateurs clients.
 - **Nom du serveur d'informations** : recherche par nom de serveur d'informations. Pour sélectionner des ordinateurs par cette méthode, saisissez le nom d'un serveur d'informations sur votre réseau dans la zone de texte. Pour rechercher plusieurs serveurs d'informations, saisissez un point-virgule « ; » entre les noms de serveurs.
 - **Nom précis du serveur habituel** : recherche par nom de serveur habituel. Pour sélectionner des ordinateurs par cette méthode, saisissez le nom d'un serveur habituel sur votre réseau dans la zone de texte. Pour rechercher plusieurs serveurs habituels, saisissez un point-virgule « ; » entre les noms de serveurs.
 - **Recherche de la plage IP** : recherche par une plage d'adresses IP. Pour sélectionner des ordinateurs par cette méthode, saisissez une plage d'adresses IP de classe B sous la plage IP.

Remarque : Si un serveur DNS sur votre réseau ne répond pas lorsque vous recherchez des clients, la recherche plante. Attendez l'expiration du délai de recherche.

4. Pour ajouter des ordinateurs exécutant Windows Server 2003 dans la recherche, cochez la case **Inclure Windows Server 2003**.
5. Cochez la case permettant de **redémarrer les ordinateurs Windows Server 2003** pour relancer les ordinateurs exécutant Windows Server 2003. Pour que la migration réussisse sur les ordinateurs Windows 2003, ils doivent redémarrer. La sélection de cette case assure leur redémarrage automatique. Si vous ne cochez pas la case permettant de **redémarrer les ordinateurs Windows Server 2003**, vous devez redémarrer manuellement votre ordinateur après la migration.
6. Cliquez sur **Rechercher**. Les résultats de la recherche s'affichent sous les serveurs ServerProtect Normal.

7. Sous la **liste de serveurs**, cliquez sur les ordinateurs sur lesquels effectuer la migration :
- Pour sélectionner tous les ordinateurs, cliquez sur **Tout sélectionner**.
 - Pour désélectionner tous les ordinateurs, cliquez sur **Tout désélectionner**.
 - Pour exporter la liste en tant que fichier .CSV, cliquez sur **Exporter vers fichier CSV**.

Si un nom d'utilisateur et un mot de passe sont requis pour la connexion à l'ordinateur cible, procédez comme suit :

- a. Cochez la case **Utiliser un mot de passe/compte de groupe**.
 - b. Cliquez sur **Définir le compte de connexion utilisateur**. La fenêtre **Enter Administrator Information** s'affiche.
 - c. Saisissez le nom d'utilisateur et le mot de passe.
 - d. Cliquez sur **OK**.
 - e. Cliquez sur **Redemander si la connexion échoue** afin de pouvoir saisir de nouveau le nom d'utilisateur et le mot de passe durant le processus de migration si la connexion est impossible.
8. Cliquez sur **Migrer**.

Remarque : L'outil ServerProtect Normal Server Migration ne désinstalle pas l'agent Control Manager pour ServerProtect. Pour obtenir des instructions sur le mode de désinstallation de l'agent, consultez votre documentation ServerProtect et/ou Control Manager.

Pendant l'installation du client OfficeScan, le délai d'attente de l'installateur client de l'outil de migration peut expirer et le résultat peut s'afficher comme un échec. Toutefois, le client peut avoir été correctement installé. Vérifiez l'installation sur l'ordinateur client de la console Web OfficeScan.

La migration échoue dans les circonstances suivantes :

- si le client distant ne peut pas utiliser le protocole NetBIOS ou que les ports 455,137~139 sont bloqués
- si le client distant ne peut pas utiliser le protocole RPC
- Si le service Remote Registry est arrêté

Outils intégrés

Les fonctionnalités des outils suivants, intégrées aux versions précédentes d'OfficeScan, sont également intégrées à cette version :

Client Mover II

Client Mover II servait à transférer les clients HTTP en ligne depuis un serveur OfficeScan HTTP vers un autre serveur. Contrairement à Client Mover I, qui s'exécute à partir de l'interface de ligne de commande, Client Mover II comprenait une console Windows.

Désormais, vous pouvez déplacer des clients vers d'autres serveurs OfficeScan via la console Web du serveur OfficeScan (consultez la rubrique *Utilisation des domaines OfficeScan* à la page 2-10 pour obtenir des instructions détaillées).

Sauvegarde de la base de données

Database Backup a réalisé une sauvegarde de la base de données du serveur OfficeScan contenant tous les paramètres OfficeScan.

Vous pouvez à présent sauvegarder la base de données à partir de la console Web. (Consultez la rubrique *Sauvegarde de la base de données OfficeScan* à la page 4-8 pour obtenir des instructions détaillées).

Database Packer

Database Packer servait à compresser la base de données OfficeScan et à organiser les informations pour réduire la taille de la base de données et augmenter l'efficacité lors de l'exécution de requêtes.

Désormais, OfficeScan compresse et réorganise automatiquement la base de données pour optimiser les performances.

Icon Cleaner

Icon Cleaner servait à supprimer les enregistrements de clients dupliqués dans la base de données OfficeScan.

Si un client utilisateur désinstalle le programme OfficeScan, le poste client notifie au serveur OfficeScan, qui supprime automatiquement le client de l'arborescence de domaine client. Vous pouvez vérifier la connexion client-serveur pour mettre à jour l'état des clients sur le réseau (consultez la rubrique *Vérification de la Connexion serveur-client* à la page 2-36).

Network Scan Switch

Network Scan Switch vous permettait d'activer et de désactiver l'autorisation du client à scanner les dossiers et les lecteurs du réseau map.

Désormais, vous pouvez activer l'analyse des lecteurs mappés et des dossiers du réseau partagés lors de la configuration des paramètres de scan clients (consultez la rubrique *Définition des options de scan* à la page 2-46 pour obtenir des instructions détaillées).

Register Shell

Register Shell vous permettait d'ajouter un raccourci de Scan manuel dans le menu de raccourcis Windows de l'ordinateur client.

Désormais, vous pouvez ajouter un raccourci de Scan manuel dans le menu de raccourcis Windows de l'ordinateur client à partir de la console Web du serveur OfficeScan sur l'écran **Paramètres généraux du client**. Dans la barre latérale, cliquez sur **Clients > Paramètres généraux du client** (consultez l'aide en ligne pour obtenir des instructions détaillées).

Remote Agent

Remote Agent permettait aux clients d'obtenir les derniers composants directement depuis le serveur ActiveUpdate de Trend Micro, au lieu de passer uniquement par le serveur OfficeScan. La mise à jour directement à partir du serveur ActiveUpdate était nécessaire lorsque les postes clients ne pouvaient pas communiquer avec le serveur OfficeScan.

Désormais, lorsque les clients ne peuvent pas communiquer avec le serveur OfficeScan (par exemple, s'ils ne sont pas connectés à votre réseau), vous pouvez les autoriser à recevoir des mises à jour de composants à partir d'autres sources en les spécifiant comme des agents de mise à jour.

Spécifiez une liste de sources de mises à jour sur l'écran Source de mise à jour et autorisez les agents de mise à jour à recevoir des mises à jour à partir des sources sur l'écran Agent de mise à jour. Ensuite, utilisez Client Packager pour créer et déployer un module vers les clients (consultez la rubrique *Utilisation d'un agent de mise à jour* à la page 2-21, *Mise à jour d'OfficeScan* à la page 2-15, et le *Guide de déploiement et d'installation* ainsi que l'aide en ligne du serveur OfficeScan pour obtenir des instructions sur Client Packager).

GUID Changer

GUID Changer assignait de nouveaux Identificateurs globaux uniques (GUID) aux clients. Si vous utilisiez des outils de traitement de l'image différents de l'utilitaire de création d'image pour créer une image disque client, vous deviez assigner un nouveau GUID à chaque client installé depuis l'image disque.

Désormais, vous devez utiliser l'utilitaire de création d'image pour créer l'image d'un client OfficeScan et la cloner. Un nouveau GUID est créé pour chaque clone (consultez la rubrique *Utilitaire de création d'image* à la page 8-10).

Questions fréquemment posées, Dépannage et Support technique

Ce chapitre explique comment dépanner les problèmes pouvant survenir avec OfficeScan.

Dans ce chapitre, vous trouverez des informations sur les sujets suivants :

- *Foire aux questions (FAQ)* à la page 9-2
- *Dépannage* à la page 9-8
- *Contacter Trend Micro* à la page 9-20

Foire aux questions (FAQ)

Voici une liste de questions fréquemment posées et leur réponse.

Installation et mise à niveau

J'ai des plusieurs questions concernant l'installation et la mise à niveau d'OfficeScan. Où puis-je trouver les réponses ?

Consultez le *Guide de déploiement et d'installation*. Vous pouvez télécharger toute la documentation d'OfficeScan sur le site suivant :

<http://www.trendmicro-europe.com/download/>

Enregistrement

J'ai plusieurs questions concernant l'enregistrement d'OfficeScan. Où puis-je trouver les réponses ?

Consultez le site Web suivant pour voir les questions fréquemment posées concernant l'enregistrement :

http://fr.trendmicro-europe.com/enterprise/support/knowledge_base_detail.php?searchSolutionID=16326

Compatibilité

OfficeScan est-il compatible avec d'autres applications antivirus et anti-programmes espions/graywares ?

OfficeScan peut certes coexister sur les mêmes ordinateurs avec d'autres applications antivirus et anti-programmes espions/graywares, cependant Trend Micro recommande vivement de désinstaller toute autre solution tierce. Les interactions entre ces applications et OfficeScan peuvent provoquer des résultats inattendus et non souhaités, rendant vos ordinateurs vulnérables à une infection virale, aux attaques des pirates informatiques, et d'autres dangers potentiels.

OfficeScan prend-il en charge les serveurs SQL ?

Non. OfficeScan ne prend pas en charge les serveurs SQL.

OfficeScan peut-il fonctionner correctement dans un environnement réseau utilisant le mode Network Address Translation (NAT)?

Oui. Vous devez activer le déploiement programmé dans un environnement NAT afin de vous assurer que vos clients reçoivent les composants mis à jour (consultez la rubrique [Utilisation de la mise à jour programmée avec le mode NAT](#) à la page 2-33).

Pare-feu pour clients – version d'entreprise

Puis-je réinstaller OfficeScan et préserver mes paramètres de pare-feu ?

Oui. Vous pouvez sauvegarder la base de données du serveur OfficeScan et certains autres fichiers de configuration dans le dossier PCCSRV du serveur OfficeScan puis écraser la nouvelle base de données et les fichiers de configuration avec les sauvegardes. Pour des instructions spécifiques, consultez le Guide de déploiement et d'installation.

Comment puis-je tester et vérifier si le pare-feu et le système de détection d'intrusion fonctionnent ?

Créez et une stratégie de test et déployez-la sur un ordinateur test de votre réseau (consultez la rubrique [Test du pare-feu](#) à la page 6-22).

Comment puis-je éviter de remplacer la liste d'exceptions de mon client lorsque je déploie un nouveau profil de pare-feu ?

Cochez la case Remplacer le niveau de sécurité/la liste d'exceptions du client sur l'écran **Liste des profils** pour pouvoir appliquer à tous les clients sélectionnés le niveau de sécurité et la liste d'exceptions définis pour cette stratégie. Si vous souhaitez que vos clients préservent leurs paramètres, comme la liste d'exceptions, décochez cette case (consultez la rubrique [Configuration des profils](#) à la page 6-18).

Mise à jour du serveur et des clients

D'où le serveur OfficeScan reçoit-il par défaut les composants mis à jour ?

Le serveur OfficeScan reçoit par défaut les composants mis à jour du serveur Trend Micro ActiveUpdate. Si vous souhaitez recevoir des mises à jour depuis d'autres sources, configurez et mettez à jour la liste des sources à la fois pour une mise à jour automatique et pour une mise à jour manuelle.

À quelle fréquence dois-je mettre à jour le serveur et le client ?

Trend Micro publie des fichiers de signatures de virus normalement tous les jours et recommande de mettre à jour le serveur et les clients tous les jours. Vous pouvez conserver le paramètre de planification par défaut sur l'écran Mise à jour automatique pour mettre à jour le serveur au quotidien.

Quant un client OfficeScan doit-il recevoir des mises à jour du serveur Web Trend Micro ?

Accordez le privilège aux clients de télécharger leurs composants depuis le serveur Trend Micro ActiveUpdate lorsque vous avez des problèmes de réseau pouvant priver de connexion au serveur OfficeScan ou aux agents de mise à jour des clients.

Combien de clients OfficeScan un agent de mise à jour peut-il gérer ?

Cela dépend des spécifications matérielles de l'agent de mise à jour. Toutefois, le serveur OfficeScan ne pourra notifier que deux cent cinquante (250) clients à la fois, maintenant la file d'attente de notification à un maximum de 250, chaque agent de mise à jour va gérer au plus 250 procédures de téléchargement simultanément (consultez la rubrique [Utilisation d'un agent de mise à jour](#) à la page 2-21).

Comment un client distant ne disposant pas d'accès au serveur OfficeScan peut-il obtenir des composants mis à jour ?

Les clients ne pouvant pas se connecter au serveur OfficeScan peuvent recevoir leurs mises à jour depuis les agents de mise à jour ou depuis le serveur ActiveUpdate de Trend Micro.

À quelle fréquence dois-je mettre à jour le client ?

Trend Micro publie des fichiers de signatures de virus normalement tous les jours et recommande de mettre à jour le serveur et les clients tous les jours. Vous pouvez modifier les paramètres du programme de déploiement sur l'écran **Déploiement automatique** (consultez la rubrique [Utilisation du déploiement automatique](#) à la page 2-29).

Messages d'alerte

Quelle est la différence entre les messages d'alerte pour le moniteur d'activité virale, la prévention des épidémies, l'alerte d'épidémie et l'alerte standard ?

- OfficeScan envoie le message d'alerte moniteur d'activité virale lors de la détection d'un nombre excessif de sessions sur votre réseau. C'est le signal d'une possible épidémie (consultez la rubrique [Configuration du moniteur d'activité virale](#) à la page 5-11).
- OfficeScan envoie le message d'alerte lorsque vous activez manuellement la prévention des épidémies et que vous configurez la notification des clients en cas d'épidémies. Activez la prévention des épidémies uniquement lorsque vous êtes certain qu'une épidémie s'est déclarée sur le réseau (consultez la rubrique [Configuration de la notification des clients en cas d'épidémies](#) à la page 5-9).
- OfficeScan envoie le message d'alerte d'épidémie lors du scan et de la détection d'un nombre excessif de virus ou d'applications de graywares (consultez la rubrique [Configuration des alertes d'épidémies](#) à la page 2-42).
- OfficeScan envoie un message d'alerte standard immédiatement après la détection du premier virus ou de la première application de graywares (consultez la rubrique [Configuration des alertes standards](#) à la page 2-40).

Scan en cours

Quels types de virus OfficeScan peut-il détecter ?

Consultez la rubrique [Définition des virus](#) à la page 1-6 pour avoir un aperçu des types de virus. Consultez également la rubrique [Définition des programmes espions et autres types de graywares](#) à la page 3-2 pour obtenir un aperçu de ce que sont les graywares et de la façon dont OfficeScan peut les traiter.

OfficeScan peut-il détecter les cookies ?

Oui. OfficeScan peut détecter et éliminer les cookies. Pour de meilleurs résultats, activez les services Damage Cleanup (consultez la rubrique [Fonctionnement des services Damage Cleanup](#) à la page 3-6).

Quelle est la meilleure façon de protéger mes clients des programmes espions ?

Pour tirer le meilleur parti des possibilités anti-programmes espions/graywares d'OfficeScan, installez les Services Damage Cleanup (DCS) avec la protection antivirus standard. Le scan permettant de rechercher les programmes espions et

autres graywares n'est pas activé par défaut. Modifier les paramètres de scan par défaut afin d'activer le scan permettant de rechercher les programmes espions et autres graywares.

Suivez les instructions de suppression des programmes espions et d'autres types de graywares et tenez compte des suggestions pour la protection contre les programmes espions et autres types de graywares (*Suppression des programmes espions, des autres types de graywares, et des menaces des chevaux de Troie* à la page 3-1). Trend Micro recommande de créer une stratégie anti-programmes espions pour votre société.

Que sont les graywares ?

Graywares est un terme général permettant de décrire les fichiers et programmes, autres que des virus et des chevaux de Troie, qui peuvent affecter négativement les performances des ordinateurs connectés à votre réseau.

Il s'agit entre autre des logiciels d'espionnage, les logiciels publicitaires, des composeurs de numéros, des canulars, des outils de piratage, des outils d'accès distant, des applications de piratage de mots de passe et autres. Le moteur de scan OfficeScan recherche les graywares et les virus. Les services Damage Cleanup peuvent éliminer des chevaux de Troie actifs et des processus de graywares.

Support technique du serveur de stratégie de Trend Micro pour Cisco Network Admission Control (NAC)

Quels modèles de routeurs Policy Server for Cisco NAC prend-il en charge ?

Consultez la rubrique *Configuration minimale requise pour le serveur de stratégie* à la page A-19.

Cisco NAC valide-t-il les clients utilisant les nouveaux composants anti-programmes espions/graywares ?

Non. Cisco NAC valide uniquement les clients utilisant leurs composants antivirus (le fichier de signatures de virus et le moteur de scan).

Console Web

La console Web du serveur OfficeScan prend-elle en charge SSL ?

Oui. Pendant l'installation du serveur OfficeScan, vous pouvez activer SSL pour les communications serveur Web-navigateur sécurisées. Consultez le *Guide de déploiement et d'installation OfficeScan* pour obtenir des instructions sur la manière d'activer SSL après l'installation du serveur OfficeScan.

Documentation

Quelle documentation est disponible pour cette version d'OfficeScan ?

Cette version d'OfficeScan contient ce qui suit : *Guide de déploiement et d'installation*, *manuel de l'administrateur*, fichier Lisez-moi, et fichiers d'aide pour la console Web du serveur OfficeScan (que vous lisez actuellement), client, programme d'installation principal, console Web du serveur de stratégie et installateur du serveur de stratégies.

Puis-je télécharger la documentation d'OfficeScan ?

Oui. Vous pouvez télécharger le Guide de déploiement et d'installation, le manuel de l'administrateur et le fichier Lisez-moi depuis le site suivant :

<http://www.trendmicro-europe.com/download/>

Dépannage

Communication client-serveur

Cette section présente quelques éléments clés de la communication client-serveur d'OfficeScan. Le fait de comprendre le fonctionnement de la communication client-serveur vous permettra de résoudre plus rapidement les éventuels problèmes et de profiter des fonctions de gestion centralisée de la console Web.

L'état réel et l'état affiché ne sont pas synchronisés principalement parce que les entrées de la base de données ne correspondent pas aux valeurs du registre client.

Les étapes suivantes décrivent le cycle de communication client-serveur :

1. Le serveur demande au client d'installer le logiciel client ou de mettre à jour ses composants.
2. Le client déclare son état dans le registre après l'installation ou la mise à jour.
3. Le client communique son état au serveur.
4. Le serveur déclare son état à la base de données.
5. Le serveur affiche les informations mises à jour sur la console Web.
6. Le serveur affiche son état mis à jour dans l'icône du client.

Le client OfficeScan ne s'installera pas sur des ordinateurs exécutant Windows XP

Vous devez désactiver le **partage simple de fichiers** sur les clients Windows XP pour qu'ils puissent réussir l'installation du programme client OfficeScan (consultez votre documentation Windows pour obtenir des instructions).

Certains composants OfficeScan ne sont pas installés

Les licences attribuées aux divers composants des produits Trend Micro peuvent varier selon les régions. Il se peut que vous n'ayez pas reçu de licence pour le pare-feu pour clients – version d'entreprise, la protection et/ou les services Damage Cleanup. Après l'installation, vous verrez un résumé des composants que votre clé d'enregistrement/code d'activation vous permet d'utiliser. Contrôlez avec votre revendeur ou votre distributeur les composants pour lesquels vous possédez des licences.

Consultez le site Web suivant pour voir les questions fréquemment posées concernant l'enregistrement :

http://fr.trendmicro-europe.com/enterprise/support/knowledge_base_detail.php?searchSolutionID=16326

Impossible d'accéder à la console Web

Il existe plusieurs causes possibles pour ce problème.

Cache du navigateur

Si vous avez procédé à une mise à jour à partir d'une version antérieure d'OfficeScan, les fichiers caches du serveur proxy peuvent empêcher le chargement correct de la console Web d'OfficeScan. Videz la mémoire cache de votre navigateur et celle de tout serveur proxy situé entre le serveur OfficeScan et l'ordinateur que vous utilisez pour accéder à la console Web.

Certificat SSL

Vérifiez par ailleurs que votre serveur Web fonctionne correctement. Si vous utilisez SSL, assurez-vous que le certificat SSL est encore valide. Consultez la documentation de votre serveur Web pour un complément d'information.

Arrêt du serveur Web

Si vous utilisez Microsoft IIS Lockdown Tool™, l'arrêt de la configuration OfficeScan (.ini) et les fichiers exécutables (.exe) peuvent être la source du problème. Consultez votre documentation Microsoft pour connaître les façons de configurer l'outil de blocage pour autoriser l'accès et l'exécution de ces fichiers.

Paramètres du répertoire virtuel

Il peut y avoir un problème avec les paramètres du répertoire virtuel si vous exécutez la console Web du serveur OfficeScan sur un serveur IIS et que le message suivant s'affiche :

*Impossible d'afficher cette page
HTTP Error 403.1 – Forbidden: Execute access is denied.
Internet Information Services (IIS)*

Ce message peut s'afficher lorsque vous utilisez l'une des adresses suivantes pour accéder à la console :

`http://<nom du serveur>/officescan/`

`http://<nom du serveur>/officescan/default.htm`

Toutefois, la console peut s'ouvrir sans problème avec l'adresse suivante :

`http://<nom du serveur>/officescan/console/cgi/cgichkmasterpwd.exe`

Pour résoudre ce problème, vérifiez les permissions d'exécution du répertoire virtuel OSCE.

Exécutez les opérations suivantes :

1. Ouvrez le gestionnaire d'Internet Information Services (IIS).
2. Dans le répertoire virtuel OSCE, choisissez **Propriétés**.
3. Sélectionnez l'onglet **Répertoire virtuel** et définissez les permissions d'exécution sur **Scripts** au lieu de sur aucun.

Modifiez aussi les permissions d'exécution du répertoire virtuel d'installation du client.

Nombre de clients incorrect sur la console Web

Il est possible que le nombre de clients affiché sur la console Web soit incorrect.

Cette situation se produit lorsque vous conservez des enregistrements clients dans la base de données après la suppression du programme client. Si, par exemple, la communication client-serveur est interrompue alors que vous êtes en train de supprimer un client, le serveur ne reçoit pas de notification de la suppression de ce client. Par conséquent, il conservera dans la base de données les informations relatives à ce client et continuera d'afficher son icône sur la console Web. Si vous réinstallez ensuite le client, le serveur créera un nouvel enregistrement dans la base de données et affichera une nouvelle icône sur la console.

Cette erreur peut apparaître pendant les étapes 4 et 5 du cycle de communication client-serveur (consultez la rubrique *Communication client-serveur* à la page 9-8).

Pour détecter les enregistrements présents en plusieurs exemplaires, utilisez la fonction Vérification de la connexion. Consultez la rubrique *Vérification de la Connexion serveur-client* à la page 2-36 pour obtenir plus d'informations.


Vous pouvez également supprimer des clients inactifs automatiquement. Consultez la rubrique *Suppression des clients inactifs* à la page 4-5 pour obtenir plus d'informations.

Etat du client incorrect sur la console Web

Il est possible qu'OfficeScan ne synchronise pas l'état affiché sur la console avec l'état actuel des clients. Cette situation se produit lorsque le client est incapable de démarrer le programme client ou lorsque le client perd sa connexion au serveur avant de pouvoir communiquer son état.

Cette erreur peut apparaître pendant les étapes 4 et 5 du cycle de communication client-serveur (consultez la rubrique *Communication client-serveur* à la page 9-8).

Pour résoudre ce problème, vous devez procéder de la façon suivante :

- Pour vérifier si la communication client-serveur est établie, utilisez la fonction Vérification de la connexion. Consultez la rubrique *Vérification de la Connexion serveur-client* à la page 2-36 pour obtenir plus d'informations. Si le serveur peut communiquer avec le client, il signale que l'état actuel du client est **En ligne**.
- Vérifiez alors si l'ordinateur client est éteint, ou si le programme client a été déchargé, supprimé ou arrêté. Ces conditions amènent le serveur à signaler que l'état actuel du client est **Hors ligne**. Si une erreur est survenue pendant l'un de ces processus, il est possible que le client n'ait pas eu le temps d'informer le serveur qu'il était en train de se fermer ou d'être déchargé, supprimé ou arrêté. Par conséquent, le serveur n'est pas informé de la nécessité de modifier l'état du client en passant de l'état **En ligne** à **Hors ligne**. Sur le poste client, vérifiez si l'icône d'OfficeScan est affichée sous la forme . Si tel est le cas, cela signifie que le client est passé en mode itinérant.

Remarque : Si ces informations ne vous aident pas à identifier la cause de votre problème, utilisez ActiveSupport pour récupérer le fichier `Ofcddebug.log` à partir du serveur et à partir du client, puis contactez le support technique de Trend Micro. Consultez l'aide du client OfficeScan pour obtenir plus d'informations sur l'exécution d'ActiveSupport.

Les numéros de versions des composants sont incorrects

Il arrive que les numéros de version des composants clients ne soient pas correctement affichés par OfficeScan. Cette situation survient lorsque le client n'est pas en mesure de déclarer son état dans le registre, ni d'envoyer cette information au serveur.

Supposons que vous ayez mis à jour le fichier de signatures d'un client, de la version 411 à la version 413. Malgré la mise à jour, vous constatez que la console affiche toujours le numéro de version 411. Cette erreur s'explique par le fait que le client n'a pas été capable d'inscrire cette nouvelle information dans le registre.

Pour résoudre le problème d'affichage incorrect, procédez comme suit :

- Utilisez ping ou telnet pour vérifier si le client est encore connecté au réseau.
- Pour vérifier si la communication client-serveur est établie, utilisez la fonction Vérification de la connexion. Si le serveur peut communiquer avec le client, il signale que l'état actuel du client est **En ligne** (consultez la rubrique *Vérification de la Connexion serveur-client* à la page 2-36).
- Si votre bande passante est limitée, assurez-vous que cette limitation ne provoque pas un délai d'attente de connexion entre le serveur et le client.
- Si vous utilisez un serveur proxy pour la communication client-serveur, assurez-vous que la configuration des paramètres proxy est correcte.
- Ouvrez un navigateur Web sur le poste client, saisissez l'adresse `http:// {Server name}:{Server port}/officeScan/cgi/cgionstart.exe` et appuyez sur la touche ENTRÉE (si vous utilisez SSL, saisissez `https:// {Server name}:{Server port}/officeScan/cgi/cgionstart.exe`). Si l'écran suivant affiche -2, cela signifie que le client peut communiquer avec le serveur. Cela signifie également que le problème peut être lié à la base de données du serveur ; elle ne contient peut-être aucun enregistrement sur l'ordinateur client. Dans ce cas, contactez le support technique de Trend Micro.
- Assurez-vous que l'utilisateur possède les droits d'administration locale qui lui permettent d'écrire dans le registre de l'ordinateur client. OfficeScan écrit les informations relatives au client (notamment la version du fichier de signatures, du moteur de scan et du programme) sont inscrites dans le registre.

- Vérifiez si l'utilisateur a modifié des fichiers ou des valeurs de registre et s'il n'a pas oublié de redémarrer ensuite le service `Tmlisten.exe` (client Windows NT/2000/XP/Server 2003) ou le service `Pccwin97.exe` (client Windows 95/98/Me/98 SE).

Remarque : Si ces informations ne vous aident pas à identifier la cause de votre problème, utilisez ActiveSupport pour récupérer le fichier `Ofcdebug.log` à partir du serveur et à partir du client, puis contactez le support technique de Trend Micro. Consultez l'aide du client OfficeScan pour obtenir plus d'informations sur l'exécution d'ActiveSupport.

Echec de l'installation à partir d'une page Web ou avec installateur à distance

Si les utilisateurs signalent qu'il leur est impossible de procéder à l'installation à partir de la page Web interne ou de l'utilitaire d'installation à distance, procédez comme suit :

- Vérifiez l'existence de la communication client-serveur en utilisant ping et telnet.
- Vérifiez que vous disposez des privilèges d'administrateur sur l'ordinateur cible sur lequel vous souhaitez installer le client.
- Vérifiez si TCP/IP est activé et correctement configuré sur l'ordinateur client.
- Vérifiez si l'ordinateur cible possède la configuration minimale requise.
- Vérifiez si un fichier a été bloqué.
- Si votre bande passante est limitée, assurez-vous que cette limitation ne provoque pas un délai d'attente de connexion entre le serveur et le client.
- Si vous utilisez un serveur proxy pour la communication client-serveur, assurez-vous que la configuration des paramètres proxy est correcte.
- Ouvrez un navigateur Web sur le poste client, saisissez l'adresse `http://{Server name}:{server port}/officeScan/cgi/cgionstart.exe` et appuyez sur la touche ENTRÉE. Si l'écran suivant affiche -2, cela signifie que le client peut communiquer avec le serveur. Cela signifie également que le problème peut être lié à la base de données du serveur ; elle ne contient peut-être aucun enregistrement sur l'ordinateur client.

L'icône du client n'apparaît pas sur la console Web après l'installation

Il peut arriver que l'icône du client n'apparaisse pas sur la console après l'installation du client. Cette situation survient lorsque le client n'est pas en mesure de communiquer son état actuel au serveur.

Pour résoudre ce problème, vous devez procéder de la façon suivante :

- Vérifiez l'existence de la communication client-serveur en utilisant ping et telnet.
- Si votre bande passante est limitée, assurez-vous que cette limitation ne provoque pas un délai d'attente de connexion entre le serveur et le client.
- Assurez-vous que le dossier \PCCSRV du serveur possède des privilèges de partage et que tous les utilisateurs se sont vus accorder des privilèges de contrôle intégral.
- Assurez-vous que les paramètres proxy du serveur OfficeScan sont corrects.
- Ouvrez un navigateur Web sur le poste client, saisissez l'adresse `http:// {OfficeScan_Server_Name} : {port number} /officeScan/cgi/cgionstart.exe` et appuyez sur la touche ENTRÉE. Si l'écran suivant affiche -2, cela signifie que le client peut communiquer avec le serveur. Cela signifie également que le problème peut être lié à la base de données du serveur ; elle ne contient peut-être aucun enregistrement sur l'ordinateur client.
- Si vous avez déplacé le client vers un nouveau serveur OfficeScan avec l'outil Client Mover I, il se peut que vous ayez à redémarrer le service OfficeScan principal (`ofservice.exe`) sur le nouveau serveur.

Remarque : Si ces informations ne vous aident pas à identifier la cause de votre problème, utilisez ActiveSupport pour récupérer le fichier `Ofcdebug.log` à partir du serveur et à partir du client, puis contactez le support technique de Trend Micro. Consultez l'aide du client OfficeScan pour obtenir plus d'informations sur l'exécution d'ActiveSupport.

Problèmes pendant la migration à partir d'un logiciel antivirus tiers

Cette section traite de certains problèmes que vous pourriez rencontrer lors de la migration à partir d'un logiciel antivirus tiers.

Migration des clients

Le programme d'installation pour le client OfficeScan utilise le programme de désinstallation d'un logiciel tiers pour le supprimer automatiquement du système de vos utilisateurs et le remplacer par le client OfficeScan. Si la désinstallation automatique échoue, les utilisateurs pourront lire le message suivant :

Echec de la désinstallation.

Il existe plusieurs causes possibles pour cette erreur :

- La clé du produit ou le numéro de version du logiciel tiers est incohérent
- Le programme de désinstallation du logiciel tiers ne fonctionne pas
- Certains fichiers du logiciel tiers manquent ou sont corrompus
- La clé de registre pour le logiciel tiers ne peut pas être nettoyée
- Le logiciel tiers ne possède pas de programme de désinstallation

Il existe également plusieurs solutions possibles pour cette erreur :

- Supprimer manuellement le logiciel tiers
- Arrêter le service pour le logiciel tiers
- Décharger le service ou le processus pour le logiciel tiers

Pour supprimer manuellement le logiciel tiers :

- Si le logiciel tiers est enregistré dans Ajout/Suppression de programmes
 - a. Ouvrez le Panneau de configuration.
 - b. Double-cliquez sur **Ajout/Suppression de programmes**.
 - c. Sélectionnez le logiciel tiers dans la liste des programmes installés.
 - d. Cliquez sur **Supprimer**.
- Si le logiciel tiers n'est pas enregistré dans Ajout/Suppression de programmes
 - a. Ouvrez le registre Windows.
 - b. Accédez à HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\Uninstall.

- c. Localisez le logiciel tiers et exécutez la valeur de chaîne de désinstallation.
- d. Si le programme d'installation du logiciel tiers est au format MSI :
 - Localisez le numéro du produit
 - Vérifiez le numéro du produit
 - Exécutez la chaîne de désinstallation

Remarque : Certaines clés de désinstallation de produit se trouvent dans le dossier Clé de produit.

Pour modifier le service pour le logiciel tiers

1. Redémarrez l'ordinateur en mode sécurisé.
2. Modifiez le démarrage automatique du service en démarrage manuel.
3. Redémarrez le système encore une fois.
4. Supprimer manuellement le logiciel tiers.

Pour décharger le service ou le processus pour le logiciel tiers

AVERTISSEMENT ! *Cette procédure peut provoquer des effets indésirables sur votre ordinateur si elle n'est pas exécutée correctement. Trend Micro vous recommande fortement de sauvegarder d'abord votre système.*

1. Déchargez le service pour le logiciel tiers.
2. Ouvrez le registre Windows, puis localisez et supprimez la clé du produit.
3. Localisez et supprimez la clé d'exécution ou la clé de service d'exécution.

Vérifiez que la clé de registre du service dans HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services a été supprimée.

Le délai de connexion du client se produit fréquemment

Si vous avez déployé un grand nombre de clients sur le réseau, il peut arriver que le délai d'attente de la connexion entre le client et le serveur soit fréquemment dépassé. Cela provient d'une limite du nombre maximum de connexions TCP/IP simultanées entre les hôtes, imposée par Microsoft Windows.

Pour résoudre ce problème, procédez ainsi au choix :

- Augmentez la plage des ports anonymes.
 - a. Ouvrez l'éditeur de la base de registre Windows (Regedit.exe).
 - b. Recherchez le chemin suivant dans la base de registre :
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramètres`
 - c. Cliquez sur **Modifier > Nouveau > DWord value**.
 - d. Saisissez **MaxUserPort** dans la colonne **Nom**.
 - e. Cliquez sur **Edition > Modifier**.
 - f. Sous **Base**, cliquez sur **Décimal**.
 - g. Saisissez une valeur dans le champ **Données de valeur**. La valeur par défaut est 5000. Trend Micro recommande d'utiliser une valeur plus élevée que le nombre total de clients installés sur le réseau. La plage de valeurs admise est comprise entre 1 et 65534.
- Diminuez la valeur par défaut du délai d'attente TCP.
 - a. Ouvrez l'éditeur de la base de registre Windows (Regedit.exe).
 - b. Localisez la clé du chemin suivant dans le registre :
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramètres`
 - c. Cliquez sur **Modifier > Nouveau > DWord value**.
 - d. Saisissez **TcpTimedWaitDelay** dans la colonne **Nom**.
 - e. Cliquez sur **Edition > Modifier**.
 - f. Sous **Base**, cliquez sur **Décimal**.

- g. Saisissez une valeur dans le champ **Données de valeur**. La valeur par défaut est 240. Trend Micro recommande d'utiliser une valeur inférieure à cette valeur. La plage de valeurs admise est comprise entre 30 et 300.

Remarque : Pour plus d'informations sur les clés de registre MaxUserPort et TcpTimedWaitDelay, effectuez une recherche dans la base de connaissances de Microsoft accessible à l'adresse <http://support.microsoft.com/>

Téléchargement impossible du courrier électronique (POP3)

Si IPv6 est activé sur votre serveur Windows XP, vous pouvez peut-être lire ce message d'erreur lorsque vous tentez de vous connecter au courrier POP3 :

The server name you entered can not be found on the network (it might be down temporarily).

Pour résoudre ce problème, supprimez le protocole IPv6 :

- Pour Windows XP sans service packs installés :
 - a. Connectez-vous à l'ordinateur Windows XP avec un compte utilisateur disposant des privilèges d'administrateur local.
 - b. Ouvrez une invite de commande.
 - c. Entrez :
`ipv6 uninstall`
- Pour Windows XP avec SP1 et SP2 :
 - a. Connectez-vous à l'ordinateur Windows XP avec un compte utilisateur disposant des privilèges pour changer la configuration réseau.
 - b. Sélectionnez **Démarrer > Panneau de configuration > Connexions réseau**.
 - c. Cliquez du bouton droit sur une connexion locale, puis sur Propriétés.
 - d. Sélectionnez **Microsoft IPv6 Developer Edition (Windows XP avec SP1)** ou **Microsoft TCP/IP version 6 (Windows XP avec SP2)**.
 - e. Cliquez sur **Désinstaller**.
 - f. Cliquez sur **OK**.

Problèmes dans les environnements utilisant le mode Traduction d'adresses réseau (NAT)

Les problèmes suivants peuvent se poser si votre réseau utilise le mode Traduction d'adresses réseau (NAT) :

- **Les clients apparaissent hors ligne sur la console Web**
- **Le serveur OfficeScan n'est pas en mesure d'avertir les clients des mises à jour et des modifications de la configuration.**

Vous pouvez contourner ces problèmes en extrayant des composants et fichiers de configuration mis à jour du serveur pour les installer sur le client à l'aide d'une mise à jour programmée. Vous pouvez donner aux clients le privilège d'activer une mise à jour programmée, ce qui leur permet de mettre à jour automatiquement tant les fichiers de configuration que les composants antivirus conformément à une planification de Déploiement automatique que vous définissez (consultez la rubrique *[Configuration des privilèges et paramètres clients](#)* à la page 2-63 pour obtenir de plus amples informations sur l'activation d'une mise à jour programmée et la rubrique *[Utilisation du déploiement automatique](#)* à la page 2-29 pour des informations sur la configuration d'une mise à jour programmée).

Exécutez les opérations suivantes :

- Avant d'installer le client OfficeScan sur les ordinateurs clients, activez le déploiement programmé sur le serveur et donnez aux clients le privilège d'activer des mises à jour programmées.
Si vous le faites après l'installation du programme client OfficeScan, accordez aux clients le privilège d'effectuer une mise à jour immédiate et effectuez ensuite la mise à jour sur l'ordinateur client afin d'obtenir les paramètres de configuration mis à jour.

Lorsque des clients effectuent une mise à jour programmée, ils reçoivent à la fois les composants et les fichiers de configuration mis à jour.

Contacteur Trend Micro

Trend Micro possède plusieurs bureaux d'entreprise et commerciaux situés dans plusieurs villes dans le monde. Pour obtenir les coordonnées mondiales, visitez le site Trend Micro Worldwide :

http://fr.trendmicro-europe.com/enterprise/about_us/contact.php

Remarque : Les informations sur ce site Web peuvent être modifiées sans préavis.

Le Centre d'informations sur les virus de Trend Micro

Les informations détaillées sur les virus sont disponibles sur Internet, gratuitement, sur le site Web Infos sécurité de Trend Micro :

<http://fr.trendmicro-europe.com/enterprise/vinfo/encyclopedia.php>

Visitez le site Infos Sécurité pour :

- Lire le Rapport hebdomadaire sur les virus, qui inclut une liste des menaces susceptibles de se déclencher dans la semaine en cours et décrit les 10 menaces les plus répandues dans le monde pour la semaine en cours
- Afficher une carte des virus des 10 premières menaces dans le monde
- Consulter l'Encyclopédie des virus, une compilation des menaces connues comprenant l'évaluation des risques, les symptômes de l'infection, les plates-formes sensibles, la routine des dommages et les instructions sur la manière de supprimer la menace, ainsi que les informations sur les canulars informatiques
- Télécharger les fichiers tests auprès de l'institut européen pour la recherche des virus informatiques (EICAR), pour vérifier que votre produit de sécurité est correctement configuré
- Lire les informations générales sur les virus, comme par exemple :
 - Le Virus Primer, qui vous permet de comprendre les différences entre les virus, les chevaux de Troie, les vers et les autres menaces
 - Le *Safe Computing Guide* de Trend Micro

- Une description de l'évaluation des risques pour vous permettre de comprendre les dommages potentiels pour une menace classée Très faible ou Faible par rapport à Moyen ou Risque élevé
- Un glossaire sur les virus et la terminologie des autres menaces de sécurité
- Téléchargez la documentation technique industrielle détaillée
- S'abonner au service des alertes de Trend Micro, pour en savoir plus sur les épidémies lorsqu'elles se produisent, et au Rapport hebdomadaire sur les virus
- En savoir plus sur les outils de mise à jour des virus disponibles gratuitement pour les Webmestres
- En savoir plus sur TrendLabsSM, le centre de support et de recherche antivirus mondial de Trend Micro

Problèmes connus

Les problèmes connus sont des fonctions du logiciel OfficeScan qui peuvent requérir temporairement une solution de rechange. Les problèmes connus sont généralement documentés dans le document Lisez-moi fourni avec votre produit. Vous pouvez également trouver le document Lisez-moi pour les produits Trend Micro dans le centre de mise à jour Trend Micro :

<http://www.trendmicro-europe.com/download/>

Vous pouvez trouver les problèmes connus dans la Base de connaissances du support technique :

<http://www.trendmicro-europe.com/kb/>

Trend Micro vous recommande de toujours vérifier le document Lisez-moi pour obtenir des informations sur les problèmes connus qui pourraient affecter l'installation ou la performance, ainsi que pour obtenir une description des nouveautés dans une version particulière, la configuration minimale requise et d'autres conseils.

Contacter le Support technique

La licence concédée avec les logiciels Trend Micro comprend généralement l'accès aux mises à jour des produits et aux fichiers de signatures ainsi qu'une assistance technique de base pendant une période d'un an à compter de la date d'achat uniquement. Cette période écoulée, vous devrez renouveler le contrat de maintenance sur une base annuelle et vous acquitter des frais de maintenance alors en vigueur chez Trend Micro.

Vous pouvez contacter Trend Micro par télécopie, par téléphone et par e-mail ou visitez le site Web

<http://www.trendmicro-europe.com>

Accélérer votre appel de support

Lorsque vous contactez la Base de connaissances, pour accélérer la résolution de vos problèmes, réunissez les informations suivantes :

- Versions de Microsoft Windows et du Service Pack
- Type de réseau
- Marque de l'ordinateur, modèle et tout matériel complémentaire connecté à votre ordinateur
- Quantité de mémoire et d'espace disque disponibles sur votre ordinateur
- Description détaillée de l'environnement d'installation
- Texte exact du message d'erreur affiché
- Étapes permettant de reproduire le problème

La Base de connaissances Trend Micro

La Base de connaissances Trend Micro est une ressource en ligne 24H sur 24, 7 jours sur 7, qui contient des milliers de procédures de support technique à effectuer soi-même pour les produits Trend Micro. Utilisez la Base de connaissances, par exemple, si vous obtenez un message d'erreur et que vous souhaitez connaître la procédure à suivre. De nouvelles solutions sont ajoutées quotidiennement.

Vous trouverez également dans la Base de connaissances un Forum Aux Questions sur les produits, des astuces importantes, des conseils antivirus préventifs et des coordonnées régionales pour le support et la vente.

Tous les clients Trend Micro ainsi que toute personne utilisant une version d'évaluation d'un produit ont accès à la Base de connaissances. Visitez :

<http://www.trendmicro-europe.com/kb/>

Si vous ne trouvez pas de réponse à une question particulière, la Base de connaissances inclut un service supplémentaire vous permettant de soumettre votre question via un message par e-mail. Le temps de réponse est généralement de 24 heures ou moins.

Envoi de fichiers suspects à Trend Micro

Vous pouvez envoyer vos virus, fichiers infectés, chevaux de Troie, vers suspects, logiciels espions et autres fichiers suspects à Trend Micro pour les évaluer. Pour cela, contactez l'assistance de votre fournisseur ou visitez l'URL de l'Assistant d'envoi de Trend Micro :

<http://www.trendmicro-europe.com/avservice/>

Cliquez sur le lien sous le type d'envoi que vous souhaitez faire.

Remarque : Les soumissions faites via l'assistant d'envoi/le docteur antivirus sont envoyées rapidement et ne sont pas sujettes aux règles et aux restrictions définies dans le contrat de support « Trend Micro Virus Response Service Level ».

Lorsque vous soumettez votre cas, un écran d'accusé de réception s'affiche. Cet écran affiche également un numéro de cas. Notez le numéro de cas pour le suivi du dossier.

À propos de TrendLabs

TrendLabs constitue l'infrastructure mondiale des centres de support de produits et de recherche antivirus de Trend Micro qui fournissent des informations sur les virus de dernière minute aux consommateurs de Trend Micro.

Les « médecins de virus » de chez TrendLabs surveillent les risques de virus potentiels dans le monde, pour garantir la protection des produits Trend Micro contre les menaces émergentes. Le point culminant quotidien de ces efforts est partagé avec les consommateurs via des mises à jour de fichiers de signatures de virus fréquentes et des perfectionnements des moteurs de scan.

TrendLabs est une équipe de plusieurs centaines d'ingénieurs et de personnel de support qualifié qui fournissent une large gamme de services de support technique et de produits. Les centres de services dédiés et les équipes de réponse rapide sont situés à Tokyo, Manille, Taipei, Munich, Paris et Forest Lake, en Californie, pour migrer les épidémies virales et fournir un support urgent.

Le siège social moderne de TrendLabs situé dans un parc informatique principal de Metro Manila, a obtenu la certification ISO 9002 pour ses procédures de gestion de qualité en 2000, un des premiers équipements de support et de recherche antivirus à être ainsi agréé. Nous pensons que TrendLabs est l'équipe leader de support et de service dans l'industrie antivirus.

Policy Server pour Cisco™ NAC Primer

La présente annexe sert de primer pour Cisco Network Admission Control (NAC). Elle apporte des informations fondamentales au sujet de la technologie NAC. Lisez cette annexe afin de vous familiariser avec les concepts et la terminologie associée à Cisco NAC avant d'installer et de configurer les divers composants de Cisco NAC.

Les sujets évoqués dans la présente annexe sont entre autres :

- *Présentation de Trend Micro Policy Server pour Cisco NAC* à la page A-2
- *Policy Server pour Cisco™ NAC Primer* à la page A-1
- *Architecture Cisco NAC* à la page A-5
- *La séquence de validation du client* à la page A-6
- *Définition du serveur de stratégie* à la page A-8
- *Définition des certificats* à la page A-16
- *Configuration minimale requise pour le serveur de stratégie* à la page A-19

Présentation de Trend Micro Policy Server pour Cisco NAC

Le serveur de stratégie Trend Micro pour Cisco Network Admission Control (NAC) permet d'évaluer l'état des composants antivirus des clients OfficeScan. Les options de configuration du serveur de stratégie vous permettent de configurer les paramètres afin d'effectuer des actions sur des clients à risque, de manière à les mettre en conformité avec les initiatives antivirus de votre société.

Ces actions sont :

- Demander aux clients de mettre à jour leurs composants client OfficeScan
- Activer le scan en temps réel
- Exécuter un scan immédiat et un nettoyage immédiat
- Afficher un message de notification sur les ordinateurs clients informant les utilisateurs en cas de violation de la stratégie antivirus.

Pour vous aider à analyser les performances de vos stratégies antivirus, vous pouvez utiliser l'option de consultation des journaux du serveur de stratégie, qui enregistre des informations telles que le moment où le serveur de stratégie a évalué les clients et le résultat de ces évaluations.

Remarque : Pour obtenir des informations supplémentaires sur la technologie Cisco NAC, consultez le site Web Cisco à l'adresse www.cisco.com/go/nac.

Composants et terminologie

Vous trouverez ci-dessous la liste des divers composants et des termes importants auxquels vous devez vous familiariser afin de comprendre et d'utiliser le Policy Server pour Cisco NAC :

Composants

Les composants suivants sont nécessaires pour la mise en œuvre Trend Micro du Policy Server pour Cisco NAC:

- **Cisco Trust Agent (CTA)** : une installation sur un client pour lui permettre de communiquer avec d'autres composants Cisco NAC
- **Client OfficeScan** : un ordinateur client sur lequel le programme client OfficeScan est installé. Pour utiliser Cisco NAC, Cisco Trust Agent doit également être installé sur l'ordinateur client
- **Périphérique d'accès au réseau** : un périphérique réseau prenant en charge la fonctionnalité Cisco NAC. Les périphériques d'accès au réseau pris en charge comprennent des routeurs Cisco, des pare-feu, des points d'accès, ainsi que des dispositifs tiers avec Terminal Access Controller Access Control System (TACACS+) ou le protocole du service utilisateur de commutation à distance (RADIUS). Pour obtenir la liste des routeurs pris en charge, consultez www.cisco.com/go/nac à la page A-20.
- **Compte serveur à accès contrôlé (ACS)** : un serveur qui reçoit les données antivirus du client OfficeScan par l'intermédiaire du périphérique d'accès au réseau et les transmet à une base de données externe d'utilisateurs pour évaluation. A un stade ultérieur du processus, le serveur ACS transmet également au périphérique d'accès au réseau le résultat de l'évaluation, qui peut comprendre des instructions à l'intention du client OfficeScan.

Remarque : Le serveur ACS compte des options de configuration en dehors du champ de la mise en œuvre de Trend Micro du Policy Server pour Cisco NAC : par exemple, il peut effectuer d'autres actions sur le client, entre autre empêcher l'accès au réseau. Reportez-vous à la documentation relative au serveur Cisco Secure Access Control pour obtenir de plus amples informations.

- **Serveur de stratégie** : ordinateur qui reçoit et évalue les données antivirus du client OfficeScan. Après l'évaluation, le serveur de stratégie détermine les actions à mener par le client OfficeScan. Ces informations sont ensuite renvoyées au client.
- **Serveur OfficeScan** : le serveur OfficeScan envoie au serveur de stratégie, un rapport sur les versions actuelles du fichier de signatures de virus et du moteur de scan, que le serveur de stratégie utilise pour évaluer le client OfficeScan.

Terminologie

Familiarisez-vous aux termes suivants liés au Policy Server pour Cisco NAC.

- **État de sécurité** : présence et actualité du logiciel antivirus installé sur un client. Dans le présent contexte, l'état de sécurité fait référence à ce qui suit : présence ou pas du programme client OfficeScan sur les clients, état de certains paramètres du client OfficeScan et âge des versions du moteur de scan et du fichier de signatures de virus.
- **Jeton d'état** : informations créées par le serveur de stratégie après validation d'un client OfficeScan, y compris des instructions qui indiquent au client OfficeScan qu'il doit exécuter des actions indiquées telles que l'activation du scan en temps réel ou la mise à jour des composants antivirus.
- **Validation du client** : le processus qui consiste à évaluer l'état de sécurité du client et à renvoyer le jeton d'état au client.
- **Règle du serveur de stratégie** : directives contenant les critères de configuration utilisés par le serveur de stratégie, afin de mesurer l'état de sécurité d'un client OfficeScan. Une règle contient également des actions que le client et le serveur de stratégie doivent exécuter si les informations sur l'état de sécurité correspondent aux critères (consultez *Définition du serveur de stratégie, des stratégies et des règles* à la page A-9 pour obtenir des informations détaillées).
- **Stratégie du serveur de stratégie** : règles du serveur de stratégie avec lesquelles il mesure l'état de sécurité des clients OfficeScan. Les stratégies contiennent également des actions que les clients et le serveur de stratégie doivent exécuter si les critères de règles associées à la stratégie ne correspondent pas à l'état de sécurité (consultez *Définition du serveur de stratégie, des stratégies et des règles* à la page A-9 pour obtenir des informations détaillées).

Architecture Cisco NAC

Figure A-1 représente une architecture Cisco NAC de base comprenant les composants décrits ci-dessus.

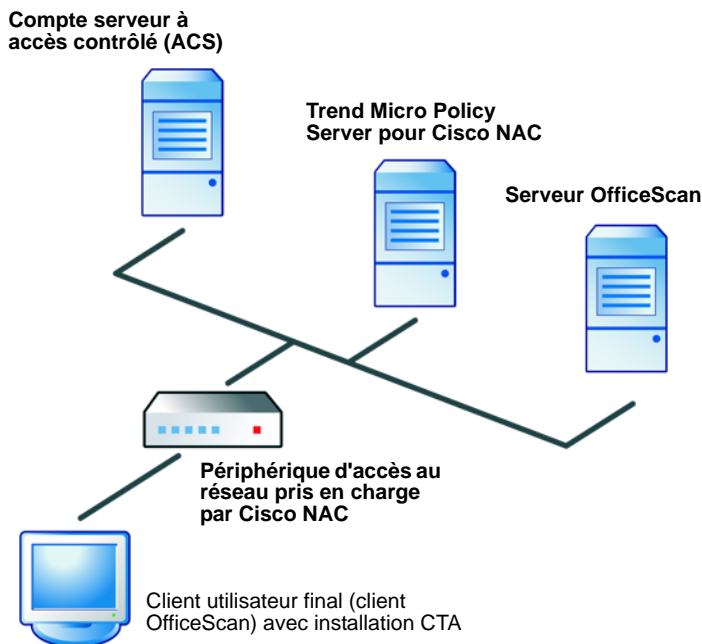


FIGURE A-1 Architecture Cisco NAC de base

Le client OfficeScan dans la Figure A-1 présente une installation CTA et peut uniquement accéder au réseau par le biais d'un périphérique d'accès au réseau prenant en charge Cisco NAC. Le périphérique d'accès au réseau se situe entre le client et les autres composants Cisco NAC.

Remarque : L'architecture de votre réseau peut être différente, en fonction de la présence ou pas de serveurs proxy, de routeurs ou de pare-feu.

La séquence de validation du client

La validation du client désigne le processus consistant à évaluer l'état de sécurité d'un client OfficeScan et à renvoyer des instructions à exécuter par le client si le serveur de stratégie considère qu'il est exposé à un risque. Le serveur de stratégie valide un client OfficeScan à l'aide de règles et de stratégies configurables.

Figure A-2 illustre la séquence des événements qui se produisent lorsqu'un client OfficeScan tente d'accéder au réseau :

ÉTAPE1: Le périphérique d'accès au réseau Cisco lance la séquence de validation en se renseignant sur l'état de sécurité du client lorsqu'il tente d'accéder au réseau.

ÉTAPE2: Le périphérique d'accès au réseau transmet alors l'état de sécurité au serveur ACS.

ÉTAPE3: Le serveur ACS transmet également l'état de sécurité au serveur de stratégie qui procède à une évaluation.

ÉTAPE4: Dans un processus distinct, le serveur de stratégie interroge périodiquement le serveur OfficeScan pour obtenir des informations sur le fichier de signatures et le moteur de scan, afin de tenir à jour ses données. Il utilise alors une stratégie que vous configurez afin de comparer de ces informations avec les données de l'état de sécurité du client.

ÉTAPE5: Ensuite, le serveur de stratégie crée un jeton d'état et le renvoie au client OfficeScan.

ÉTAPE6: Enfin, le client exécute sur lui-même les actions configurées dans le jeton d'état.

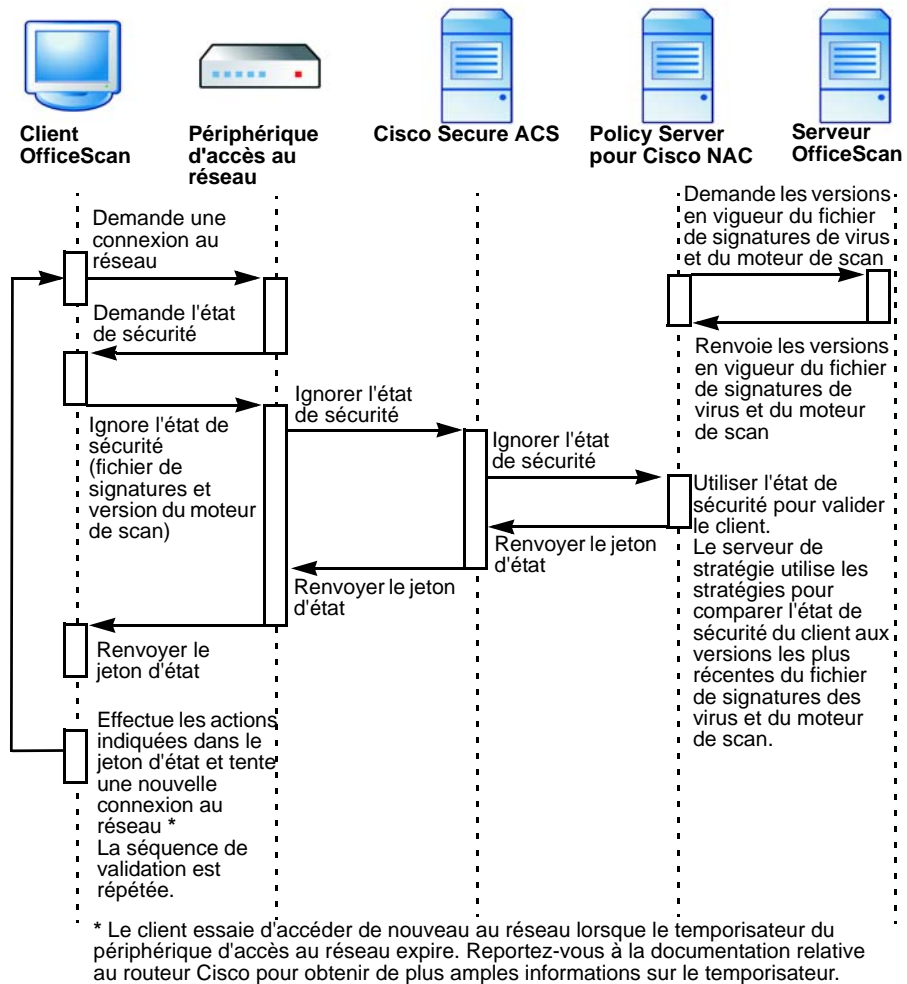


FIGURE A-2 Séquence de validation d'accès au réseau

Définition du serveur de stratégie

Le serveur de stratégie évalue l'état de sécurité du client OfficeScan et crée le jeton d'état. Il effectue cette évaluation en comparant l'état de sécurité aux versions les plus récentes du fichier de signatures de virus et du moteur de scan envoyées par le serveur OfficeScan dont le client est membre. Il renvoie le jeton d'état au serveur Cisco Secure ACS, qui le transmet lui-même au client par l'intermédiaire du périphérique d'accès au réseau Cisco.

L'installation de serveurs de stratégie supplémentaires sur un réseau unique peut améliorer les performances lorsqu'un grand nombre de clients tentent d'accéder simultanément au réseau et agir comme sauvegarde lorsqu'un serveur de stratégie devient inutilisable. Si plusieurs serveurs OfficeScan sont installés sur un réseau, le serveur de stratégie traite les demandes de tous les serveurs OfficeScan enregistrés sur ce réseau. De même, plusieurs serveurs de stratégie peuvent traiter des demandes d'un serveur OfficeScan unique qui est enregistré sur tous les serveurs de stratégie. La Figure A-3 illustre la relation de serveurs OfficeScan et de serveurs de stratégie multiples.

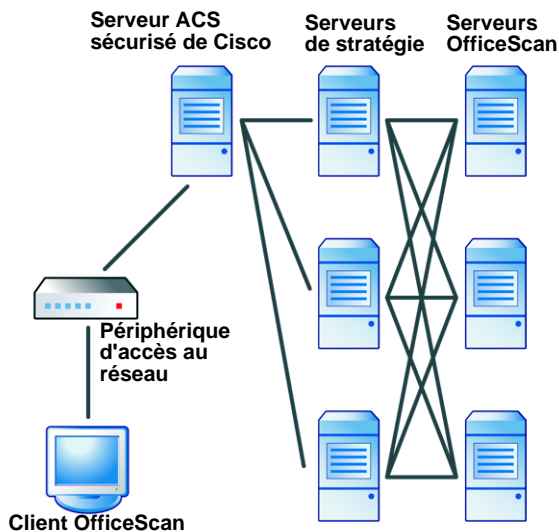


FIGURE A-3 Relation de multiples serveurs OfficeScan et de serveurs de stratégies

Vous pouvez aussi installer le serveur de stratégie sur le même ordinateur que le serveur OfficeScan.

Définition du serveur de stratégie, des stratégies et des règles

Les serveurs de stratégie utilisent des stratégies et des règles configurables pour favoriser l'application des stratégies et consignes de sécurité de votre entreprise.

Les *règles* sont composées de critères spécifiques que les serveurs de stratégies comparent à l'état de sécurité du client OfficeScan. Si l'état de sécurité du client correspond aux critères configurés dans une règle, le client et le serveur exécutent les actions spécifiées dans la règle (voir *[Demander au serveur de stratégie et au client OfficeScan d'effectuer des actions](#)* à la page A-11).

Les *stratégies* sont composées d'une ou plusieurs règles. Attribuez une stratégie à chaque serveur OfficeScan enregistré sur votre réseau en modes Épidémie et normal (consultez *[Mise en œuvre de la prévention contre les épidémies virales](#)* à la page 5-2).

Si l'état de sécurité du client OfficeScan correspond aux critères d'une règle appartenant à la stratégie, le client OfficeScan exécute les actions configurées dans la règle. Mais si l'état de sécurité du client ne correspond pas à tout ou partie des critères de règles associés à la stratégie, vous pouvez configurer des actions par défaut dans la stratégie que le client et le serveur devront exécuter (consultez *[Demander au serveur de stratégie et au client OfficeScan d'effectuer des actions](#)* à la page A-11).

Conseil : Si vous souhaitez que certains clients d'un domaine OfficeScan disposent de stratégies, en mode Épidémie et normal, différentes de celles des autres clients du même domaine, Trend Micro vous suggère de restructurer le domaine en groupes de clients présentant les mêmes exigences (consultez *[Utilisation des domaines OfficeScan](#)* à la page 2-10).

Création des règles

Les règles comprennent des critères d'état de sécurité, des réponses par défaut associées à des clients et des actions à exécuter par les clients et par le serveur de stratégie.

Critères d'état de sécurité

Les règles comprennent les critères d'état de sécurité suivants :

- L'état du scan en temps réel du client indique si le scan en temps réel est activé ou désactivé.
- Actualité de la version du moteur de scan du client – indique si le moteur de scan est à jour.
- État du fichier de signatures de virus du client – quel est le degré de mise à jour du fichier de signatures de virus. Le serveur de stratégie détermine ce point en vérifiant l'un des éléments suivants :
 - si le fichier de signatures de virus est antérieur d'une série de versions par rapport à la version du serveur de stratégie ;
 - si le fichier de signatures de virus a été émis plusieurs jours avant la validation.

Réponses par défaut des règles

Les réponses vous aident à connaître l'état des clients OfficeScan de votre réseau lors de la validation des clients. Elles apparaissent dans les journaux de validation du client du serveur de stratégie et correspondent à des jetons d'état. Vous avez le choix entre les réponses par défaut suivantes :

- **Sain** : le client est conforme à vos stratégies de sécurité
- **Vérification** : le client doit mettre à jour ses composants antivirus.
- **Quarantaine** : le client présente un risque élevé d'infection.
- **Infecté** : le client est infecté ou présente un risque d'infection.
- **Inconnu** : autre état.

Remarque : Vous ne pouvez ni ajouter, ni supprimer, ni modifier les réponses.

Demander au serveur de stratégie et au client OfficeScan d'effectuer des actions

Si l'état de sécurité du client correspond aux critères des règles, le serveur de stratégie peut exécuter les actions suivantes :

- Créer une entrée dans un journal de validation client du serveur de stratégie (consultez *Utilisation des journaux de validation du client* à la page B-33 pour obtenir de plus amples informations à ce sujet).

Si l'état de sécurité du client correspond aux critères des règles, le client OfficeScan peut exécuter les actions suivantes :

- Activer le scan en temps réel du client, afin que le client OfficeScan scanne tous les fichiers à l'ouverture ou à l'enregistrement (consultez *Configuration du scan en temps réel* à la page 2-51 pour obtenir de plus amples informations à ce sujet)
- Mettre à jour tous les composants OfficeScan (consultez *Mise à jour d'OfficeScan* à la page 2-15 pour obtenir de plus amples informations)
- Scanner le client après l'activation du scan en temps réel ou après une mise à jour
 - Si ce qui précède est sélectionné, les services Anti-Spyware (nettoyage immédiat) s'exécutent automatiquement avec l'option d'exécution automatique d'un scan immédiat

Remarque : Activer le scan en temps réel pour obtenir l'exécution automatique de la fonction Scan immédiat.

- Afficher un message de notification à l'utilisateur du client

Règles par défaut

Le serveur de stratégie met à votre disposition des règles par défaut pour vous aider à configurer vos paramètres. Les règles couvrent les situations de sécurité courantes et l'activation d'une action que Trend Micro recommande. Les règles suivantes sont disponibles par défaut :

Nom de la règle : Sain

Critères correspondants :

état du scan en temps réel : activé

moteur de scan et fichier de signatures de virus à jour

Réponse en cas de correspondance des critères :

sain

Action du serveur :

aucune

Action du client :

aucune

Nom de la règle : Vérification

Critères correspondants :

L'état des signatures de virus du client est au minimum antérieur à celui du serveur OfficeScan sur lequel le client est enregistré.

Réponse en cas de correspondance des critères :

vérification

Action du serveur :

créer une entrée dans le journal de validation du client

Action du client :

mettre à jour les composants

exécuter un nettoyage immédiat sur le client après l'activation du scan en temps réel ou l'exécution d'une mise à jour.

Afficher le message de notification à l'utilisateur du client

Conseil : Si vous utilisez cette règle, Trend Micro vous recommande d'utiliser le déploiement automatique. Cette opération permet d'assurer que les clients reçoivent le dernier fichier de signatures de virus immédiatement après le téléchargement des nouveaux composants par le serveur OfficeScan (consultez *Utilisation du déploiement automatique* à la page 2-29).

Nom de la règle : Mise en quarantaine

Critères correspondants :

Le fichier de signatures de virus est au minimum cinq versions antérieures au fichier de signatures du serveur OfficeScan sur lequel le client est enregistré,

Réponse en cas de correspondance des critères :

mise en quarantaine

Action du serveur :

créer une entrée dans le journal de validation du client

Action du client :

mettre à jour les composants

Exécuter un nettoyage immédiat automatique et un scan immédiat sur le client après l'activation du scan en temps réel ou l'exécution d'une mise à jour.

afficher le message de notification à l'utilisateur du client

Nom de la règle : Non protégé

Critères correspondants :

état du scan en temps réel : désactivé

Réponse en cas de correspondance des critères :

infecté

Action du serveur :

créer une entrée dans le journal de validation du client

Action du client :

activer le scan du client en temps réel

afficher le message de notification à l'utilisateur du client

Création des stratégies

Les stratégies comprennent un nombre indéfini de règles, et de réponses et d'actions par défaut.

Application des règles

Le serveur de stratégie applique les règles dans un ordre donné, ce qui vous permet de leur attribuer des priorités. Vous pouvez modifier l'ordre des règles, ajouter des règles et supprimer des règles d'une stratégie.

Réponses par défaut des stratégies

Comme pour les règles, les stratégies possèdent des réponses par défaut vous permettant de connaître l'état des clients OfficeScan de votre réseau lors de la validation des clients. Cependant, les réponses par défaut ne sont associées aux clients que lorsque l'état de sécurité de ceux-ci ne correspond à aucune règle de la stratégie.

Les réponses des stratégies et des règles sont identiques (consultez *Réponses par défaut des règles* à la page A-10 pour obtenir la liste des réponses).

Demander au serveur de stratégie et au client OfficeScan d'effectuer des actions

Le client OfficeScan et le serveur de stratégie peuvent exécuter les mêmes actions pour les stratégies que pour les règles. Cependant, les actions ne sont exécutées que lorsque l'état de sécurité du client ne correspond à aucune règle de la stratégie (consultez *Demander au serveur de stratégie et au client OfficeScan d'effectuer des actions* à la page A-11 pour obtenir la liste des actions).

Stratégies par défaut

Le serveur de stratégie met à votre disposition des stratégies par défaut pour vous aider à configurer vos paramètres. Deux stratégies sont disponibles : une pour le mode normal et une pour le mode d'attaque.

Nom de la stratégie : Stratégie par défaut en mode normal

Règles par défaut associées à cette stratégie :

non protégé, Quarantaine et Vérification

Réponse si aucune des règles ne correspond :

sain

Action du serveur :

aucune

Action du client :

aucune

Nom de la stratégie : Stratégie par défaut en mode épidémie

Règles par défaut associées à cette stratégie :

sain

Réponse si aucune des règles ne correspond :

infecté

Action du serveur :

créer une entrée dans le journal de validation du client

Action du client :

activer le scan du client en temps réel

mettre à jour les composants

Exécuter un nettoyage immédiat et un scan immédiat sur le client après l'activation du scan en temps réel ou l'exécution d'une mise à jour.

afficher le message de notification à l'utilisateur du client

Définition de la synchronisation

Synchronisez régulièrement le serveur de stratégie sur les serveurs OfficeScan enregistrés afin de garder les versions du serveur de stratégie, du fichier de signatures de virus, du moteur de scan et de l'état de l'épidémie du serveur (mode normal ou mode attaque) à jour par rapport à ceux du serveur OfficeScan. Pour effectuer la synchronisation, procédez comme suit :

- Manuellement – exécute la synchronisation au moment de votre choix dans l'écran Résumé (consultez *Consultez le résumé des informations d'un serveur de stratégie* à la page B-23)
- Programmée – définit un planning de synchronisation par OfficeScan (consultez *Configuration de la synchronisation programmée* à la page B-36)

Définition des certificats

La technologie Cisco NAC fait appel aux certificats numériques suivants afin d'établir une bonne communication entre les divers composants :

- **Certificat ACS** : établit une communication fiable entre le serveur ACS et le serveur d'autorité de certificat (CA). Le serveur d'autorité de certificat signe le certificat ACS avant que vous ne l'enregistriez sur le serveur ACS.
- **certificat CA** : authentifie les clients OfficeScan auprès du compte serveur à accès contrôlé (ACS). Le serveur OfficeScan déploie le certificat CA sur le serveur ACS et sur les clients OfficeScan (fourni avec le pack Cisco Trust Agent).
- **certificat SSL du serveur de stratégie** : établit une communication HTTPS sécurisée entre le serveur de stratégie et le compte serveur à accès contrôlé (ACS). Le certificat SSL du serveur de stratégie est automatiquement généré par le serveur de stratégie, pendant l'installation de ce dernier.

Conseil : Le certificat SSL du serveur de stratégie est facultatif. Cependant, Trend Micro conseille l'encodage des données échangées entre le serveur de stratégie et le serveur ACS.

La Figure A-4 illustre les étapes de la création et du déploiement des certificats ACS et CA :

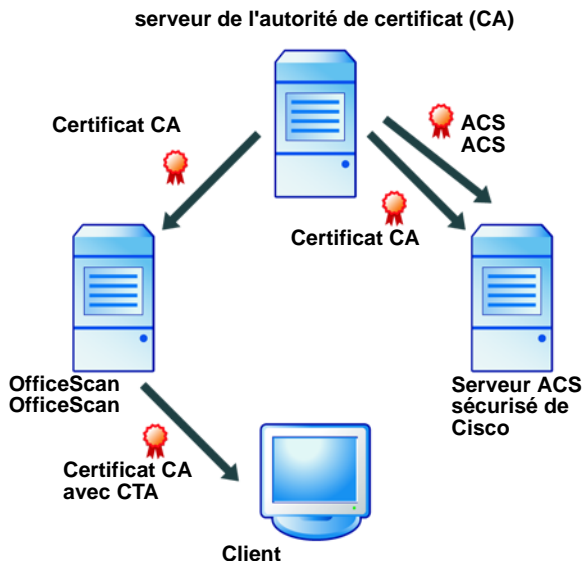


FIGURE A-4 Création et déploiement d'un certificat ACS et CA

1. Après l'émission par le serveur ACS d'une demande de signature de certificat au serveur CA, ce dernier émet un certificat (le certificat ACS). Vous pouvez alors installer le certificat ACS sur le serveur ACS. Le processus est décrit comme *Inscription du serveur ACS sécurisé de Cisco* : à la page B-4.
2. Le serveur CA exporte ensuite un certificat CA du serveur CA et l'installe et sur le serveur ACS. Consultez *Exporter et installer le certificat CA* à la page B-8 pour obtenir des instructions détaillées.
3. Enregistrez ensuite une copie de ce même certificat CA sur le serveur OfficeScan.
4. Le serveur OfficeScan déploie le certificat CA sur les clients avec le CTA. Consultez *Déploiement de Cisco Trust Agent* à la page B-13 pour obtenir des instructions détaillées.

Définition du certificat CA

Les clients OfficeScan avec des installations CTA procèdent à une authentification auprès du serveur ACS avant de communiquer l'état de sécurité du client. Il existe plusieurs méthodes d'authentification (consultez la documentation du serveur ACS sécurisé de Cisco pour obtenir plus de détails). Vous avez par exemple peut être déjà activé l'authentification de l'ordinateur pour le serveur ACS sécurisé de Cisco à l'aide de Windows Active Directory, que vous pouvez configurer afin de produire automatiquement un certificat client pour l'utilisateur final lorsqu'un nouvel ordinateur est ajouté dans le répertoire actif. Pour obtenir des instructions à ce sujet, consultez la base de connaissance Microsoft, article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows.

Pour les utilisateurs de réseau qui disposent de leur propre serveur d'autorité de certificat (CA), mais dont les clients utilisateurs finaux ne possèdent pas encore de certificats, OfficeScan prévoit un mécanisme destiné à distribuer un certificat racine aux clients OfficeScan. Distribuez le certificat pendant l'installation CTA (qui a lieu pendant l'installation d'OfficeScan) ou à partir de la console Web OfficeScan. OfficeScan distribue le certificat lorsqu'il déploie Cisco Trust Agent chez les clients (consultez *Déploiement de Cisco Trust Agent* à la page B-13).

Remarque : Si vous avez déjà acquis un certificat auprès d'une autorité de certificat ou si vous avez produit et distribué vos propres certificats aux clients utilisateurs finaux, il est inutile de recommencer.

Avant de distribuer le certificat aux clients, enregistrez le serveur ACS auprès du serveur CA et préparez le certificat (consultez *Inscription du serveur ACS sécurisé de Cisco* : à la page B-4).

Configuration minimale requise pour le serveur de stratégie

Voici la configuration minimale requise pour l'installation du serveur de stratégie et de Cisco Trust Agent (CTA).

Système d'exploitation

- Série Microsoft™ Windows™ NT (Service Pack 6a)
- Série Windows 2000 (Service Pack 2)
- Windows XP (Édition professionnelle uniquement, Service Pack 1)
- Windows Server 2003

Matériel

- Processeur Intel™ Pentium™ II 300 MHz ou équivalent
- 128 Mo de RAM
- 300 Mo d'espace disque disponible
- Écran avec résolution 800 x 600 pixels, 256 couleurs minimum
- Microsoft Internet Explorer 5.5 ou supérieur

Serveur Web

- Microsoft Internet Information Server (IIS)
 - sous Windows NT : version 4.0
 - sous Windows 2000 : version 5.0
 - sous Windows XP : version 5.1
 - sous Windows Server 2003 : version 6.0
- Serveur Web Apache 2.0 ou supérieur (pour Windows 2000/XP/Server 2003 uniquement)

Configuration minimale requise pour la console Web

Pour utiliser la console de management (Web) du serveur OfficeScan, il vous faut :

- Matériel :
 - Processeur Intel Pentium 133 MHz ou équivalent
 - 64 Mo de mémoire vive disponible

- 30 Mo d'espace disque disponible
- Écran avec résolution 800 x 600 pixels, 256 couleurs minimum
- Logiciels :
 - Microsoft Internet Explorer 5.5 ou supérieur

Configuration requise pour Cisco Trust Agent (CTA)

Le Cisco Trust Agent ne peut être installé que sur des ordinateurs équipés de Windows NT/2000/XP.

CTA sur Windows NT/2000

- Processeur Intel Pentium 150 MHz ou équivalent
- Microsoft Windows NT 4.0 avec SP6a ou supérieur, Windows 2000 Server/Advanced Server avec SP2 ou supérieur, Windows 2000 Pro avec SP 2 ou supérieur
- Windows Installer 2.0
- 128 Mo de RAM
- 80 Mo d'espace disque disponible

CTA sur Windows XP/Windows Server 2003

- Processeur Intel Pentium 300 MHz ou équivalent
- Microsoft Windows XP édition familiale ou professionnelle avec SP1
- 256 Mo de RAM
- 80 Mo d'espace disque disponible

Modèles de dispositifs Cisco acceptés

Voir le site Internet de Cisco NAC pour obtenir une liste des modèles de dispositifs acceptables :

www.cisco.com/go/nac

Déploiement du Policy Server pour Cisco NAC

La présente annexe décrit la manière dont il convient d'installer et de configurer le Policy Server pour Cisco Network Admission Control (NAC). Il comprend aussi des informations sur le déploiement de Cisco Trust Agent (CTA) et sur la création et le déploiement de certificats numériques utilisés entre les divers composants Cisco NAC. Avant de lire la présente annexe, il est préférable de vous familiariser avec l'Annexe A: Policy Server pour Cisco™ NAC Primer.

Les sujets évoqués dans la présente annexe sont entre autres :

- *Présentation générale du déploiement de Policy Server pour NAC* à la page B-2
- *Inscription du serveur ACS sécurisé de Cisco* : à la page B-4
- *Exporter et installer le certificat CA* à la page B-8
- *Préparation du certificat SSL du serveur de stratégie* à la page B-10
- *Déploiement de Cisco Trust Agent* à la page B-13
- *Installation du Policy Server pour Cisco NAC* à la page B-16
- *Configuration du serveur ACS* à la page B-19
- *Configuration du Policy Server pour Cisco NAC* à la page B-21

Remarque : Cette annexe comprend des instructions de base destinées à installer et configurer le Policy Server pour Cisco NAC. Pour obtenir de plus amples

informations au sujet de la configuration et de l'administration des serveurs ACS sécurisés de Cisco et autres produits Cisco, veuillez consulter la documentation Cisco la plus récente que vous trouverez sur le site Web suivant : <http://www.cisco.com/univercd/home/home.htm>

Présentation générale du déploiement de Policy Server pour NAC

Suivez la procédure ci-dessous pour déployer Policy Server pour Cisco NAC :

1. **Installez le serveur OfficeScan** : installez le serveur OfficeScan sur le réseau (consultez le *Guide de déploiement et d'installation*).
2. **Installez les clients OfficeScan** : installez le programme client OfficeScan sur tous les clients dont vous souhaitez estimer la protection antivirus à l'aide du serveur de stratégie (Consultez le *Guide de déploiement et d'installation*).
3. **Inscription du serveur ACS sécurisé de Cisco** : établit une relation fiable entre le serveur ACS et un serveur d'autorité de certification (CA) en demandant au serveur ACS d'émettre une demande de signature de certificat. Enregistrez ensuite le certificat CA signé (appelé certificat ACS) sur le serveur ACS (Consultez *Inscription du serveur ACS sécurisé de Cisco* : à la page B-4).
4. **Exportation et installation d'un certificat CA** : exporte le certificat CA vers le serveur ACS et enregistre une copie sur le serveur OfficeScan. Cette étape est uniquement nécessaire si vous n'avez pas déployé de certificat sur les clients et le serveur ACS (Consultez *Exporter et installer le certificat CA* à la page B-8).
5. **Déployer Cisco Trust Agent et le certificat CA** : déploie Cisco Trust Agent et le certificat CA sur tous les clients OfficeScan afin qu'ils puissent envoyer leur état de sécurité au serveur de stratégie (Consultez *Déploiement de Cisco Trust Agent* à la page B-13).
6. **Installer Policy Server pour Cisco NAC** : installe Policy Server pour Cisco NAC afin qu'il gère les requêtes envoyées par le serveur ACS (consultez *Installation du Policy Server pour Cisco NAC* à la page B-16).
7. **Exporter un certificat SSL depuis le serveur de stratégie** : exporte un certificat SSL du serveur de stratégie au serveur ACS Cisco afin d'établir une communication SSL sécurisée entre les deux serveurs (consultez *Installation du Policy Server pour Cisco NAC* à la page B-16).

8. **Configurer le serveur ACS** : configure le serveur ACS de manière à ce qu'il transmette les demandes de validation d'état au serveur de stratégie (consultez *Configuration du serveur ACS* à la page B-19).
9. **Configurez Policy Server pour Cisco NAC** : créez et modifiez des règles et des stratégies pour appliquer la stratégie de sécurité de votre entreprise aux clients OfficeScan (consultez *Configuration du Policy Server pour Cisco NAC* à la page B-21).

Remarque : Les procédures suivantes ne sont fournies que pour référence et peuvent varier en fonction des mises à jour ou de la présence d'interfaces Microsoft et/ou Cisco.

Avant d'effectuer l'une des tâches de la présente annexe, vérifiez que le ou les périphériques d'accès réseau de votre réseau prennent en charge Cisco NAC (consultez www.cisco.com/go/nac à la page A-20). Reportez-vous à la documentation de votre périphérique pour les instructions d'installation et de configuration. Installez également le serveur ACS sur votre réseau. Reportez-vous à la documentation relative au serveur ACS sécurisé de Cisco pour savoir comment procéder.

Inscription du serveur ACS sécurisé de Cisco :

Fait intervenir le serveur ACS sécurisé de Cisco auprès du serveur de l'autorité de certification (CA) afin d'établir une relation de confiance entre les deux serveurs. La procédure suivante est destinée aux utilisateurs qui fonctionnent avec un serveur d'autorité de certificat Windows afin de gérer les certificats sur le réseau. Si vous utilisez une autre application ou un autre service CA, consultez la documentation livrée par le fournisseur.

Pour faire intervenir le serveur ACS sécurisé de Cisco auprès d'un serveur d'autorité de certification Windows :

1. Générez une demande de signature de certificat auprès du serveur ACS sécurisé de Cisco :
 - a. Dans la barre de navigation de la console Web ACS, cliquez sur **System Configuration**.
 - b. Cliquez sur **ACS Certificate Setup**.
 - c. Cliquez sur **Generate Certificate Signing Request**. Le serveur ACS sécurisé de Cisco affiche le tableau **Generate new request** dans l'écran **Generate Certificate Signing Request**.
 - d. Dans la case **Certificate subject**, saisissez **cn=** suivi du nom que vous aimeriez utiliser en objet de ce certificat ACS, par exemple, **cn=ACSTrend**.
 - e. Dans la zone de texte **Private key file**, saisissez le chemin d'accès complet du répertoire et le nom du fichier dans lequel la clé privée est enregistrée, par exemple, **c:\privateKeyFile.pem**.
 - f. Dans la zone de texte **Private key password**, saisissez un nouveau mot de passe qui sera utilisé comme mot de passe de la clé privée et saisissez-le de nouveau dans le champ **Retype private key password**.
 - g. A partir de la liste **Key length**, sélectionnez la longueur de la clé qui doit être utilisée. Les choix de longueur de clé sont 512 ou 1024 (valeur par défaut) bits.
 - h. Dans la liste **Digest to sign with**, sélectionnez l'assimilation (ou algorithme arbitraire). Les choix de signature avec Digest sont MD2, MD5, SHA et SHA1 (par défaut).

- i. Cliquez alors sur **Envoyer**. Le serveur ACS sécurisé de Cisco affiche une demande de signature de certificat (CSR) dans la zone d'affichage, à droite, sous une bannière qui affiche le message suivant :

« Now your certificate signing request is ready. You can copy and paste it into any certification authority enrollment tool. »
2. Utilisez un outil d'inscription auprès d'une autorité de certification telle que Windows 2000 Server Certification Authority, pour signer le certificat :
 - a. Vérifiez que Certificate Services Web Enrollment Support soit installé sur le serveur Windows 2000 que vous utilisez pour le service des demandes de certificat.
 - b. Saisissez ce qui suit : `http:// {CA_Server} /certsrv/`, où `{CA_Server}` est l'adresse Web du serveur Windows 2000 que vous utilisez afin d'assurer le service des demandes de certificat. L'écran de **Bienvenue** Microsoft Certificate Services apparaît.
 - c. Cliquez sur **Request a Certificate** et cliquez sur **Suivant >**. L'écran **Choose Request Type** apparaît.
 - d. Cliquez sur **Advanced request** et cliquez sur **Suivant >**. L'écran **Advanced Certificate Requests** apparaît.
 - e. Cliquez sur **Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**, puis cliquez sur **Suivant**. L'écran **Submit a Saved Request** apparaît.
 - f. Si le serveur CA est installé sur un ordinateur équipé Active Directory, sélectionnez **Serveur Web** à côté de **Certificate Template**.
 - g. Copiez le CSR depuis l'écran du serveur ACS sécurisé de Cisco et collez-le dans le champ **Demandes enregistrées**.
 - h. Cliquez alors sur **Envoyer >**. Le serveur de certificat enregistre la demande.
3. Émettez la demande de certificat depuis le serveur CA :

Remarque : Si votre serveur CA est configuré de manière à émettre des certificats automatiquement, à la demande, passez à l'étape suivante.

- a. Sur le serveur CA qui traite la requête, cliquez sur **Démarrer > Exécuter**. L'écran **Exécuter** apparaît.

- b. Saisissez **mmc** dans le champ **Ouvrir**. Un nouvel écran de console Web s'ouvre.
 - c. Cliquez sur **Console > Add/Remove Snap-in**. L'écran **Add/Remove Snap-in** apparaît.
 - d. Cliquez sur **Ajouter**. L'écran **Add Standalone Snap-in** apparaît.
 - e. Cliquez sur **Autorité de certificat** et cliquez sur **Ajouter**. L'écran **Autorité de certification** apparaît.
 - f. Cliquez sur **Ordinateur local** et cliquez sur **Terminer**.
 - g. Cliquez sur **Fermer** pour fermer l'écran **Add Standalone Snap-in**.
 - h. Cliquez sur **OK** pour fermer l'écran **Add Standalone Snap-in**.
 - i. Dans l'arborescence de la console, cliquez sur **Autorité de certification > {local certification authority}/Pending Requests**, où {local certification authority} est le nom que vous avez attribué au serveur de l'autorité de certification pendant l'installation.
 - j. Cliquez avec le bouton droit de la souris sur la requête, puis cliquez sur **Émission**.
4. Téléchargez le certificat CA à partir de la page Web Microsoft Certificate Services.
- a. Ouvrez de nouveau la page Web Microsoft Certificate Services à partir du serveur ACS (consultez Étape b à la page B-5).
 - b. Cliquez sur **Check on pending certificate**.
 - c. Cliquez sur la demande de certificat et cliquez sur **Suivant**.
 - d. Cliquez sur **DER encoded** puis cliquez sur **Download CA certificate**.
L'écran de téléchargement du fichier apparaît, accompagné d'un avertissement de sécurité.
 - e. Cliquez sur **Enregistrer**.
 - f. Enregistrez le certificat à un emplacement sur le disque dur local du serveur ACS.
5. Installez le certificat signé sur le serveur ACS.
- a. Ouvrez la console de gestion Cisco Secure ACS.
 - b. Dans la barre de navigation, cliquez sur **System Configuration**.

- c. Cliquez sur **ACS Certificate Setup**.
- d. Cliquez sur **Install ACS Certificate**. Cisco Secure ACS affiche l'écran **Install ACS Certificate**.
- e. Sélectionnez **Read certificate from file**, puis saisissez le chemin d'accès complet du répertoire et le nom de fichier de certificat dans la zone de texte **Fichier certificat**.
- f. Dans la zone de texte **Private key file**, saisissez le chemin d'accès complet du répertoire et le nom du fichier qui contient la clé privée.
- g. Dans la zone de texte **Private key password**, saisissez le mot de passe de la clé privée.

Remarque : Il s'agit de la valeur que vous avez saisie dans **Private key password** dans la page **Generate Certificate Signing Request** (consultez *Inscription du serveur ACS sécurisé de Cisco* : à la page B-4).

- h. Cliquez alors sur **Soumission**.
6. Relancez le serveur ACS :
- a. Cliquez sur **Configuration système > Contrôle de service**.
 - b. Cliquez sur **Redémarrer**.

Exporter et installer le certificat CA

Le client OfficeScan s'authentifie auprès du serveur ACS avant d'envoyer les données de l'état de sécurité. Le certificat CA est nécessaire pour que cette authentification puisse avoir lieu. Commencez par exporter le certificat CA du serveur CA vers les serveurs ACS et OfficeScan. Ensuite, lorsque vous créez la compression de déploiement de l'agent CTA, le certificat CA est inclus (consultez [Définition du certificat CA](#) à la page A-18 et [Déploiement de Cisco Trust Agent](#) à la page B-13).

Exécutez les opérations suivantes pour exporter et installer le certificat CA.

- Exportez le certificat CA depuis le serveur de l'autorité de certificat
- Installez-le sur le serveur Cisco ACS sécurisé
- Enregistrez une copie sur le serveur OfficeScan

Remarque : La procédure suivante est destinée aux utilisateurs qui fonctionnent avec un serveur d'autorité de certificat Windows afin de gérer les certificats sur le réseau. Si vous utilisez une autre application ou un autre service d'autorité de certification, consultez la documentation livrée par le fournisseur.

Pour exporter et installer un certificat CA en vue de la distribution :

1. Exportez le certificat depuis le serveur de l'autorité de certification (CA) :
 - a. Sur le serveur CA, cliquez sur **Démarrer > Exécuter**. L'écran **Exécuter** apparaît.
 - b. Saisissez **mmc** dans le champ **Ouvrir**. Un nouvel écran de console de management s'ouvre.
 - c. Cliquez sur **Fichier > Add/Remove Snap-in**. L'écran **Add/Remove Snap-in** apparaît.
 - d. Cliquez sur **Certificats** et cliquez sur **Ajouter**. L'écran **Certificates snap-in** apparaît.
 - e. Cliquez sur **Computer Account** et cliquez sur **Next >**. L'écran **Select Computer** apparaît.
 - f. Cliquez sur **Ordinateur local** et cliquez sur **Terminer**.

- g. Cliquez sur **Fermer** pour fermer l'écran **Add Standalone Snap-in**.
 - h. Cliquez sur **OK** pour fermer l'écran **Add Standalone Snap-in**.
 - i. Dans l'arborescence de la console, cliquez sur **Certificats > Trusted Root > Certificats**.
 - j. Dans la liste, sélectionnez le certificat que vous distribuerez aux clients et le serveur ACS.
 - k. Cliquez sur **Action > Toutes les tâches > Exporter...** Le Certificate Export Wizard s'ouvre.
 - l. Cliquez sur **Suivant >**.
 - m. Cliquez sur **DER encoded binary x.509** puis cliquez sur **Suivant >**.
 - n. Saisissez un nom de fichier et naviguez vers un répertoire dans lequel le certificat sera exporté.
 - o. Cliquez sur **Suivant >**.
 - p. Cliquez sur **Terminer**. Une fenêtre de confirmation apparaît.
 - q. Cliquez sur **OK**.
2. Installez le certificat sur le serveur Cisco ACS sécurisé
- a. Cliquez sur **Configuration système > ACS Certificate Setup > ACS Certification Authority Setup**.
 - b. Saisissez le chemin d'accès complet et le nom du fichier du certificat dans le champ **CA certificate file**.
 - c. Cliquez alors sur **Soumission**. Cisco Secure ACS vous invite à redémarrer le service.
 - d. Cliquez sur **Configuration système > Contrôle de service**.
 - e. Cliquez sur **Redémarrer**. Cisco Secure ACS redémarre.
 - f. Cliquez sur **Configuration système > ACS Certificate Management > Edit Certificate Trust List**. L'écran **Edit Certificate Trust List** apparaît.
 - g. Cochez la case correspondant au certificat importé lors de l'installation b. et cliquez sur **Envoyer**. Le serveur ACS sécurisé de Cisco vous invite à redémarrer le service.
 - h. Cliquez sur **Configuration système > Contrôle de service**.
 - i. Cliquez sur **Redémarrer**. Cisco Secure ACS redémarre.

3. Copiez le certificat (fichier .CER) sur l'ordinateur sur lequel le serveur OfficeScan est installé, vous pourrez ainsi le déployer vers le client avec le CTA (consultez *Déploiement de Cisco Trust Agent* à la page B-13 pour obtenir de plus amples informations).

Remarque : Enregistrez le certificat sur un lecteur local ; les lecteurs mappés ne sont pas acceptés.

Préparation du certificat SSL du serveur de stratégie

Pour établir une connexion SSL sécurisée entre le serveur ACS et le serveur de stratégie, préparez un certificat spécialement conçu pour être utilisé avec SSL. Le programme d'installation du serveur de stratégie génère automatiquement le certificat SSL.

Pour préparer le certificat du serveur de stratégie SSL en vue de la distribution :

1. Exportez le certificat depuis Certification Store sur mmc :
 - **Si le serveur de stratégie fonctionne sur IIS :**
 - a. Sur le serveur de stratégie, cliquez sur **Démarrer > Exécuter**. L'écran **Exécuter** apparaît.
 - b. Saisissez **mmc** dans le champ **Ouvrir**. Un nouvel écran de console de management s'ouvre.
 - c. Cliquez sur **Console > Add/Remove Snap-in**. L'écran **Add/Remove Snap-in** apparaît.
 - d. Cliquez sur **Ajouter**. L'écran **Add Standalone Snap-ins** apparaît.
 - e. Cliquez sur **Certificats** et cliquez sur **Ajouter**. L'écran **Certificates snap-in** apparaît.
 - f. Cliquez sur **Computer Account** et cliquez sur **Next >**. L'écran **Select Computer** apparaît.
 - g. Cliquez sur **Ordinateur local** et cliquez sur **Terminer**.
 - h. Cliquez sur **Fermer** pour fermer l'écran **Add Standalone Snap-in**.

- i. Cliquez sur **OK** pour fermer l'écran **Add Standalone Snap-in**.
- j. Dans l'arborescence de la console, cliquez sur **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
- k. Sélectionnez le certificat dans la liste :

Remarque : Vérifiez le certificat d'emprunte en double cliquant sur le certificat, puis en sélectionnant **Propriétés**. L'emprunte doit être la même que celle du certificat qui se trouve dans la console IIS.

Pour vérifier, ouvrez la console IIS et cliquez avec le bouton de droite sur **site Web virtuel** ou sur le **site Web par défaut** (selon le site Web sur lequel vous avez installé le serveur de stratégie) puis sélectionnez **Propriétés**. Cliquez sur **Directory Security**, puis cliquez sur **Afficher Certificat** pour consulter les détails du certificat, et ce y compris l'empreinte.

- l. Cliquez sur **Action > Toutes les tâches > Exporter...** Le Certificate Export Wizard s'ouvre.
 - m. Cliquez sur **Suivant >**.
 - n. Cliquez sur **DER encoded binary x.509** ou **Base 64 encoded X.509** puis cliquez sur **Suivant >**.
 - o. Saisissez un nom de fichier et naviguez vers un répertoire dans lequel le certificat sera exporté.
 - p. Cliquez sur **Suivant >**.
 - q. Cliquez sur **Terminer**. Une fenêtre de confirmation apparaît.
 - r. Cliquez sur **OK**.
- **Si le serveur de stratégie fonctionne sous Apache 2.0 :**
 - a. Obtenez le fichier certificat `server.cert`. L'endroit où se trouve le fichier dépend du serveur OfficeScan du serveur de stratégie, que vous avez installé en premier lieu :
 - Si vous avez installé le serveur OfficeScan avant d'installer le serveur de stratégie, le fichier se trouve dans le répertoire suivant :
`C:\Programmes\Trend Micro\OfficeScan\PCSRV\Private\certificate`

- Si vous avez installé le serveur de stratégie avant d'installer le serveur OfficeScan, le fichier se trouve dans le répertoire suivant :
C:\Programmes\Trend Micro\OfficeScan\PolicyServer\
Private\certificate
 - b. Copiez le fichier certificat sur le serveur ACS.
2. Installez le certificat sur le serveur Cisco ACS sécurisé
- a. Sur la console Web ACS, cliquez sur **Configuration système > ACS Certificate Setup > ACS Certification Authority Setup**.
 - b. Saisissez le chemin d'accès complet et le nom du fichier du certificat dans le champ **CA certificate file**.
 - c. Cliquez alors sur **Soumission**. Cisco Secure ACS vous invite à redémarrer le service.
 - d. Cliquez sur **Configuration système > Contrôle de service**.
 - e. Cliquez sur **Redémarrer**. Cisco Secure ACS redémarre.

Déploiement de Cisco Trust Agent

Le Cisco Trust Agent (CTA) permet la communication entre les clients OfficeScan et les périphériques d'accès réseau qui prennent en charge Cisco NAC. Lorsque vous avez installé et déployé le serveur OfficeScan et les clients OfficeScan, déployez le CTA chez les clients OfficeScan à partir de la console Web. Le logiciel de déploiement de CTA contient le certificat CA que vous avez enregistré sur le serveur OfficeScan (consultez [Exporter et installer le certificat CA](#) à la page B-8).

Remarque : Installez le client Windows Installer 2.0 pour NT 4.0 chez les clients avant de déployer l'agent.

Pour déployer le CTA sur les clients de la console Web d'OfficeScan.

1. Ouvrez la console Web du serveur OfficeScan.
2. Effectuez l'une des actions suivantes :
 - Si vous avez déjà distribué des certificats aux clients, passez à Étape 3
 - Si vous n'avez pas encore distribué les certificats aux clients, procédez comme suit :
 - i. Cliquez sur **Certificat du client**, l'écran **Importation du certificat client** apparaît.
 - ii. Saisissez le chemin d'accès complet et le nom du fichier du certificat CA enregistré sur le serveur. Pour obtenir des instructions sur la préparation d'un certificat CA, consultez [Exporter et installer le certificat CA](#) à la page B-8.
 - iii. Cliquez sur **Importer**. Les informations sur le certificat s'affichent.

Remarque : Si vous n'avez pas accepté les conditions du contrat de licence Cisco lors de l'installation du serveur OfficeScan, il vous est impossible de déployer l'agent. Lorsque vous cliquez sur **Déploiement de l'agent**, les informations relatives à la licence apparaissent de nouveau. Lisez attentivement le contrat de licence puis cliquez sur **Oui** pour confirmer votre acceptation.

3. Cliquez sur **Déploiement de l'agent** dans le menu. L'arborescence client apparaît.
4. Sélectionnez les clients ou domaines dans lesquels déployer le CTA, puis cliquez sur **Déploiement de l'agent** dans la barre latérale. L'écran **Installation / Désinstallation de l'agent** apparaît.
5. Cliquez sur **Installer / Mettre à niveau Cisco Trust Agent** puis cliquez sur **Enregistrer**. La page **Définir l'installation de CTA** apparaît.
6. Cliquez sur **Fermer**.

Remarque : Si le client chez qui l'agent est déployé n'est pas connecté lorsque vous cliquez sur **Install Cisco Trust Agent**, OfficeScan remplit automatiquement la demande de déploiement lorsque le client se connecte.

Si vous avez déjà préparé un certificat CA avant d'installer le serveur OfficeScan, il existe une option de déploiement de l'agent CTA pendant l'installation du serveur OfficeScan à l'aide de l'installateur principal.

Pour déployer CTA sur les clients à l'aide du programme d'installation principal du serveur OfficeScan :

1. Pendant l'installation du serveur OfficeScan, l'écran **Sélection des composants** du programme d'installation principal du serveur OfficeScan apparaît. Pour obtenir des instructions sur l'utilisation du programme d'installation principal du serveur OfficeScan, consultez le *Guide de déploiement et d'installation*.
2. Cochez la case **Activer le déploiement de l'agent pour Cisco NAC**.
3. Effectuez l'une des actions suivantes :
 - Si vous avez déjà distribué des certificats aux clients utilisateurs finaux de Cisco Secure NAC, cliquez sur **Suivant>**.
 - Si vous devez distribuer des certificats aux clients :
 - i. Cliquez sur **Importer certificat**. Un navigateur apparaît.
 - ii. Sélectionnez le fichier de certificat préparé dans le navigateur, puis cliquez sur **OK**. Pour obtenir des instructions sur la préparation d'un fichier certificat, consultez la rubrique *Exporter et installer le certificat CA* à la page B-8.
 - iii. Cliquez sur **Suivant >**.
4. Poursuivez l'installation principale du serveur OfficeScan.

Mise à niveau et déploiement de Cisco Trust Agent 2.0

Si vous disposez de la version 4.0 ou supérieur du serveur Access Control Server (ACS) Cisco NAC, vous devez procéder à une mise à niveau de l'agent Cisco Trust Agent vers la version 2.0. Une fois l'agent mis à niveau, vous ne pouvez pas revenir à la version précédente.

Pour mettre à niveau l'agent :

1. Dans la barre latérale, cliquez sur **Cisco NAC**.
2. Cliquez sur **Mise à niveau de l'agent**.
3. Cliquez sur **Mise à niveau**. Le serveur OfficeScan procède à la mise à niveau de l'agent vers la version 2.0 sur le serveur.
4. Cliquez sur **Déploiement de l'agent** dans la barre latérale.
5. Cliquez sur **Installer/Mettre à niveau Cisco Trust Agent** pour déployer manuellement l'agent vers vos clients OfficeScan.
6. Cliquez sur **Enregistrer** pour enregistrer vos paramètres sans déployer l'agent ou sur **Appliquer à tous** pour déployer l'agent.

Vérification de l'installation de Cisco Trust Agent

Lorsque vous avez déployé le CTA chez les clients, vérifiez si l'installation a réussi en consultant l'arborescence des clients. L'arborescence des clients contient une colonne intitulée **Programme CTA**, qui apparaît dans les aperçus **Mise à jour**, **Afficher tout** ou **Antivirus**. Les installations de CTA qui ont réussi contiennent un numéro de version du programme CTA.

Vous pouvez également vérifier si le processus CTAD . EXE s'exécute sur l'ordinateur client.

Installation du Policy Server pour Cisco NAC

Il existe deux façons d'installer le serveur de stratégie :

- L'installateur du serveur de stratégie sur le CD version Entreprise
- Le programme d'installation principal du serveur OfficeScan (installe à la fois le serveur OfficeScan et le serveur de stratégie sur un même ordinateur)

Remarque : Le programme d'installation principal installe à la fois le serveur OfficeScan et la console Web du serveur de stratégie sur un serveur Web que vous précisez : IIS ou Apache. Si le programme d'installation ne trouve pas de serveur Apache sur le système ou si la version du serveur Apache installée n'est pas au minimum la version 2.0 ou supérieure, il installe automatiquement Apache version 2.0.52.

Le serveur ACS, le serveur de stratégie et le serveur OfficeScan doivent se trouver sur le même segment de réseau pour garantir une communication efficace.

AVERTISSEMENT ! Avant d'installer le serveur Web Apache, consultez le site Web Apache pour obtenir les informations les plus récentes sur les mises à niveaux, les correctifs et les problèmes de sécurité : www.apache.org.

Pour installer le Policy Server pour Cisco NAC, utilisez le programme d'installation du serveur de stratégie :

1. Connectez l'ordinateur sur lequel vous souhaitez installer le Policy Server pour Cisco NAC.
2. Placez le logiciel d'installation du Policy Server pour Cisco NAC qui se trouve sur le CD – version Entreprise.
3. Double-cliquez sur `setup.exe` pour installer le programme d'installation.
4. Suivez les instructions d'installation.

Vous pouvez aussi installer le serveur de stratégie sur le même ordinateur que le serveur OfficeScan.

Pour installer Policy Server pour Cisco NAC à partir de l'installateur principal OfficeScan :

1. Pendant l'installation du serveur OfficeScan, l'écran **Sélection des composants** du programme d'installation principal du serveur OfficeScan apparaît. Pour obtenir des instructions sur l'utilisation du programme d'installation principal du serveur OfficeScan, consultez le *Guide de déploiement et d'installation* et l'aide du programme d'installation.
2. Cochez la case **Installer le serveur Policy Server pour Cisco NAC**.
3. Cliquez sur **Suivant >**.
4. Poursuivez l'installation principale du serveur OfficeScan.
5. Lorsque l'écran Bienvenue pour Trend Micro Policy Server pour Cisco NAC apparaît, cliquez sur **Suivant >**. L'écran **Contrat de licence du Policy Server pour Cisco NAC** apparaît.
6. Lisez le contrat et cliquez sur **OK** pour continuer. L'écran **Choisir l'emplacement de destination** apparaît.
7. Si nécessaire, modifiez l'emplacement de destination par défaut en cliquant sur **Parcourir...** et sélectionnez une nouvelle destination pour l'installation du serveur de stratégie.
8. Cliquez sur **Suivant >**. L'écran **Serveur Web** apparaît.
9. Sélectionnez le serveur Web pour le serveur de stratégie :
 - **Serveur IIS** : cliquez ici pour installer sur un serveur Web IIS existant.
 - **Serveur Apache 2.0** : cliquez ici pour installer sur un serveur Web Apache 2.0.
10. Cliquez sur **Suivant >**. L'écran **Configuration du Serveur Web** apparaît.
11. Configurez les informations suivantes :
 - Si vous avez choisi d'installer le serveur de stratégie sur un serveur IIS, sélectionnez l'une des options suivantes :
 - **Site Web IIS par défaut** : cliquez ici pour installer par défaut en tant que site Web IIS.
 - **Site Web IIS virtuel** : cliquez ici pour installer en tant que site Web IIS virtuel.

- À côté de **Port**, saisissez un port qui sera utilisé en tant que port d'écoute du serveur.

Remarque : Si le serveur de stratégie et le serveur OfficeScan sont installés sur le même ordinateur et le même serveur Web, les numéros de ports sont les suivants :

serveur Web Apache /IIS sur le site Web par défaut : le serveur de stratégie et le serveur OfficeScan partagent le même port

Tous deux sur le serveur Web IIS sur le site Web virtuel : le port d'écoute par défaut du serveur de stratégie est le port 8081 et le port SSL est le 4344. Le port d'écoute par défaut du serveur OfficeScan est le 8080 et son port SSL est le 4343.

- Si vous installez le serveur de stratégie sur un serveur IIS, vous avez également la possibilité d'activer la sécurité Secured Socket Layer (SSL). Cochez la case Activer SSL. Saisissez le nombre d'années durant lesquelles le certificat SSL sera valide (par défaut, 3 ans) et un numéro de port SSL. Si vous activez SSL, ce numéro de port servira de port d'écoute du serveur. L'adresse du serveur de stratégies se présentera comme suit :

`https://{nom_serveur_stratégie}:{numéro port} ou`

`https://{nom_serveur_stratégie}:{numéro port} (si vous activez SSL)`

12. Cliquez sur **Suivant**. L'écran **Installation terminée** apparaît.
13. Vous avez terminé l'installation de votre serveur de stratégie. Cliquez sur **Terminer**.

Le programme d'installation principal du serveur OfficeScan va se poursuivre.

Remarque : Si vous effectuez la mise à jour à partir d'une version précédente d'OfficeScan, le programme d'installation principal procède à la mise à niveau vers OfficeScan 7,0 et installe le serveur de stratégie (si vous spécifiez son installation).

Configuration du serveur ACS

Pour permettre à Cisco Secure ACS de transmettre des demandes d'authentification au Policy Server pour Cisco NAC, ajoutez le Policy Server pour Cisco NAC dans **External Policies** pour que la base de données de l'utilisateur externe utilise l'authentification.

Remarque : Vous pouvez configurer le serveur ACS pour qu'il exécute des fonctions telles que le blocage de l'accès des clients au réseau. Ces fonctions ACS ne font pas partie du champ d'action de Policy Server pour Cisco NAC et ne sont donc pas reprises dans cette documentation. Pour obtenir des détails sur la configuration des autres fonctions ACS, consultez votre documentation ACS.

Pour configurer le serveur ACS afin de l'utiliser avec le Policy Server pour Cisco NAC :

1. Ouvrez la console de gestion Cisco Secure ACS.
2. Cliquez sur **Bases de données utilisateur externe > Configuration de la base de données > Network Admission Control**.
3. Dans **External User Database Configuration**, cliquez sur **Configurer**. L'écran **Network Admission Control Expected Host Configuration** apparaît.
4. Dans **Credential Validation Policies**, cliquez sur **External Policies**. L'écran **Select External Policies** apparaît.
5. Cliquez sur **New External Policy**. L'écran **External Policy Configuration** apparaît.
6. Saisissez un **Nom** et une **Description** pour le serveur de stratégie externe.
7. Cochez la case **Primary Server Configuration** et saisissez l'URL suivant du serveur de stratégie dans le champ URL :

```
https://{IP_serveur_stratégie}:{Numéro_port}/antibody/
cgi-bin/PostureRequest.dll?PostureRequest
```

Par exemple :

```
https://192.168.16.134:4343/antibody/cgi-bin/
PostureRequest.dll?PostureRequest
```

8. Saisissez respectivement dans les champs **Nom d'utilisateur** et **Mot de passe**, le nom d'utilisateur et le mot de passe que vous avez précisés sous **Connexion ACS** pendant l'installation du serveur de stratégie.
9. Sélectionnez le certificat SSL du serveur de stratégie que vous avez préparé. Pour plus d'informations sur le certificat, consultez la rubrique *Préparation du certificat SSL du serveur de stratégie* à la page B-10.
10. Dans **Forwarding Credential Types**, sélectionnez **Trend : AV** dans la liste **Available Credentials** et cliquez dessus ->. **Trend : AV** apparaît dans la liste **Selected Credentials**.
11. Cliquez alors sur **Soumission**. L'écran **Select External Policies** apparaît, il porte le nom du serveur de stratégie répertorié dans la liste **Available Policies**.
12. Cliquez sur le nom du serveur de stratégie externe dans la liste **Available Policies** et cliquez dessus ->. Le serveur de stratégie apparaît dans la liste **Stratégies sélectionnées**.
13. Cliquez alors sur **Soumission**. Le nom de votre stratégie externe apparaît dans le tableau **Credential Validation Policies**.

Configuration du Policy Server pour Cisco NAC

Lorsque OfficeScan et le serveur de stratégie est installé et que le client OfficeScan et le Trust Agent Cisco sont déployés, configurez le Policy Server pour Cisco NAC. Pour configurer un serveur de stratégie, accédez à la console Web du serveur de stratégies par l'intermédiaire de l'option **Serveurs de stratégie** dans la console Web.

Ce chapitre décrit les aspects suivants de la configuration du serveur de stratégie :

- *Ajout et suppression de serveurs de stratégie* démarrage à la page B-22 décrit comment gérer les serveurs de stratégie sur une console Web OfficeScan
- *Consultez le résumé des informations d'un serveur de stratégie* démarrage à la page B-23 vous montre comment obtenir un aperçu des serveurs de stratégie de votre réseau
- *Ajout ou modification de serveurs OfficeScan* démarrage à la page B-26 est la première étape de la configuration des serveurs de stratégie
- *Configuration des règles* démarrage à la page B-28 vous montre comment créer et modifier des règles qui contiennent des stratégies
- *Configuration des stratégies* démarrage à la page B-30 vous montre comment créer et modifier des stratégies qui déterminent comment le serveur de stratégie mesure l'état de sécurité du client
- *Utilisation des journaux de validation du client* démarrage à la page B-33 donne un aperçu de la manière dont vous pouvez utiliser des journaux pour comprendre l'état de sécurité des clients de votre réseau
- *Exécution des tâches d'administration* démarrage à la page B-35 décrit comment modifier le mot de passe du serveur de stratégie et comment établir un programme de synchronisation

Ajout et suppression de serveurs de stratégie

La première étape de la configuration des serveurs de stratégies consiste à ajouter les serveurs de stratégie installés sur le serveur OfficeScan. Vous pouvez ainsi ouvrir la console Web du serveur de stratégie à partir de la console Web d'OfficeScan. L'écran **Serveurs de stratégies** affiche tous les serveurs de stratégie déjà installés sur votre réseau. Vous pouvez y ajouter ou y supprimer des serveurs de stratégies.

Pour ajouter un serveur de stratégie :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste des serveurs de stratégies.
2. Cliquez sur **Ajouter**. L'écran **Serveurs de stratégie** apparaît.
3. Saisissez l'adresse complète du serveur de stratégie et le numéro de port utilisé par le serveur pour les communications HTTPS (par exemple : `https://policy-server:4343/`). Saisissez également la description du serveur (facultatif).
4. Saisissez un mot de passe à utiliser lorsque vous vous connectez à la console de gestion du serveur de stratégie et confirmez-le.
5. Cliquez sur **Ajouter**.

Pour supprimer un serveur de stratégies :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste des serveurs de stratégies.
2. Cochez la case du serveur de stratégies à supprimer.
3. Cliquez sur **Supprimer**.

Remarque : Pour valider tous les clients de votre réseau, ajoutez tous les serveurs OfficeScan à au moins un serveur de stratégie.

Consultez le résumé des informations d'un serveur de stratégie

L'écran **Résumé** contient des informations à propos du serveur de stratégie, y compris les paramètres de configuration des stratégies et des règles, les journaux de validation des clients et les serveurs OfficeScan enregistrés sur un serveur de stratégie.

L'adresse IP et le numéro de port du serveur de politique pour Cisco NAC apparaissent dans le haut de l'écran **Résumé**.

Le tableau **Résumé de configuration** affiche le nombre de serveurs OfficeScan enregistrés sur le serveur de stratégie, les stratégies du serveur de stratégie et les règles qui composent les stratégies.

Pour voir et modifier les détails du résumé de la configuration d'un serveur de stratégie :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste des serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations. L'écran **Résumé** apparaît ; il affiche le tableau **Résumé de la configuration**.
3. Cliquez sur le lien à côté de l'élément dont vous souhaitez consulter les paramètres de configuration :
 - **Serveur(s) OfficeScan enregistré(s)** : le serveur OfficeScan actuellement sur le réseau
 - **Stratégies** : stratégies du serveur de stratégie utilisables par les serveurs OfficeScan enregistrés
 - **Règle(s)** : règles du serveur de stratégie composant les stratégies

Si vous souhaitez appliquer les mêmes paramètres à plusieurs serveurs de stratégie de votre réseau, y compris des règles et des stratégies identiques, exportez-les d'un serveur et importez-les dans les autres.

Conseil : Trend Micro conseille de configurer les mêmes paramètres sur tous les serveurs de stratégie de votre réseau pour assurer la cohérence de la stratégie antivirus.

Pour exporter les paramètres de configuration du serveur de stratégie :

1. Cliquez sur **Cisco NAC > Serveurs de stratégie** dans la barre latérale. L'écran **Serveurs de stratégies** apparaît et affiche la liste de tous les serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations. L'écran **Résumé** apparaît ; il affiche le tableau **Résumé de la configuration**.
3. Cliquez sur **Exporter**.
4. Cliquez sur **Enregistrer** et sélectionnez une destination.

Remarque : Les paramètres de configuration du serveur de stratégie sont enregistrés sous forme de fichier binaire avec l'extension .dat.

Pour importer les paramètres de configuration du serveur de stratégie :

1. Cliquez sur **Cisco NAC > Serveurs de stratégie** dans la barre latérale. L'écran **Serveurs de stratégies** apparaît et affiche la liste de tous les serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations. L'écran **Résumé** apparaît ; il affiche le tableau **Résumé de la configuration**.
3. Cliquez sur **Importer**. L'écran **Résumé – Configurations de l'importation** apparaît.
4. Cliquez sur **Parcourir** et sélectionnez l'emplacement d'origine du fichier de configuration à importer.
5. Cliquez sur **Importer**. Les paramètres du fichier s'affichent.
6. Cliquez sur **Enregistrer**.

Le tableau **Journaux de validation du client** possède un lien vers le journal de validation actuel, enregistré sous forme de fichier .CSV.

Pour afficher le journal de validation actuel :

- Cliquez sur **Afficher le journal de validation actuel**. Le journal s'ouvre dans le tableau par défaut des fichiers .CSV de votre ordinateur.

Le tableau **Serveurs OfficeScan enregistrés** affiche une liste en lecture seule des adresses IP des serveurs OfficeScan enregistrés sur votre réseau, de la date de la dernière synchronisation, de la version actuelle du fichier des signatures de virus et de la dernière date de mise à jour, ainsi que la version actuelle du moteur de scan.

Pour synchroniser le serveur de stratégie aux serveurs OfficeScan enregistrés :

- Cliquez sur **Synchroniser avec OfficeScan**. L'écran **Résumé – Résultats de la synchronisation** apparaît, contenant les informations suivantes en lecture seule :
Nom du serveur OfficeScan : nom de l'hôte ou adresse IP des serveurs OfficeScan enregistrés.

Résultat de la synchronisation : réussite ou échec de la synchronisation.

Dernière synchronisation : date de la dernière synchronisation réussie.

Pour plus d'informations sur la synchronisation, consultez la rubrique *Définition de la synchronisation* à la page A-16.

Ajout ou modification de serveurs OfficeScan

Enregistrez le serveur de stratégie au moins sur un serveur OfficeScan pour que le serveur de stratégie puisse recevoir les fichiers de signatures de virus et les informations relatives à la version du moteur de scan (consultez Figure A-2 pour obtenir des informations sur le rôle que le serveur OfficeScan joue dans le processus de validation).

Remarque : Pour que le serveur de stratégie valide tous les clients de votre réseau, ajoutez tous les serveurs OfficeScan à au moins un serveur de stratégie.

Ajoutez un nouveau serveur OfficeScan ou modifiez les paramètres d'un serveur OfficeScan existant sur l'écran **Serveurs OfficeScan**.

Pour ajouter ou modifier un serveur OfficeScan :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste des serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations. L'écran **Résumé** correspondant s'affiche. Choisissez l'une des méthodes suivantes pour accéder à l'écran **Ajout d'un serveur OfficeScan** :
 - Dans l'écran **Résumé** cliquez sur le lien correspondant au nombre de serveur(s) OfficeScan enregistré(s).
 - Cliquez sur **Configurations > Serveurs OfficeScan** dans la barre latérale. L'écran **Serveur OfficeScan** apparaît.
3. Pour ajouter un serveur :
 - Cliquez sur **Ajouter**. L'écran **Ajout d'un serveur OfficeScan** apparaît.Pour modifier les informations relatives à un serveur existant :
 - Cliquez sur le nom d'un serveur OfficeScan à modifier. L'écran **Mettre à jour serveur OfficeScan** apparaît.
4. A côté de **Adresse du serveur OfficeScan**, tapez l'adresse IP, le nom de serveur ou le nom de domaine complet (FQDN) du serveur que vous souhaitez ajouter.

5. A côté de **Numéro de port HTTP**, tapez le numéro du port qu'utilise le serveur OfficeScan pour la communication HTTP.

Remarque : Tapez le port serveur HTTP que vous avez configuré pendant l'installation du serveur OfficeScan (par défaut : 8080). Ce n'est PAS le port utilisé pour la communication HTTPS (si vous utilisez SSL). Pour afficher le numéro de port à partir de la console Web d'OfficeScan, cliquez sur **Administration** > **Serveur Web** dans la barre latérale.

Si vous modifiez les informations relatives à un serveur OfficeScan existant, son nom apparaît en regard de **Nom du serveur OfficeScan**. Si vous ajoutez un nouveau serveur, **n.a** s'affiche.

6. Dans **Informations sur la stratégie**, sélectionnez les stratégies à utiliser lorsque le réseau est normal ou lorsque le mode épidémie est activé.
7. Configurez les paramètres du proxy si un serveur proxy se trouve entre le serveur OfficeScan et le serveur de stratégie.
 - a. Cochez la case **Activer proxy HTTP**.
 - b. Saisissez l'adresse IP et le numéro de port du serveur proxy.

Si le serveur proxy utilise une authentification, cochez la case **Authentification** et tapez le nom d'utilisateur et le mot de passe d'accès au serveur.
8. Cliquez sur **Enregistrer**.

Configuration des règles

Les règles sont les briques des stratégies et en constituent le contenu. La configuration des règles constitue l'étape suivante de la configuration du serveur de stratégie (voir *Création des règles* à la page A-10 pour obtenir des informations détaillées sur les règles).

Ajout ou modification d'une règle

Pour ajouter ou modifier une règle :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste des serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations. L'écran **Résumé** correspondant s'affiche. Choisissez l'une des méthodes suivantes pour accéder à l'écran **Règles** :
 - Dans l'écran **Résumé**, cliquez sur le lien correspondant au nombre de **Règles**.
 - Cliquez sur **Configurations > Règles**. L'écran **Règles** apparaît.
3. Pour ajouter une nouvelle règle :
 - Cliquez sur **Ajouter**. L'écran **Nouvelle règle** apparaît.

Pour modifier une règle existante :

 - Cliquez sur le nom de la règle. L'écran **Modifier règle** correspondant s'affiche.
4. En regard de **Nom de règle** et de **Description**, tapez un nom pour la stratégie et une description (facultative).
5. Dans **Critères correspondants**, sélectionnez les critères auxquels les clients OfficeScan doivent correspondre pour qu'une réponse soit renvoyée. Le serveur de stratégie renvoie une réponse lorsque tous les critères sélectionnés correspondent. Si les critères n'ont pas de correspondance, le serveur de stratégie renvoie la réponse que vous avez configurée dans la stratégie à laquelle cette règle est appliquée.
 - Pour déclencher une réponse en fonction de l'état de la fonction Scan en temps réel, cochez la case à côté de **Le scan en temps réel du client est** et cliquez sur **Activé** ou **Désactivé**.

- Pour déclencher une réponse en fonction de l'état de la fonction Scan en temps réel, cochez la case à côté de **Le moteur de scan du client est** et cliquez sur **A jour** ou **Pas à jour**.
 - Pour déclencher une réponse basée sur l'état du fichier de signatures de virus, cochez la case à côté de **État du fichier de signatures de virus du client** et cliquez sur l'une des options suivantes :
 - **Selon la version** : la version du fichier de signatures de virus du client OfficeScan est au maximum ou au minimum de { } versions plus ancienne que celle du fichier de signatures de virus du serveur OfficeScan.
Sélectionnez **au maximum** ou **au minimum** et le nombre de versions dans les listes.
 - **Selon la date de publication du fichier de signatures** : la date de la version du fichier de signatures de virus du client OfficeScan est au maximum ou au minimum de { } jours plus ancienne que celle du fichier de signatures de virus du serveur OfficeScan.
Sélectionnez **au maximum** ou **au minimum** et le nombre de jours dans les listes.
6. A côté de **Réponse renvoyée**, sélectionnez la réponse qu'OfficeScan renverra si l'état de sécurité du client correspond à tous les éléments de **Critères correspondants** (consultez *Réponses par défaut des règles* à la page A-10 pour obtenir des informations complémentaires à ce sujet) :
- **Sain**
 - **Vérification**
 - **Infecté**
 - **En quarantaine**
 - **Inconnu**

Remarque : Vous ne pouvez, ni ajouter, ni supprimer d'éléments de la liste **Réponse par défaut**.

7. Dans **Actions côté serveur**, cochez la case **Consigner cet incident si tous les critères correspondent** pour que le serveur de stratégie consigne cet incident.

8. Dans **Actions côté client**, sélectionnez parmi les options suivantes pour les clients OfficeScan si tous les critères de la stratégie correspondent (consultez *[Demander au serveur de stratégie et au client OfficeScan d'effectuer des actions](#)* à la page A-11 pour obtenir des explications au sujet de ces actions) :
 - **Activer le scan du client en temps réel**
 - **mettre à jour les composants**
 - **Scanner après l'activation du scan en temps réel ou après une mise à jour**
 - **Exécuter un nettoyage immédiat ou un scan immédiat**
 - **Exécuter un nettoyage immédiat**
 - **Afficher le message de notification sur l'ordinateur client** (si nécessaire, modifiez le message)
9. Cliquez sur **Enregistrer**.

Configuration des stratégies





Lorsque vous avez configuré les nouvelles règles ou vérifié que les règles par défaut conviennent à vos besoins de sécurité, configurez des stratégies que ces serveurs OfficeScan enregistrés puissent utiliser (voir *[Création des stratégies](#)* à la page A-14 pour obtenir des informations détaillées sur les stratégies).

Ajout ou modification d'une stratégie

Ajoutez une nouvelle stratégie Cisco NAC ou modifiez une stratégie existante pour déterminer les règles qui sont appliquées et pour agir sur les clients au cas où l'état de sécurité du client ne correspond à aucune règle.

Pour ajouter une nouvelle stratégie :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste de tous les serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations. L'écran **Résumé** correspondant s'affiche. Choisissez l'une des méthodes suivantes pour accéder à l'écran **Stratégies** :
 - Dans l'écran **Résumé**, cliquez sur le lien correspondant au nombre de **Stratégies**.

- Cliquez sur **Configurations > Stratégies** dans la barre latérale.
L'écran **Stratégies** apparaît.
3. Pour ajouter une stratégie :
 - Cliquez sur **Ajouter**. L'écran **Nouvelle stratégie** apparaît.
 Pour modifier une stratégie :
 - Cliquez sur un nom de stratégie. L'écran **Modifier stratégie** correspondant s'affiche.
 4. En regard de **Nom de stratégie** et de **Description**, tapez un nom pour la stratégie et une description (facultative).
 5. Dans **Règles**, sélectionnez les règles existantes qui constitueront la stratégie. Les règles existantes apparaissent dans la colonne **Règles disponibles**. Les règles sont appliquées dans l'ordre dans lequel elles apparaissent dans la colonne **Règles utilisées**.
-
- Remarque :** Si rien ne correspond aux critères d'une règle particulière, le serveur de stratégie passe à la règle suivante.
-
- Pour déplacer les règles entre les colonnes **Règles disponibles** et **Règles utilisées**, cliquez sur une règle, puis sur «» ou «».
 - Pour modifier l'ordre des règles utilisées, cliquez sur la règle puis sur  ou .
 6. Dans **Réponse par défaut**, sélectionnez la réponse que le serveur de stratégie doit envoyer si aucune règle ne transmet de réponse :
 - **Sain**
 - **Vérification**
 - **Infecté**
 - **En quarantaine**
 - **Inconnu**
-
- Remarque :** Vous ne pouvez, ni ajouter, ni supprimer d'éléments de la liste **Réponse par défaut**.
-

7. Dans **Actions côté serveur**, cochez la case **Consigner cet incident si tous les critères correspondent** pour que le serveur de stratégie consigne cet incident (consultez *Utilisation des journaux de validation du client* à la page B-33 pour obtenir des informations détaillées).
8. Dans **Actions côté client**, sélectionnez parmi les actions suivantes qu'OfficeScan prendra pour les clients OfficeScan si tous les critères de la stratégie correspondent (consultez *Demander au serveur de stratégie et au client OfficeScan d'effectuer des actions* à la page A-11 pour obtenir des explications au sujet de ces actions) :
 - **Activer le scan du client en temps réel**
 - **Mettre à jour les composants**
 - **Scanner après l'activation du scan en temps réel où une mise à jour manuelle est réalisée**
 - **Exécuter un nettoyage immédiat ou un scan immédiat**
 - **Exécuter un nettoyage immédiat**
 - **Afficher le message de notification sur le poste de travail du client**
9. Cliquez sur **Enregistrer**.

Remarque : Seule une stratégie peut être associée simultanément à un serveur OfficeScan. Vous pouvez affecter une stratégie lorsque le réseau est en mode normal et une autre lorsque le réseau est en mode Epidémie (consultez *Ajout ou modification de serveurs OfficeScan* à la page B-26 et *Mise en œuvre de la prévention contre les épidémies virales* à la page 5-2 pour obtenir de plus amples informations à ce sujet).

Utilisation des journaux de validation du client

Utilisez les journaux de validation du client pour afficher des informations détaillées sur les clients après validation par le serveur de stratégie. La validation se produit lorsque le serveur ACS récupère les données d'état de sécurité du client et les envoie au serveur de stratégie, qui les compare aux stratégies et aux règles (consultez [La séquence de validation du client](#) à la page A-6).

Remarque : Pour afficher les journaux de validation du client, vous devez permettre au serveur de stratégie de consigner les validations du client lors de l'ajout ou de la modification d'une règle / stratégie en cochant la case placée sous **Actions côté serveur** (consultez à ce sujet [Ajout ou modification d'une règle](#) à la page B-28 et [Ajout ou modification d'une stratégie](#) à la page B-30).

Affichage des journaux de validation du client

Le serveur de stratégie enregistre les journaux de validation du client sous format de fichiers .CSV. Ouvrir les fichiers journaux dans un tableur.

Pour afficher et enregistrer les journaux de validation du client :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste de tous les serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations.
3. Dans la barre latérale, cliquez sur **Journaux > Affichage des journaux de validation du client**. L'écran **Affichage des journaux de validation du client** apparaît avec la liste des journaux triée par ordre de date ascendant.
4. Pour afficher un journal, cliquez sur sa date.

Configuration de la maintenance des journaux du client

Le serveur de stratégie archive les journaux de validation des clients lorsqu'ils atteignent la taille que vous avez indiquée. Le serveur de stratégie supprime les journaux de validation des clients archivés lorsqu'un nombre spécifié est atteint. Précisez la manière dont le serveur de stratégie assure la maintenance des journaux de validation des clients.

Pour configurer la maintenance des journaux :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste de tous les serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations.
3. Dans la barre latérale, cliquez sur **Journaux > Maintenance du journal**. L'écran **Maintenance des journaux** apparaît.
4. À côté de **Format du journal**, cliquez sur le type de format que le serveur de stratégie devra enregistrer :
 - **Simple** :
 - Heure de validation
 - Adresse IP du client
 - Résultat de la validation
 - **Détaillé** :
 - Heure de validation
 - Adresse IP du client
 - Résultat de la validation
 - État du service de scan en temps réel du client
 - Version du moteur de scan du client
 - Version du fichier de signatures de virus du client
 - Date de mise en circulation du fichier de signatures de virus sur le client
 - Emplacement du serveur OfficeScan
 - Stratégie correspondante
 - Règle correspondante

- Version du moteur de scan du serveur
 - Version du fichier de signatures de virus du serveur
 - Date de mise en circulation du fichier de signatures de virus sur le serveur
5. Tapez la taille maximale de chaque journal (entre 1 et 1 024 Mo). Le serveur de stratégie crée un nouveau fichier de journal lorsque la taille maximale est atteinte.
 6. Tapez le nombre de fichiers de journaux dont le serveur de stratégie doit assurer la maintenance (entre 2 et 30).
 7. Cliquez sur **Enregistrer**.

Exécution des tâches d'administration

Exécutez des tâches administratives suivantes sur le serveur de stratégie :

- Modifier le mot de passe – modifie le mot de passe qui a été configuré lors de l'ajout du serveur de stratégie (consultez *Ajout et suppression de serveurs de stratégie* à la page B-22)
- Configurer un programme de synchronisation – définit un programme de synchronisation des serveurs OfficeScan enregistrés auprès du serveur de stratégie

Modification des mots de passe

La connexion au serveur de stratégie nécessite l'authentification par mot de passe. Utilisez l'écran **Modifier le mot de passe** pour modifier les mots de passe.

Pour modifier le mot de passe du serveur de stratégie :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste de tous les serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations.
3. Dans la barre latérale, cliquez sur **Administration > Modification du mot de passe**. L'écran **Modifier le mot de passe** apparaît.

4. Tapez le mot de passe créé lors de la configuration d'un nouveau serveur de stratégie.
5. Saisissez le nouveau mot de passe.
6. Saisissez encore une fois le nouveau mot de passe pour confirmer.
7. Cliquez sur **Enregistrer**.

Configuration de la synchronisation programmée

Le serveur de stratégie doit se procurer périodiquement la version du fichier de signatures de virus et du moteur de scan sur le serveur OfficeScan, afin d'évaluer l'état de sécurité du client OfficeScan. C'est pourquoi vous ne pouvez activer ou désactiver la synchronisation programmée. Par défaut, le serveur de stratégie se synchronise au(x) serveur(s) OfficeScan toutes les cinq minutes (voir *Définition de la synchronisation* à la page A-16 pour obtenir des informations complémentaires).

Remarque : Vous pouvez synchroniser manuellement le serveur de stratégie au moment de votre choix dans l'écran **Résumé** (consultez *Consultez le résumé des informations d'un serveur de stratégie* à la page B-23)

Pour définir un planning de synchronisation des serveurs :

1. Dans la barre latérale de la console Web d'OfficeScan, cliquez sur **Cisco NAC > Serveurs de stratégie**. L'écran **Serveurs de stratégies** apparaît et affiche la liste des serveurs de stratégies.
2. Cliquez sur le nom du serveur de stratégie dont vous souhaitez consulter les informations.
3. Dans la barre latérale, cliquez sur **Administration > Synchronisation programmée**. L'écran **Synchronisation programmée** apparaît.
4. Tapez l'intervalle (3 à 1 440 minutes) entre deux synchronisations programmées.
5. Cliquez sur **Enregistrer**.

Utilisation de Control Manager™ avec OfficeScan

Cette annexe présente Trend Micro Control Manager et décrit la manière dont il permet de simplifier la gestion de l'antivirus Trend Micro et des solutions de sécurité du contenu au sein de votre société. Vous y trouverez également des instructions sur la manière dont il convient d'installer l'agent pour OfficeScan, ainsi que la manière dont vous pouvez accéder au serveur OfficeScan à partir de la console de management Control Manager.

Les sujets évoqués dans la présente annexe sont entre autres :

- *Présentation du Control Manager* à la page C-2
- *Possibilités offertes par Control Manager et OfficeScan* à la page C-2
- *Présentation de Control Manager Agent* à la page C-3
- *Prérequis à l'installation de l'Agent* à la page C-3
- *Obtention de la Clé d'encodage publique* à la page C-4
- *Installation de l'agent Control Manager* à la page C-5
- *Accès à OfficeScan par le Control Manager* à la page C-8
- *Suppression de l'agent* à la page C-9

Présentation du Control Manager

Trend Micro Control Manager™ est une console de management centrale qui gère les produits et services Trend Micro, les solutions antivirus tierces et les produits de sécurisation du contenu au niveau de la passerelle, du serveur de messagerie, du serveur de fichiers et des postes de travail des entreprises. La console de management à interface Web Control Manager fournit un point de surveillance unique pour les solutions antivirus et les produits et services de sécurisation du contenu dans tout le réseau.

Control Manager permet aux administrateurs du système de surveiller et de notifier les activités telles que des infections, des violations de la sécurité ou des points d'entrée des virus. Les administrateurs du système peuvent télécharger et déployer des composants de mise à jour dans le réseau, contribuant ainsi à garantir une protection cohérente et actuelle. Les composants de mise à jour comprennent les fichiers de signature de virus, les moteurs de scan et les règles de lutte contre les pourriels. Control Manager permet de réaliser à la fois des mises à jour manuelles et programmées. Control Manager permet la configuration et la gestion des produits, en groupe ou séparément, afin d'obtenir une flexibilité accrue.

Possibilités offertes par Control Manager et OfficeScan

Control Manager repose sur le concept de management centralisé Trend Micro, qui a été lancé avec Trend Virus Control System (Trend VCS). Si vous utilisez actuellement Trend VCS, vous pouvez acheter une mise à jour pour pouvoir bénéficier de toutes les nouvelles fonctionnalités du Control Manager. Pour obtenir de plus amples informations au sujet de la mise à jour de votre serveur de management de Trend VCS vers Control Manager, consultez le *Guide de mise en route du Control Manager*.

Control Manager vous permet de :

- configurer, surveiller et assurer la maintenance des logiciels Trend Micro, y compris OfficeScan, à partir d'une console unique, indépendamment du lieu ou de la plate-forme ;
- simplifier la mise en œuvre des stratégies de sécurité antivirus de votre société ;

- Déléguer des tâches et déterminer le contrôle des accès sur la base d'une structure hiérarchique. Vous pouvez affecter divers accès opérateurs séparés à des branches individuelles de la hiérarchie
- Répondre rapidement aux attaques à l'aide du service de prévention des attaques

Présentation de Control Manager Agent

Un agent Control Manager est une application installée sur un ordinateur lors de l'installation du produit Trend Micro. L'agent permet au Control Manager de gérer le produit. Il reçoit des commandes du serveur Control Manager, les applique au produit géré et collecte des journaux qu'il envoie au Control Manager.

Prérequis à l'installation de l'Agent

Les prérequis à l'installation de l'agent sont les mêmes que ceux qui sont applicables à l'installation du serveur OfficeScan.

Remarque : Vous ne pouvez installer l'agent Control Manager sur Microsoft Windows .NET™ Server.

Pour obtenir des informations sur la configuration minimale requise pour le serveur OfficeScan, consultez le *Guide de déploiement et d'installation*.

Informations requises pour l'installation de l'agent

Avant de déployer l'agent, il vous faut disposer des informations suivantes :

- Le nom de domaine complet (FQDN) ou l'adresse IP du serveur Control Manager.
- Des privilèges d'administrateur pour le serveur sur lequel vous souhaitez installer l'agent.
- Un ID utilisateur Control Manager avec des privilèges Administrateur, Power User ou Opérateur. Il est très important d'assurer la maintenance de ce compte. Si l'ID utilisateur de Control Manager est supprimé, l'agent ne pourra pas s'enregistrer une nouvelle fois auprès du serveur Control Manager.
- L'endroit où se trouve la clé d'encodage publique du serveur Control Manager sur lequel vous enregistrerez les agents

Obtention de la Clé d'encodage publique

Tous les produits gérés par Control Manager doivent disposer d'une clé d'encodage publique afin de s'enregistrer et d'établir les communications avec le serveur Control Manager. Obtenir la clé d'encodage publique à l'aide de la console de management de Control Manager.

Pour obtenir la Clé d'encodage publique :

1. Sur l'un des ordinateurs du réseau, ouvrez un navigateur Web et saisissez l'adresse `http://{Control Manager Server Name}/ControlManager`, où {Control Manager Server Name} est le nom de l'ordinateur ou l'adresse IP du serveur Control Manager.

L'écran de **Bienvenue** de la console de management Control Manager apparaît.
2. Saisissez votre ID d'utilisateur et votre mot de passe.
3. Cliquez sur **Produits**.
4. Cliquez sur **Ajout/Suppression d'agents de produits**.
5. Cliquez du bouton droit de la souris sur **Clé d'encodage publique**, puis cliquez sur **Enregistrer sous**.
6. Enregistrez la clé d'encodage publique `E2EPublic.dat` à un endroit accessible sur le serveur OfficeScan où l'agent sera installé.

Installation de l'agent Control Manager

Lorsque vous avez obtenu la clé d'encodage publique et que vous l'avez enregistrée sur le serveur OfficeScan, installez l'agent.

Les méthodes d'installation de l'agent suivantes sont disponibles :

- **L'installateur principal du serveur OfficeScan** : installe l'agent lorsque vous installez le serveur OfficeScan (consultez le *Guide de déploiement et d'installation*)
- **Le programme d'installation de l'agent de Control Manager** : utilise l'outil d'installation distant disponible dans la console de management Control Manager et sur le CD OfficeScan Standard à l'emplacement suivant :

`output/CMAgent/ControlMangerAgent Setup.exe`

Pour installer l'agent :

1. Effectuez l'une des actions suivantes :
 - Si vous optez pour l'installation à l'aide de l'installation principale d'OfficeScan, lorsque l'écran **Sélectionner les composants** apparaît, cochez la case **Installer l'agent Control Manager**. Ensuite, l'écran d'installation de l'agent Control Manager apparaît.
 - Si vous optez pour l'installation de l'agent Control Manager à partir du CD inclus, double-cliquez sur le fichier `Setup.exe` qui se trouve dans le dossier `Programs\OfficeScan\cmagent`. La fenêtre de l'installateur apparaît.
2. Saisissez un ID existant pour le serveur Control Manager. Trend Micro vous recommande d'utiliser l'ID racine.
3. Confirmez le nom du serveur OfficeScan dans le champ **Nom d'entité**.
4. Cliquez sur **Suivant**.
 Si l'installateur ne détecte pas l'installation de Control Manager (y compris du serveur Control Manager ou de l'agent Control Manager) sur l'ordinateur, l'écran **Setup Message Routing Path** apparaît.
 Si l'installateur détecte une installation de Control Manager sur l'ordinateur, une invite apparaît qui vous demande si vous souhaitez reconfigurer les paramètres de la mise à jour de la version actuelle de l'agent Control Manager.

- Cliquez sur **Non** pour conserver les paramètres originaux et terminer la mise à jour.
- Cliquez sur **Oui** pour modifier les paramètres. L'écran **Setup Message Routing Path** apparaît.

Remarque : Lorsque vous mettez à jour la version actuelle de l'agent Control Manager, vous ne pouvez pas modifier le nom du compte Control Manager associé à l'agent. L'installateur préserve le nom du compte utilisé dans l'installation précédente.

5. Spécifiez un chemin pour les messages entrants qui proviennent du serveur Control Manager :
 - **Any host** : cliquez pour que l'agent accepte les messages entrants de tous les hôtes du réseau.
 - **IP port forwarding** : cliquez ici si les messages entrants du serveur Control Manager passent par un pare-feu ou un périphérique de réseau qui utilise le transfert de port et saisissez l'adresse IP du périphérique, le numéro de port que le périphérique écoute et le numéro de port vers lequel il transfère les messages.
 - **Proxy server** : cliquez ici si les messages entrants passent par un serveur proxy puis cliquez sur **Proxy Server Configuration** pour configurer les paramètres du serveur proxy. L'écran **Proxy Configuration** apparaît.
- a. Saisissez le nom du serveur proxy, le numéro de port qu'il utilise et saisissez le protocole qu'il prend en charge (HTTP ou SOCKS 4/5).
- b. Si le serveur proxy utilise des informations d'identification, cochez la case **Authentification required** et saisissez le nom d'utilisateur et le mot de passe.
- c. Cliquez sur **OK** pour retourner à l'écran **Setup Message Routing Path**.
- d. Précisez le chemin pour les messages sortants.
 - **Route direct to server** : cliquez ici si les messages sortants, y compris les commandes, prennent directement la direction du serveur Control Manager
 - **Proxy server** : cliquez ici si les messages sortants passent par un serveur proxy puis cliquez sur **Proxy Server Configuration** pour configurer les paramètres du serveur proxy. L'écran **Proxy Configuration** apparaît.

- i. Saisissez le nom du serveur proxy, le numéro de port qu'il utilise et saisissez le protocole qu'il prend en charge (HTTP ou SOCKS 4/5).
 - ii. Si le serveur proxy utilise des informations d'identification, cochez la case **Authentication required** et saisissez le nom d'utilisateur et le mot de passe.
 - iii. Cliquez sur OK pour retourner à l'écran **Setup Message Routing Path**.
6. Cliquez sur **Suivant**. L'écran **Register with Control Manager** apparaît.
7. Cliquez sur **Import** pour sélectionner la clé d'encodage publique `E2EPublic.dat` envoyée par le serveur Control Manager (consultez *Obtention de la Clé d'encodage publique* à la page C-4).
8. Sélectionnez la clé d'encodage publique, puis cliquez sur **Ouvrir**. Les informations sur Control Manager apparaissent sous **Informations sur le serveur**.
9. Cliquez sur **Suivant**. Lorsque l'installation est terminée, un message de confirmation apparaît.
10. Cliquez sur **OK**.

Accès à OfficeScan par le Control Manager

L'agent de Control Manager pour OfficeScan accepte des commandes du serveur Control Manager et demande à OfficeScan d'exécuter des actions. Par exemple, lorsque vous cliquez sur **Tâches > Deploy engines** dans la console Control Manager, l'agent demande à OfficeScan de déployer le moteur de scan le plus récent.

Pour ouvrir la console Control Manager :

1. Sur l'un des ordinateurs du réseau, ouvrez un navigateur Web et saisissez l'adresse `http://{Control Manager Server Name}/ControlManager`, où {Control Manager Server name} peut être le nom de l'ordinateur ou l'adresse IP du serveur Control Manager.

L'écran de **Bienvenue** de la console Control Manager apparaît.

2. Cliquez sur **Produits**.
3. Dans le **Répertoire Produits**, cliquez sur le serveur OfficeScan qui doit être géré. Les onglets suivants s'affichent :
 - **État du produit** : affiche des informations sur le serveur OfficeScan, telles que le nom du serveur, le nombre de composants de cette version, le système d'exploitation utilisé sur le serveur et les détails relatifs à l'agent Control Manager
 - **Configuration** : accès à la console Web d'OfficeScan
 - **Tâches** : déploie le moteur de scan, le fichier de signatures de virus et le modèle damage cleanup, permet d'effectuer des scans en temps réel et d'exécuter un Scan immédiat
 - **Journaux** : affiche les journaux des événements et de sécurité de Control Manager

Suppression de l'agent

Vous pouvez aisément supprimer l'agent Control Manager de Trend Micro pour OfficeScan en utilisant la fonction **Ajout/Suppression de programmes** de Windows.

Pour supprimer l'agent :

1. Sur le serveur où est installé l'agent, cliquez sur le menu **Démarrer**, puis cliquez sur **Paramètres > Panneau de configuration > Ajout/Suppression de programmes**. La fenêtre **Ajout/Suppression de programmes** apparaît. Cliquez sur **agent Control Manager de Trend Micro pour OfficeScan**, puis cliquez sur **Modifier/Supprimer**. Un écran de confirmation apparaît.
2. Cliquez sur **Oui**. Windows supprime l'agent du serveur. Lorsque l'agent est complètement supprimé, cliquez sur **OK**.

Remarque : La suppression du serveur OfficeScan entraîne automatiquement la suppression de l'agent Control Manager d'OfficeScan...

Configuration d'OfficeScan grâce à des compagnons et des logiciels tiers

Cette annexe décrit comment installer et utiliser Windows Protection Manager pour qu'il contribue à gérer votre OfficeScan pour Wireless et Check Point™ SecureClient™ pour vérifier la configuration de sécurité de vos clients.

Les sujets évoqués dans la présente annexe sont entre autres :

- *À propos de Wireless Protection Manager* à la page D-2
- *Installation de Wireless Protection Manager* à la page D-4
- *Utilisation de Wireless Protection Manager* à la page D-5
- *Aperçu de l'architecture et de la configuration de Check Point Firewall* à la page D-10
- *Configuration de Check Point pour OfficeScan* à la page D-13
- *Installation du support SecureClient sur le client OfficeScan* à la page D-15

À propos de Wireless Protection Manager

Un assistant numérique personnel (PDA) et autres outils informatiques portables augmente le nombre de modes de communication entre outils, ainsi que les risques d'infection. Aujourd'hui, il est courant pour un PDA de présenter des fonctionnalités Internet.

Remarque : Dans ce manuel, le terme « PDA » est utilisé pour décrire les assistants numériques personnels et les autres outils informatiques portables.

OfficeScan pour Wireless offre aux ordinateurs portables une protection antivirus facile à utiliser, qui permet aux outils sans fil de se défendre contre les menaces potentielles. Les codes malicieux ou autres menaces spécifiquement conçues pour les plates-formes portables peuvent s'infiltrer sur votre Palm, Pocket PC ou EPOC pendant les opérations de projection, de synchronisation ou d'accès à Internet.

Vous devez installer Wireless Protection Manager sur votre poste de travail ou ordinateur portable pour aider à gérer les fichiers OfficeScan pour Wireless installés, synchronisés ou mis à jour sur votre PDA. Il reçoit aussi des informations sous la forme de journaux du PDA.



FIGURE D-1 Relation entre Wireless Protection Manager sur votre ordinateur et la protection sans fil sur votre PDA

Remarque : Wireless Protection Manager n'apporte aucune protection contre les virus à votre poste de travail ou ordinateur portable.

Configuration minimale requise du PDA

Votre PDA nécessite la configuration suivante pour qu'il puisse fonctionner avec Trend Micro OfficeScan pour Wireless.

Palm

- Palm™ OS 3.x ou 4.x
- 2Mo de mémoire
- 100K de mémoire disponible pour l'installation des programmes
- Le poste de travail doit être équipé de Palm Desktop™ 3.1 ou supérieur et des applications HotSync™

Pocket PC

- Windows CE 3.0
- 16 Mo de RAM
- 1 Mo de mémoire disponible pour l'installation du programme
- Le poste de travail doit être équipé de Microsoft ActiveSync™ 3.1 ou supérieur

EPOC

- Psion Revo™ ou Revo™ Plus
- 8 Mo de RAM
- 200K de mémoire disponible pour l'installation du programme
- Le poste de travail doit être équipé de l'application PsiWin 2.3.2

Installation de Wireless Protection Manager

Vous devez installer les éléments suivants pour apporter une protection contre les virus sur votre PDA.

- Wireless Protection Manager sur votre ordinateur
- OfficeScan pour Wireless sur votre PDA

Avant d'installer Wireless Protection Manager, assurez-vous d'avoir déjà installé votre logiciel de synchronisation (par exemple, Palm Desktop) et que votre PDA est fermement et correctement installé dans son sabot.

Pour installer Wireless Protection Manager :

1. Dans la barre d'état système, cliquez sur l'icône du client OfficeScan, puis cliquez sur l'icône **OfficeScan Main**. La fenêtre client OfficeScan apparaît.
2. Dans l'onglet **Boîte à outils**, cliquez sur **Installer/Mettre à niveau Wireless Protection**. Une zone de message s'affiche. Cliquez sur **Oui** pour procéder à l'installation. L'assistant d'installation apparaît.
3. Cliquez sur **Suivant**. L'écran **Contrat de licence** apparaît.
4. Cliquez sur **J'accepte les conditions du contrat de licence**, puis cliquez sur **Suivant**. Vous devez donner votre accord pour continuer l'installation. L'écran **Informations du client** apparaît.
5. Vérifiez l'exactitude des informations et cliquez sur **Suivant**. L'écran **Dossier de destination** apparaît. Vous pouvez choisir l'endroit où vous souhaitez installer Wireless Protection Manager ou utiliser l'emplacement par défaut. Pour modifier l'emplacement, cliquez sur **Modifier**, puis recherchez un emplacement.
6. Cliquez sur **Suivant**. Cochez la case de la plate-forme de votre PDA, en fonction du logiciel de synchronisation que vous avez déjà installé (par exemple, Palm Desktop).
7. Cliquez sur **Suivant**, puis cliquez sur **Installer**.
8. Cliquez sur **Terminer**.

Lorsque vous avez sélectionné la plate-forme logicielle de synchronisation et que vous avez installé Wireless Protection Manager sur votre ordinateur, OfficeScan pour Wireless est automatiquement installé sur votre PDA.

Remarque : Pour les PDA sous Palm OS, la prochaine fois que vous exécutez HotSync, OfficeScan pour Wireless est installé sur votre PDA. De plus, lorsque OfficeScan pour Wireless est installé, vous devez fermer et rouvrir manuellement HotSync Manager. Vous devez rechercher HotSync Manager pour obtenir des journaux de virus de l'outil sous Palm OS.

Utilisation de Wireless Protection Manager

Utilisez Wireless Protection Manager pour mettre à jour votre fichier de signatures de virus et le moteur de scan sur les PDA. Vous pouvez préciser l'emplacement des éléments téléchargés pour obtenir les composants mis à jour, configurer les paramètres proxy et synchroniser les fichiers entre le programme principal et les fichiers sur votre PDA.

Mise à jour OfficeScan pour Wireless

Pour protéger votre PDA contre les dernières menaces, vous devez mettre à jour votre moteur de scan et vos fichiers de signatures de virus. Même si tous les composants peuvent être mis à jour, de nouveaux fichiers de signatures de virus sont publiés au moins chaque semaine. La mise à jour de votre fichier de signatures vous apporte la protection la plus récente et permet à OfficeScan pour Wireless de rechercher les virus les plus récents ou autres programmes malveillants.

Trend Micro vous conseille de procéder à des mises à jour régulières de votre fichier de signatures de virus afin de maintenir un degré de protection élevé.

De plus, comme de nouveaux virus sont découverts et que les virus existants évoluent, il devient nécessaire de mettre à jour certains fichiers programme et d'ajouter de nouvelles fonctionnalités au moteur de scan. La mise à jour de votre moteur de recherche vous garantit que OfficeScan pour Wireless agit sur les nouvelles instructions des signatures de virus et qu'il supprime les virus.

La mise à jour de votre protection sans fil passe par les étapes suivantes :

1. Téléchargement manuel des fichiers à partir du serveur Trend Micro ActiveUpdate ou d'une autre source précisée
2. Synchronisation des fichiers avec votre PDA

Téléchargement des mises à jour des composants

Vous devez procéder au téléchargement des mises à jour des composants à partir du serveur Trend Micro ActiveUpdate ou d'une autre source de mise à jour précisée. Ces composants comprennent les fichiers de signatures des virus, le moteur de scan et autres fichiers programme.

Pour vous assurer que vous disposez de la technologie Trend Micro de protection antivirus la plus récente, vous devez maintenir vos fichiers à jour.

Pour télécharger les mises à jour des composants :

1. Ouvrez Wireless Protection Manager.
2. Cliquez sur l'onglet **Mise à jour manuelle**.
3. Sous **Source téléchargement composant**, confirmez que la source de mise à jour est correcte. Si ce n'est pas le cas, choisissez l'une des options suivantes :
 - Cliquez sur **Serveur ActiveUpdate de Trend Micro** pour télécharger à partir de Trend Micro
4. Cliquez sur **Autre source** pour télécharger à partir d'un autre emplacement précisé.
5. Cliquez sur **Mettre à jour**.

Activation de la configuration des paramètres proxy

Si vous utilisez un serveur proxy sur votre réseau, vous devez saisir l'adresse IP et le numéro de port de ce serveur proxy. Il se peut aussi que vous deviez fournir les informations d'identification de connexion.

Pour activer et configurer des paramètres proxy :

1. Ouvrez Wireless Protection Manager.
2. Dans la barre de menu, cliquez sur **Option > Paramètres proxy**. La fenêtre **Paramètres proxy** apparaît.
3. Sous **Serveur proxy**, cochez la case **Utiliser un serveur proxy...**
4. Dans **Nom de l'hôte**, saisissez l'adresse IP ou le nom du serveur proxy (par exemple, proxy.yourcompany.com).
5. Dans **Port**, saisissez le numéro de port du serveur proxy (par exemple, 80).
6. Dans **Protocole**, cliquez sur le protocole utilisé par votre serveur proxy (**HTTP** ou **SOCKS**).
7. Sous **Authentification**, sous **Utilisateur** et **Mot de passe**, saisissez les informations d'identification de connexion de votre serveur proxy.
8. Cliquez sur **OK**.

Synchronisation avec votre PDA

Pour vous assurer que les dernières mises à jour des composants soient sur votre PDA, vous devez synchroniser les fichiers de mise à jour de votre ordinateur avec votre PDA.

Avant de procéder à une synchronisation manuelle par le biais de Wireless Protection Manager, veuillez faire ce qui suit :

- Assurez-vous que votre PDA soit fermement et correctement installé dans le sabot
- Fermez tous les logiciels antivirus qui fonctionnent sur votre PDA

Remarque : Cette fonction ne fonctionne actuellement que sur les PDA qui utilisent les plates-formes Pocket PC et EPOC. Pour les PDA Palm, vous devez procéder à une synchronisation manuelle à l'aide de la fonction Palm HotSync.

Pour synchroniser votre PDA

1. Ouvrez Wireless Protection Manager.
2. Cliquez sur l'onglet **Synchronisation manuelle**.
3. Cliquez sur **Synchroniser**.

Utilisation des journaux

Tous les événements viraux sont enregistrés comme entrées du journal. Les entrées journal contiennent des informations utiles sur les événements viraux qui se sont produits, y compris le type de scan de virus, la date et l'heure auxquelles le virus a été détecté, le nom du fichier et du virus, ainsi que les actions effectuées.

Affichage des journaux

Si vous avez détecté un virus, affichez le journal des virus enregistrés sur Wireless Protection Manager pour obtenir de plus amples informations. Avant d'afficher les journaux, n'oubliez pas de synchroniser Wireless Protection Manager avec votre PDA pour vous assurer que vous pouvez consulter les journaux les plus récents.

Pour afficher les journaux de virus :

1. Ouvrez Wireless Protection Manager.
2. Cliquez sur l'onglet **Journal de virus**.

3. Dans **Select log range**, cochez la case du type de PDA correspondant au journal que vous souhaitez consulter.
4. Exécutez les opérations suivantes :
 - Pour consulter tous les journaux, dans la liste **Log for** sélectionnez **Toutes les dates**.
 - Pour consulter les journaux dans une plage de dates spécifique dans la liste **Log for** sélectionnez **Specified date range** et sélectionnez la plage de dates.
5. Cliquez sur **Afficher les journaux**.

Gestion des journaux sur votre PDA

Le journal des virus enregistre des informations sur les virus détectés pendant les précédentes recherches, ainsi que les actions prises contre ces virus.

Pour consulter le journal, saisissez **Journal** sur l'écran principal de votre PDA.

L'écran **Virus Scan Log** affiche des informations au sujet des virus détectés ainsi que de la taille du journal en octets. Cliquez sur **Précédent** pour revenir dans l'écran principal.

Pour supprimer les entrées du journal, saisissez **Effacer les journaux**. Une zone de message s'affiche et confirme la suppression du journal. Tapez **Oui** pour supprimer les entrées du journal ou **Non** pour avorter l'opération.

Supprimer les journaux

Supprimez les entrées du journal Wireless Protection Manager si les informations qu'elles fournissent ne sont plus utiles. Si le numéro du journal consomme un espace disque trop important, vous pouvez aussi supprimer les entrées de certaines dates.

Pour supprimer des journaux :

1. Ouvrez Wireless Protection Manager.
2. Cliquez sur l'onglet **Journal de virus**.
3. Sous **Delete logs manually**, dans la liste **Delete logs before**, sélectionnez une date.
4. Cliquez sur **Effacer les journaux**. Un message de confirmation apparaît. Cliquez sur **Oui** pour supprimer tous les journaux antérieurs ou égaux à la date que vous avez sélectionnée.

Aperçu de l'architecture et de la configuration de Check Point Firewall

L'installation d'OfficeScan peut être complètement intégrée dans Check Point SecureClient utilisant Secure Configuration Verification (SCV) dans le cadre d'Open Platform for Security (OPSEC). Il est préférable de vous familiariser avec la documentation Check Point SecureClient OPSEC avant de lire ce chapitre. Vous pouvez trouver la documentation d'OPSEC à l'adresse www.opsec.com.

Check Point SecureClient a la possibilité de confirmer la configuration de sécurité des ordinateurs connectés au réseau à l'aide des contrôles Secure Configuration Verification (SCV). Les contrôles SCV sont un ensemble de conditions définissant un système client configuré en toute sécurité. Le logiciel tiers peut communiquer la valeur de ces conditions à Check Point SecureClient. Check Point SecureClient compare alors ces conditions aux conditions du fichier SCV afin de déterminer si le client est considéré comme sécurisé.

Les contrôles SCV sont exécutés régulièrement afin de s'assurer que seuls des systèmes configurés de manière sécurisée soient autorisés à se connecter au réseau.

SecureClient utilise des serveurs de stratégies pour propager des contrôles SCV vers tous les clients enregistrés sur le système. L'administrateur configure les contrôles SCV sur le serveur de stratégie à l'aide de l'éditeur SCV.

L'éditeur SCV est un outil fourni par Check Point qui vous permet de modifier les fichiers SCV pour la propagation de l'installation du client. Pour faire fonctionner l'éditeur SCV, situez et exécutez le fichier `SCVeditor.exe` sur le serveur de stratégie. Dans l'Éditeur SCV, ouvrez le fichier `local.scv` dans le répertoire `C:\FW1\NG\Config` (remplacer `C:\FW1` par le chemin d'installation pour le pare-feu Check Point s'il est différent du chemin par défaut).

Pour obtenir des instructions spécifiques sur l'ouverture et la modification d'un fichier SCV à l'aide de l'Éditeur SCV, consultez [*Configuration de Check Point pour OfficeScan*](#) à la page D-13.

Intégration avec OfficeScan

Le client OfficeScan transmet régulièrement le numéro de fichier de signatures des virus et le numéro du moteur de scan à SecureClient pour vérification. SecureClient compare alors ces valeurs avec les valeurs du fichier client `local.scv`. Voici ce à quoi ressemble le fichier `local.scv` si vous l'ouvrez dans un éditeur de texte :

```
(SCVObject
  :SCVNames (
    : (OfceSCV
      :type (plugin)
      :parameters (
        :CheckType (OfceVersionCheck)
        :LatestPatternVersion (701)
        :LatestEngineVersion (7.1)
        :PatternCompareOp (">=")
        :EngineCompareOp (">=")
      )
    )
  )
  :SCVPolicy (
    : (OfceSCV
      )
  )
  :SCVGlobalParams (
    :block_connections_on_unverified (true)
    :scv_policy_timeout_hours (24)
  )
)
```

Dans cet exemple, le contrôle SCV permettra de réaliser des connexions par le biais du pare-feu si la version du fichier des signatures est la version 701 ou supérieure et si le numéro du moteur de scan est 7.1 ou ultérieur. Si le moteur de scan ou le fichier

des signatures est antérieur, toutes les connexions qui passent par le pare-feu Check Point sont bloquées. Ces valeurs peuvent être modifiées à l'aide de l'éditeur SCV dans le fichier `local.scv` sur le serveur de stratégie.

Remarque : Check Point ne met pas automatiquement à jour le fichier de signatures et le numéro de version du moteur de scan dans le fichier SCV. Lorsque OfficeScan met à jour le moteur de scan ou le fichier de signatures, vous devez modifier manuellement la valeur des conditions dans le fichier `local.scv` pour les maintenir actuels. Si vous ne mettez pas à jour les versions du moteur de scan et des signatures, Check Point autorise le trafic qui provient des clients disposant de fichiers de signatures ou de moteurs de scan antérieurs, permettant ainsi un risque potentiel d'infiltration de nouveaux virus dans le système.

Configuration de Check Point pour OfficeScan

Pour modifier le fichier `local.scv`, vous devez télécharger et exécuter l'éditeur SCV (`SCVeditor.exe`).

Pour configurer le fichier **Secure Configuration Verification** :

1. Téléchargez `SCVeditor.exe` depuis le site de téléchargement de Check Point à l'adresse :
`www.checkpoint.com/techsupport/ng/fp3_updates.html#opsecsdk`
L'éditeur SCV fait partie du pack OPSEC SDK.
2. Exécutez `SCVeditor.exe` sur le serveur de stratégie. La console de l'éditeur SCV s'ouvre à l'écran.
3. Étendre le répertoire **Produits** et sélectionnez **user_policy.scv**.
4. Cliquez sur **Édition > Produit > Modifier**, puis saisissez **OfceSCV** dans la case **Modifier**. Cliquez sur **OK**.

Remarque : Si votre fichier `local.scv` contient déjà des stratégies produit pour un logiciel tiers, créez une nouvelle stratégie en cliquant sur **Édition > Produit > Ajouter**, puis saisissez **OfceSCV** dans le champ **Ajouter**.

5. Ajoutez à présent cinq paramètres. Pour ajouter un paramètre, cliquez sur **Modifier > Paramètres > Ajouter**, puis saisissez un **Nom** et une **Valeur** dans les champs correspondants. Le Tableau D-1 donne la liste des noms et des valeurs des paramètres. Les noms et les valeurs des paramètres sont sensibles à la casse et doivent être saisis dans l'ordre indiqué dans Tableau D-1

Nom	Valeur
TypeContrôle	ContrôleVersionOfce
VersionDernièresSignatures	{numéro du fichier de signatures actuel}
VersionDernierMoteur	{numéro du moteur de scan actuel}
DernièreDateSignatures	{date d'émission du fichier de signatures actuel}
ComparerSignaturesOp	>=
ComparerMoteurOp	>=
MessageErreurSignatures	
MessageErreurMoteur	


TABLEAU D-1. Les noms et les valeurs des paramètres du fichier SCV

Saisissez le numéro du fichier de signatures actuel et le numéro du moteur de scan au lieu du texte dans les accolades du Tableau D-1. Vous pouvez consulter les dernières versions des signatures de virus et du moteur de scan des clients en cliquant **Mise à jour & mise à niveau** sur la barre latérale de la console Web OfficeScan. Le numéro de la version de signature apparaît à droite du graphique circulaire représentant le pourcentage des clients protégés.

6. Sélectionnez **Block connections on SCV unverified**.
7. Cliquez sur **Édition > Produit > Mettre en oeuvre**.
8. Cliquez sur **Fichier > Generate Policy File** pour créer le fichier. Sélectionnez le fichier existant `local.scv` afin de l'écraser.

Installation du support SecureClient sur le client OfficeScan

Si certains de vos utilisateurs se connectent au réseau de l'entreprise par le biais de Virtual Private Network (VPN) et qu'ils disposent à la fois du Check Point SecureClient et du client OfficeScan sur leur ordinateur, vous pouvez leur demander d'installer le support SecureClient. Ce module permet à SecureClient d'exécuter régulièrement des contrôles SCV sur les clients VPN afin de s'assurer que seuls des systèmes configurés soient autorisés à se connecter au réseau.

Les utilisateurs peuvent vérifier que Check Point SecureClient est installé sur leur ordinateur en vérifiant la présence de l'icône  dans la barre d'état système ou d'un élément appelé **Check Point SecureClient** sur l'écran Windows **Ajout/Suppression de programmes**.

Pour installer le support SecureClient

1. Ouvrez la console client.
2. Cliquez sur l'onglet **Boîte à outils**.
3. Dans **Support Check Point SecureClient**, cliquez sur **Install/Upgrade SecureClient support**. Un écran de confirmation apparaît.
4. Cliquez sur **Oui**. Le client se connecte au serveur et télécharge le module. Lorsque le téléchargement est terminé, le message « Enregistrer OfficeScan SCV » apparaît.
5. Cliquez sur **OK**.

Glossaire terminologique

Voici une liste des termes utilisés dans ce document :

Terme	Description
Adresse IP dynamique (DIP)	Une adresse IP dynamique est une adresse IP attribuée par un serveur DHCP. L'adresse MAC de l'ordinateur reste la même ; toutefois, le serveur DHCP peut attribuer une nouvelle adresse IP à l'ordinateur, en fonction de la disponibilité.
Agent Control Manager	Installé sur un serveur OfficeScan pour l'enregistrement sur le serveur Control Manager. L'administration d'OfficeScan peut ainsi avoir lieu par le biais de la console de management Control Manager.
Applications de piratage des mots de passe	Logiciel qui aide les pirates à déchiffrer les noms d'utilisateurs et mots de passe d'un compte.
ARP conflictuel	Un type d'attaque dans le cadre duquel un pirate envoie une requête de protocole de résolution d'adresse avec la même adresse IP source et de destination. L'ordinateur cible s'envoie continuellement une réponse ARP (son adresse MAC) et dès lors gèle ou se plante.
Attaque de refus de service (DoS Attack)	Une attaque sur un ordinateur ou un réseau provoquant une perte de « service », à savoir une connexion réseau. En général, les attaques DoS ont une incidence négative sur la bande passante du réseau ou surchargent les ressources de l'ordinateur telles que la mémoire.
Attaque terrestre	Type d'attaque dans le cadre de laquelle des paquets de synchronisation IP (SYN), dont les adresses sources et cibles sont identiques, sont envoyés à un ordinateur, celui-ci s'envoyant en retour un accusé-réception de la synchronisation (SYN/ACK). Cela peut geler ou ralentir la machine.

Terme	Description
Authentification, autorisation et mesure (AAA)	Les trois principaux services utilisés pour contrôler l'accès du client de l'utilisateur final aux ressources informatiques. Authentification : identification d'un client, en général par saisie d'un nom d'utilisateur et d'un mot de passe. Autorisation : privilèges d'exécution de certaines commandes accordés à l'utilisateur. Mesure : mesure des ressources utilisées pendant une session, en général consignée dans des journaux. Le serveur de contrôle d'accès (ACS) sécurisé de Cisco est l'application par Cisco d'un serveur AAA.
Autorité de certificat (CA)	Une autorité sur un réseau qui distribue des certificats numériques pour réaliser des connexions authentifiées et sécurisées entre les ordinateurs et / ou les serveurs.
Canulars	Logiciel qui entraîne un comportement anormal d'un ordinateur, par exemple il peut faire vibrer l'écran.
Certificat ACS	Sert à établir une communication fiable entre le serveur ACS et le serveur d'autorité de certification (CA). Le serveur d'autorité de certificat signe le certificat ACS et celui-ci est enregistré sur le serveur ACS.
Certificat CA	Utilisé pour authentifier les clients de l'utilisateur final avec le serveur ACS de Cisco. Le certificat CA est déployé sur le serveur ACS et sur les clients (fourni avec Cisco Trust Agent par le serveur OfficeScan).
Certificat SSL	Certificat numérique créant une communication HTTPS sécurisée entre le serveur de stratégie et le serveur ACS.
Certificat SSL du serveur de stratégie	Sécurise la communication HTTPS entre le serveur de stratégie et le serveur ACS. Le certificat SSL du serveur de stratégie est automatiquement généré pendant l'installation du serveur de stratégie.
Certificats Numériques	Pièce jointe servant à la sécurité. Le plus souvent, les certificats authentifient les clients auprès des serveurs tels que des serveurs Web. Ils contiennent les éléments suivants : informations sur l'identité de l'utilisateur, un code public (pour le codage) et la signature numérique d'une autorité de certification (CA) pour vérifier la validité du certificat.
Chevaux de Troie	Programmes exécutables qui ne se multiplient pas mais reposent sur les systèmes pour effectuer des opérations malveillantes telles que l'ouverture des ports aux pirates.
Cisco Trust Agent (CTA)	Installé sur les ordinateurs clients de l'utilisateur final pour communiquer l'état de sécurité à des périphériques d'accès au réseau Cisco. Peut être déployé sur les clients OfficeScan à partir de la console Web d'OfficeScan.
Code Java malicieux	Virus indépendant du système d'exploitation écrit ou imbriqué dans Java.
Code malicieux ActiveX	Un type de virus qui réside dans les pages Web qui exécutent des contrôles ActiveX.

Terme	Description
Composeurs de numéros	Logiciel qui modifie les paramètres Internet du client et oblige le poste du client à composer des numéros de téléphone préconfigurés à l'aide d'un modem
Compte serveur à accès contrôlé (ACS)	Transmet au serveur de stratégie les demandes d'authentification du périphérique d'accès au réseau, afin de valider l'état de sécurité de l'utilisateur final. Le serveur ACS passe également le jeton d'état du serveur de stratégie au périphérique d'accès au réseau (ACS). Le serveur ACS peut également être configuré pour exécuter des actions sur le client de l'utilisateur final par l'intermédiaire du périphérique d'accès au réseau.
Contrat de licence utilisateur final (CLUF)	<p>Un contrat de licence utilisateur final ou CLUF est un contrat légal passé entre un éditeur de programme et l'utilisateur final. Il décrit généralement les restrictions s'appliquant à l'utilisateur qui peut refuser de conclure l'accord en ne cliquant pas sur « J'accepte » au cours de l'installation. En cliquant sur « Je n'accepte pas », l'utilisateur mettra évidemment fin à l'installation du produit programme.</p> <p>De nombreux utilisateurs acceptent par inadvertance d'installer un programme espion et d'autres types de graywares sur leur ordinateur lorsqu'ils cliquent sur « J'accepte » sur des invites du CLUF s'affichant lors de l'installation de certains programmes gratuits.</p>
Correctifs (hot fixes) et autres correctifs	Solutions globales pour les problèmes liés à la clientèle ou les failles récemment découvertes en matière de sécurité que vous pouvez télécharger à partir du site Web de Trend Micro et déployer vers le serveur OfficeScan et/ou le programme client.
Enregistreur de frappe	Un programme qui capture et enregistre l'historique des frappes et des clics de souris, éventuellement sans que l'utilisateur en soit informé.
État de sécurité	Présence et actualité du logiciel antivirus installé sur le client de l'utilisateur final. L'état de sécurité des clients OfficeScan indique si le programme client OfficeScan est installé et l'ancienneté des versions des composants antivirus.
Fragment de chevauchement	Similaire à une attaque Teardrop, cette attaque de refus de service envoie des fragments TCP de chevauchement à un ordinateur. L'en-tête du premier fragment TCP est écrasée et susceptible de pouvoir passer au travers du pare-feu. Le pare-feu peut ensuite autoriser les fragments suivants, qui peuvent contenir un code malicieux, à se frayer un chemin vers l'ordinateur cible.
Fragment minuscule	Avec ce type d'attaque, un fragment TCP de petite taille force la première en-tête de paquet TCP dans le fragment suivant. Cela peut amener les routeurs filtrant le trafic à ignorer les fragments suivants, pouvant contenir des données malveillantes.
Fragment trop important	Attaque de refus de service dans le cadre de laquelle un pirate dirige un paquet TCP/UDP surdimensionné sur un ordinateur cible. Par conséquent, la mémoire tampon des ordinateurs peut déborder, ce qui risque de geler ou redémarrer la machine.

Terme	Description
Graywares	Fichiers et programmes, autres que des virus, qui peuvent affecter négativement les performances des ordinateurs connectés à votre réseau. Il s'agit entre autre des logiciels d'espionnage, les logiciels publicitaires, des composeurs de numéros, des canulars, des outils de piratage, des outils d'accès distant, des applications de piratage de mots de passe et autres. Le moteur de scan OfficeScan recherche les graywares et les virus.
HTTPS	Protocole HTTP utilisant Secure Socket Layer (SSL).
Hyper Text Transfer Protocol (HTTP)	Il s'agit d'un protocole standard utilisé pour transférer des pages Web (y compris des graphiques et contenus multimédia) d'un serveur vers un client via Internet.
IGMP fragmenté	Une attaque de refus de service a lieu lorsque des paquets d'IGMP fragmentés sont envoyés à un ordinateur cible qui ne peut pas les traiter correctement. Cela peut geler ou ralentir la machine.
Internet Control Message Protocol ICMP (Internet Control Message)	Il arrive qu'une passerelle ou un hôte de destination utilise le protocole ICMP pour communiquer avec un hôte source afin d'indiquer une erreur dans le traitement des datagrammes, par exemple. Le protocole ICMP utilise le support de base du protocole IP comme s'il s'agissait d'un protocole de niveau plus élevé ; cependant, le protocole ICMP fait en réalité partie intégrante du protocole IP et doit être implémenté par chaque module IP. Les messages ICMP sont envoyés dans les cas suivants : par exemple, lorsqu'un datagramme ne parvient pas à atteindre sa destination, lorsque la passerelle ne possède pas la capacité tampon de transférer un datagramme et lorsque la passerelle peut diriger l'hôte afin d'acheminer le trafic via une route plus courte. Le protocole IP n'est pas conçu pour être parfaitement fiable. Le but de ces messages de contrôle est d'obtenir un retour d'informations concernant les problèmes dans l'environnement de communication, et non de rendre le protocole IP fiable.
Intrusion Système de détection (IDS)	Les systèmes de détection d'intrusion font généralement partie des pare-feux. Un IDS peut contribuer à identifier des signatures dans les paquets réseau indiquant une attaque du client.
Jeton d'état	Le serveur de stratégie crée le jeton d'état après validation par l'utilisateur final. Comprend des informations disant que le client OfficeScan peut exécuter des actions indiquées telles que l'activation du scan en temps réel ou la mise à jour des composants antivirus.
Logiciels publicitaires	Similaire au logiciel espion, ce logiciel récolte des données utilisateur telles que les préférences de navigation, qui pourraient être utilisées à des fins publicitaires.
Outils d'accès à distance	Outils utilisés pour aider les pirates à s'infiltrer et à contrôler un ordinateur à distance
Outils de piratage	Outils utilisés pour aider les pirates à s'infiltrer sur le poste client.

Terme	Description
Pare-feu stateful inspection	Le pare-feu Stateful inspection est un pare-feu qui contrôle toutes les connexions au client et rappelle tous les états de connexion. Il peut identifier les conditions spécifiques de toute connexion, prédire les actions qui doivent être prises et détecter tout viol des conditions normales. Cela augmente significativement les chances qu'un pare-feu détecte une attaque sur un client.
Périphérique d'accès au réseau	Serveurs d'accès au réseau, pare-feu, routeurs, commutateurs ou points d'accès sans fil prenant en charge la fonctionnalité Cisco NAC.
Ping	Un utilitaire qui envoie une requête d'écho ICMP à une adresse IP puis attend la réponse. L'utilitaire Ping peut déterminer si l'ordinateur qui porte l'adresse IP spécifiée est connecté ou pas.
Ping of Death	Attaque de refus de service dans le cadre de laquelle un pirate dirige un paquet ICMP surdimensionné sur un ordinateur cible. Par conséquent, la mémoire tampon des ordinateurs peut déborder, ce qui risque de geler ou redémarrer la machine.
Programme espion	Type de graywares installant des composants sur un ordinateur en vue d'enregistrer les habitudes de navigation sur le web (essentiellement à des fins de marketing). L'auteur ou toute autre personne intéressée récupère alors les informations envoyées par le programme espion lorsque l'ordinateur est en ligne. Ces programmes sont souvent téléchargés lors de « téléchargements gratuits », ils ne signalent pas leur existence à l'utilisateur et ne demandent aucune autorisation pour installer les différents composants. Les informations recueillies par ces composants peuvent inclure les saisies effectuées par l'utilisateur, ce qui signifie que les informations confidentielles telles que les noms de connexion, les mots de passe et les numéros de carte de crédit sont susceptibles d'être dérobés.
Protocole DHCP (Dynamic Host Control Protocol)	Tout dispositif, comme un ordinateur ou un commutateur par exemple, doit posséder une adresse IP pour pouvoir être connecté à un réseau, mais l'adresse ne doit pas forcément être statique. Un serveur DHCP, utilisant le protocole DHCP, peut attribuer et gérer les adresses IP de manière dynamique chaque fois qu'un dispositif se connecte à un réseau.
Protocole FTP (File Transfer Protocol)	Il s'agit d'un protocole standard utilisé pour transférer des fichiers d'un serveur vers un client via Internet. Consultez « Network Working Group RFC 959 » pour de plus amples informations.
Protocole IP	« Le protocole Internet permet de transmettre des blocs de données appelés datagrammes depuis l'emplacement source vers l'emplacement de destination, ces deux emplacements étant des hôtes identifiés par des adresses de longueur définie. » (RFC 791)
Protocole Post Office 3 (POP 3)	Il s'agit d'un protocole standard pour le stockage et le transfert des messages depuis un serveur vers une application cliente de courrier électronique.

Terme	Description
Protocole SMTP (Simple Mail Transport Protocol)	Il s'agit d'un protocole standard utilisé pour acheminer les messages d'un serveur à l'autre et de l'ordinateur client au serveur via Internet
Protocole TCP (Transmission Control Protocol)	Protocole de bout en bout, fiable et basé sur les connexions, conçu pour s'adapter dans une hiérarchie de protocoles en couches prenant en charge des applications multi-réseaux. Le protocole TCP dépend des datagrammes IP pour la résolution des adresses. Consultez DARPA Internet Program RFC 793 pour de plus amples informations.
Protocole UDP (User Datagram Protocol)	Il s'agit d'un protocole de communication sans connexion utilisé avec le protocole IP pour les programmes d'application permettant d'envoyer des messages à d'autres programmes. Consultez DARPA Internet Program RFC 768 pour de plus amples informations.
Règle de serveur de stratégie	Les règles sont composées de critères spécifiques que les serveurs de stratégie comparent aux données d'état de sécurité du client OfficeScan. Si un aspect de l'état de sécurité du client correspond aux critères que vous avez configurés dans une règle, le client exécute les actions que vous avez indiquées.
Remote Authentication Dial-In User Service (RADIUS)	Système d'authentification demandant aux clients de saisir un nom d'utilisateur et un mot de passe. Les serveurs ACS sécurisés de Cisco prennent en charge RADIUS.
Secure Socket Layer (SSL)	SSL est un modèle proposé par Netscape Communications Corporation pour l'utilisation du système cryptographique à clé publique RSA, qui permet de coder et d'authentifier les contenus transférés via des protocoles de niveau élevé comme les protocoles HTTP, NNTP et FTP.
Serveur de stratégie	Serveur responsable de la détermination du jeton d'état des clients utilisateurs finaux ; télécharge périodiquement le fichier de signatures des virus à jour et les informations de version du moteur de scan à partir des serveurs OfficeScan du réseau. Installe le serveur de stratégie à partir de l'assistant d'installation principal d'OfficeScan ou du CD version Entreprise.
Sites hameçons	Un site Web qui induit les utilisateurs à fournir des détails personnels tels que des informations relatives à sa carte de crédit. Les liens vers les sites hameçon sont souvent envoyés dans des messages e-mail factices déguisés en messages légitimes de sociétés bien connues.
SOCKS 4	Un protocole TCP utilisé par les serveurs proxy afin d'établir une connexion entre les clients sur le réseau interne ou LAN et ordinateurs ou serveurs externes au LAN. Le protocole SOCKS 4 fait des demandes de connexion, établit des circuits proxy et relaie les données vers la couche application du modèle OSI.
Stratégie de serveur de stratégie	Composées de règles, les stratégies servent au serveur de stratégie à mesurer l'état de sécurité du client utilisateur final. Une stratégie est affectée à chaque serveur OfficeScan enregistré sur le réseau.

Terme	Description
SYN Flood	Attaque de refus de service dans le cadre de laquelle un programme envoie plusieurs paquets de synchronisation TCP (SYN) à un ordinateur, celui-ci envoyant alors continuellement des réponses d'accusé-réception de synchronisation (SYN/ACK). Cela peut épuiser la mémoire d'un ordinateur et finalement bloquer la machine.
Teardrop	Similaire à une attaque de fragment de chevauchement, cette attaque de refus de service a trait à des fragments IP. Une valeur de décalage prêtant à confusion dans le deuxième fragment IP ou un fragment ultérieur peut provoquer le blocage du système d'exploitation de l'ordinateur qui réceptionne en cas de tentative de reconstruction des fragments.
Telnet	Il s'agit d'une méthode standard de liaison entre les dispositifs terminaux via le protocole TCP grâce à la création d'un « terminal virtuel de réseau ». Consultez « Network Working Group RFC 854 » pour de plus amples informations.
Terminal Access Controller Access Control System (TACACS+)	Protocole de sécurité activé par l'intermédiaire des commandes AAA utilisées pour l'authentification des clients des utilisateurs finaux. Les serveurs ACS de Cisco prennent en charge TACACS+.
Traduction d'adresses réseau	La traduction d'adresses réseau est une fonction exécutée par les pare-feux de la passerelle et les routeurs. Un tableau sauvegardé sur le pare-feu ou le routeur enregistre les adresses IP des dispositifs à l'intérieur de la passerelle et les mappe à l'adresse IP externe de la passerelle. Les en-têtes des paquets provenant du réseau sont éliminés et ces paquets sont envoyés à leur destination affectés d'un en-tête contenant l'adresse IP externe du routeur ou de la passerelle. L'adresse IP de destination du paquet sortant est enregistrée de sorte que, lors de l'arrivée d'une réponse de la destination, le routeur puisse la transférer à la bonne adresse IP interne. De cette manière, les adresses IP des dispositifs du réseau interne sont masquées.
TrendLabs	TrendLabs est le réseau mondial des centres de recherche antivirus et de support de Trend Micro et fournit une assistance 24 heures sur 24, 7 jours sur 7 à tous les clients Trend Micro à travers le monde.
Validation du client	Processus d'évaluation par un serveur de stratégie Cisco NAC de l'état de sécurité d'un client OfficeScan et renvoi d'un jeton d'état au client.
Vers	Un programme automatique (ou ensemble de programmes) qui peut répandre des copies fonctionnelles de lui-même ou de ses segments dans d'autres systèmes informatiques, souvent par courrier électronique. Un vers peut aussi être appelé un virus réseau.
Virus	Un programme de virus qui se multiplie. Pour ce faire, le virus doit s'attacher à d'autres fichiers programmes et s'exécute chaque fois que le programme hôte est exécuté (consultez <i>Définition des virus</i> à la page 1-6 pour obtenir des informations plus détaillées).

Terme	Description
Virus de macro	Un type de virus encodé comme application macro qui se trouve souvent dans un document.
Virus de réseau	Virus qui utilisent les protocoles réseau tels que TCP, FTP, UDP, HTTP et e-mail pour se multiplier. Souvent, ils n'affectent pas les fichiers systèmes ou ne modifient pas les secteurs d'amorçage des disques durs. Par contre, les virus de réseau infectent la mémoire des ordinateurs en l'obligeant à inonder le réseau de trafic, ce qui peut entraîner des ralentissements, voire même une panne complète du réseau.
Virus de test	Un fichier inerte agissant comme un véritable anti-virus et détecté par un logiciel de recherche de virus. Utilise des fichiers test tels que le script de test EICAR, afin de vérifier que votre installation antivirus fonctionne correctement.
Virus du secteur d'amorçage	Un type de virus qui infecte le secteur d'amorçage d'une partition ou d'un disque.
Virus HTML, VBScript ou JavaScript	Virus qui résident dans des pages Web et sont téléchargés par un navigateur.
Virus qui infectent les fichiers COM et EXE	Un type de virus qui se dissimule sous les apparences d'une application en utilisant une extension de fichier .exe ou .com.

Index

A

- accès en écriture interdit dans les fichiers et les dossiers 5-7
- accord de privilèges aux clients 2-63
- ActiveAction 2-47
- ActiveX 1-6, 3-5
 - définition E-2
 - et des programmes espions 3-5
- Adresse IP dynamique (DIP)
 - définition E-1
- affichage
 - état du client 2-5
 - Informations résumées relatives au serveur
 - OfficeScan 2-4
 - journaux 7-2
 - journaux de mise à jour du client 7-5
 - journaux de mise à jour du serveur 7-5
 - journaux de vérification de la connexion 7-7
 - journaux de virus 7-2
 - journaux des événements du système 7-6
 - Journaux du pare-feu pour clients - version d'entreprise 7-8
- Agent Control Manager
 - configuration requise C-3
 - définition E-1
 - informations requises C-4
 - installation C-5
 - suppression C-9
- agent de mise à jour 2-21
- agents
 - Agent de mise à jour 2-21
 - Cisco Trust Agent (CTA) B-13
 - mise à niveau vers la version 2.0 B-15
 - Control Manager E-1
- ajout de domaine 2-11
- alerte d'épidémie 2-6
 - configuration 2-42

- Déroutement SNMP 2-44
- e-mail 2-43
- Journal des événements Windows NT 2-44
- pageur 2-43
- alerte standard 2-6
 - configuration 2-40
 - Déroutement SNMP 2-41
 - e-mail 2-36, 2-41
 - pageur 2-41
- amélioration de la mise à jour programmée des clients
 - nouvelle fonctionnalité 1-3
- applications de piratage des mots de passe 1-8, 3-2
 - définition E-1
- arborescence du domaine 2-9
 - icônes 2-10
 - sélection dans 2-12
- ARP conflictuel
 - définition E-1
- assistant d'envoi
 - URL 9-23
- attaque de refus de service (DoS Attack)
 - définition E-1
- attaque terrestre
 - définition E-2
- authentification, autorisation et mesure (AAA)
 - définition E-2
- autorité de certification (CA)
 - définition E-2

B

- base de connaissances 2-8, 9-23
 - URL 1-27
- blocage
 - dossiers partagés 5-2
 - ports 5-4

C

- canulars 1-8, 3-2
 - définition E-2
- carte des virus 9-20

- centre d'informations sur les virus 9-20
 - alerte virale 9-21
 - carte des virus 9-20
 - documentation technique 9-21
 - encyclopédie des virus 9-20
 - évaluation des risques 9-21
 - fichier test EICAR 9-20
 - glossaire des termes de menaces de sécurité 9-21
 - outils Webmaster 9-21
 - rapport hebdomadaire sur les virus 9-20
 - Safe Computing Guide 9-21
 - service d'abonnement 9-21
 - TrendLabs 9-21
 - virus Primer 9-21
- certificat ACS B-4
 - définition E-2
- certificat CA A-18
 - définition E-2
 - exportation et installation B-8
- certificat client
 - importation vers le serveur OfficeScan 2-6
- certificat SSL
 - définition E-2
- certification ICSA 1-12
- certification ISO 9002-voir TrendLabs 9-24
- certificats A-16
 - ACS B-4
 - CA A-18, B-8
 - serveur de stratégie SSL B-10
- certificats numériques
 - définition E-1
- chevaux de Troie 1-6
 - définition E-2
- Cisco NAC 2-6
 - foire aux questions (FAQ) 9-6
- Cisco Trust Agent (CTA) 1-9, B-13
 - configuration système pour Windows NT/2000 A-20
 - configuration système pour Windows XP A-20
 - définition E-2
 - déploiement 2-6
 - mise à niveau 2-6
 - mise à niveau vers la version 2.0 B-15
- clé d'encodage publique pour Control Manager C-4
- client
 - messages d'alerte
 - modification 2-45
 - nouvelles fonctionnalités 1-3
- Client Packager 8-10
- clients 1-22
 - accord de privilèges
 - privilèges client 2-63
 - affichage de l'état 2-5
 - agent de mise à jour 2-21
 - classifications 1-22
 - déconnecté 1-23
 - fichiers de configuration 1-10
 - gestion 1-17
 - importation et exportation des paramètres de
 - privilège et de scan 2-71
 - itinérants 1-23
 - journaux de mise à jour 7-5
 - mise à jour 2-24
 - composants et fichiers de configuration 2-25
 - normal 1-22
 - privilèges 2-4
 - recherche 2-13
 - suppression des inactifs 4-5
 - utilitaire de création d'image 8-10
- clients 32 et 64 bits 1-25
- clients inactifs 2-6
 - suppression 4-5
- clients itinérants 1-23
 - mise à jour 1-24
 - privilèges 1-23
- clients normaux 1-22
- communication sécurisée de la console Web 1-19
- compatibilité
 - Foire aux questions (FAQ) 9-2
- composants 1-9
 - mise à jour 2-15
 - rétrogradation 2-7, 2-34
- composeurs de numéros 1-8, 3-2
 - définition E-2
- compte serveur à accès contrôlé (ACS) B-19
 - définition E-3
 - inscription B-4

- configuration
 - alertes d'épidémie 2-42
 - alertes standards 2-40
 - gestionnaire de quarantaine 4-6
 - moniteur d'activité virale du pare-feu 6-21
 - notification des clients en cas d'épidémies 5-9
 - notifications d'épidémies 5-9
 - paramètres anti-programmes espions 3-9
 - paramètres de scan 2-46
 - paramètres proxy Internet 2-20
 - Policy Server pour Cisco NAC B-21
 - scan en temps réel 2-51
 - scan immédiat 2-59
 - scan manuel 2-48
 - scan programmé 2-54
 - serveur ACS B-19
- configuration du script de connexion 8-3
- configuration requise
 - console Web du serveur de stratégie A-19
- configuration système requise
 - serveur de stratégie A-19
- console de management
 - fonctions 1-26
- console Web
 - arborescence du domaine 2-9
 - autres liens 2-8
 - déconnexion 2-8
 - foire aux questions (FAQ) 9-7
 - mise à jour 2-4
 - ouverture 2-2
 - présentation 2-3
- contacter Trend Micro 9-20
- contrat de licence utilisateur final (CLUF)
 - définition E-3
- Control Manager C-2
 - accès au serveur OfficeScan C-8
 - agent C-3
 - clé d'encodage publique C-4
 - fonctionnalités avec OfficeScan C-2
 - installation de l'agent C-5
 - présentation C-2
- contrôle
 - épidémies 1-16
- contrôle journaux virus réseau/réduction bande passante
 - nouvelle fonctionnalité 1-4

- correctifs 1-9
 - correctifs (hot fixes) 1-9
 - correctifs (hot fixes) et autres correctifs
 - définition E-3
- correctifs de sécurité 1-9

D

- décodeur de fichiers 8-11
- déconnexion 2-8
- dépannage 8-1, 9-1
- déplacement des clients depuis un domaine 2-11
- déploiement
 - Cisco Trust Agent (CTA) 2-6
- déploiement automatique 2-29
- déploiement manuel 2-31
- désinstallation
 - Agent Control Manager C-9
 - clients 2-5
- documentation 1-27
 - Foire aux questions (FAQ) 9-7
- documentation technique 9-21
- domaine
 - ajout 2-11
 - déplacement des clients depuis 2-11
 - gestion 1-17
 - renommer 2-12
 - sélection dans 2-12
 - suppression 2-11
 - utilisation de 2-10

E

- éditeur SCV D-10
- encyclopédie des virus 9-20
- enregistreur de frappe
 - définition E-3
- envoi de fichiers suspects à Trend Micro 9-23
- épidémies
 - contrôle 1-16
- état de sécurité
 - définition E-3
- évaluation des risques
 - centre d'informations sur les virus 9-21
- événements 1-22
- exportation et importation des paramètres de scan 2-4

F

- fichier de signatures de virus du réseau 1-9
- fichier de signatures des virus 1-9
 - à propos de 1-10
 - numérotation 1-11
- fichiers et dossiers exclus des actions de scan 2-57
- fichiers infectés :
 - envoi vers le dossier de quarantaine 1-16
- foire aux questions (FAQ) 9-2
 - Cisco NAC 9-6
 - compatibilité 9-2
 - console Web 9-7
 - documentation 9-7
 - messages d'alerte 9-5
 - mise à jour 9-4
 - pare-feu pour clients - version d'entreprise 9-3
 - scan 9-5
- fragment de chevauchement
 - définition E-3
- fragment minuscule
 - définition E-3
- fragment trop important
 - définition E-3

G

- gestion
 - domaines et clients 1-17
- gestionnaire de quarantaine 2-6, 4-6
- glossaire des termes de menaces de sécurité 9-21
- graywares
 - définition E-4

H

- HTTP 1-21
- HTTPS
 - définition E-4

I

- icônes
 - arborescence du domaine 2-10
 - client itinérant 1-24
 - client normal 1-22
- IGMP fragmenté
 - définition E-4

- importation et exportation des paramètres de privilège et de scan des clients 2-71
- informations du serveur Web
 - modification 4-4
- inscription du serveur ACS sécurisé de Cisco B-4
- installation
 - Agent Control Manager C-5
 - installation à distance 2-5
 - Policy Server pour Cisco NAC B-16
- installation à distance
 - installation 2-5
- installation de serveurs multiples et de serveurs distants
 - nouvelle fonctionnalité 1-5
- intégration de la sauvegarde de la base de données
 - nouvelle fonctionnalité 1-5
- Intelliscan 2-48
- Internet 1-20
- Internet Information Server (IIS) 1-20

J

- Java
 - code malicieux 1-6
 - définition E-2
- journaux 2-7
 - affichage 7-2
 - événement du système 2-7, 7-6
 - fonction contrôle journaux virus réseau/réduction bande passante 1-4
 - gestion 7-9
 - maintenance 2-8
 - mise à jour 2-7
 - mise à jour du client 7-5
 - mise à jour du serveur 7-5
 - validation du client serveur de stratégie B-33
 - vérification de la connexion 2-7, 7-7
 - virus 2-7, 7-2
- journaux de mise à jour 2-7
- journaux de vérification de la connexion 2-7, 7-7
- journaux de virus 2-7, 7-2
- journaux des événements du système 2-7, 7-6
- journaux des virus réseau communiqués au Control manager
 - nouvelle fonctionnalité 1-5

L

- licence du produit
 - licence 2-6
- local.scv D-11
- logiciel publicitaire 1-8, 3-2
 - définition E-4

M

- messages d'alerte
 - Foire aux questions (FAQ) 9-5
- messages d'alerte du client 2-6
- mise à jour des clients 2-7, 2-24
 - agent de mise à jour 2-21
 - clients itinérants 1-24
 - composants et fichiers de configuration 2-25
 - fichiers de configuration 1-10
 - foire aux questions (FAQ) 9-4
 - sélection d'une source de mise à jour du client 2-25
 - utilisation de la fonction de mise à jour immédiate 2-32
 - utilisation du déploiement automatique 2-29
 - utilisation du déploiement manuel 2-31
 - vérification 2-33
- mise à jour du serveur 2-17
 - Foire aux questions (FAQ) 9-4
 - mise à jour manuelle du serveur 2-19
 - utilisation de la mise à jour programmée automatique 2-18
- mise à jour immédiate 1-24, 2-32
- mise à jour incrémentielle
 - nouvelle fonctionnalité 1-3
- mise à jour manuelle
 - client 2-31
 - serveur 2-19
- mise à jour programmée
 - mises à jour du serveur 2-18
- mise à niveau
 - Cisco Trust Agent (CTA) 2-6
- mises à jour automatiques
 - client 2-29
- modèle Damage Cleanup 1-9, 3-7
- modèles de routeurs Cisco A-20
- moniteur d'activité virale 1-19, 2-4, 5-11

- moniteur d'activité virale du pare-feu 2-5, 6-8
 - configuration 6-21
- mot de passe
 - configuration 2-6
 - modification de la console Web 4-2
 - modification du serveur de stratégie B-35
- moteur Damage Cleanup 1-9, 3-7
- moteur de scan 1-9
 - à propos de 1-11
 - certification ICSA 1-12
 - événements qui déclenchent une mise à jour 1-12
 - mise à jour 1-12
 - URL pour trouver la version actuelle 1-13

N

- nettoyage immédiat 2-5, 3-8
- notification d'installation
 - notification d'installation destinée aux clients 2-5
- notification des clients en cas d'épidémies 5-9
- nouvelles fonctionnalités
 - amélioration de la mise à jour programmée des clients 1-3
 - contrôle journaux virus réseau/réduction bande passante 1-4
 - côté client 1-3
 - côté serveur 1-5
 - installation de serveurs multiples et de serveurs distants 1-5
 - intégration de la sauvegarde de la base de données 1-5
- journaux des virus réseau communiqués au Control Manager 1-5
- mise à jour incrémentielle 1-3
- plusieurs sources de mise à jour 1-5
- prise en charge des plates-formes sous Windows
 - serveur pour les clients 1-3
- protection contre les programmes espions et autres graywares
 - nouvelle fonctionnalité 1-3
- scan des fichiers adaptable 1-3

O

OfficeScan

- avantages et capacités 1-18
- client 1-22
- console de management 1-26
- intégration avec SecureClient D-11
- serveur 1-20

OfficeScan pour Wireless 1-17

options de scan 2-4, 2-46

outils 2-8

- administrateur 2-8, 8-3
- client 2-8, 8-10
- Client Mover I 8-13
- Client Packager 8-10
- configuration du script de connexion 8-3
- décodeur de fichiers 8-11
- outil Touch 8-15
- précédemment pris en charge 8-19
- server Tuner 8-9
- utilitaire de création d'image 8-10
- Vulnerability Scanner (Scanner de faille) 8-3

outils administrateurs 2-8, 8-3

outils clients 2-8, 8-10

outils d'accès à distance

- définition E-4

outils d'accès à distance 1-8, 3-2

outils de piratage 1-8, 3-2

- définition E-4

outils Webmaster 9-21

P

packers 1-6

paramètres clients généraux 2-5

paramètres de scan

- configuration 2-46
- exclusion des fichiers et des dossiers 2-57
- scan en temps réel 2-51
- scan immédiat 2-59
- scan manuel 2-48, 2-54
- scan programmé 2-54

pare-feu pour clients - version d'entreprise 2-5, 7-8

configuration 6-13

configuration du moniteur d'activité virale du

- pare-feu 6-21

définition 6-2

déploiement 6-9

désactivation 6-23

foire aux questions (FAQ) 9-3

fonctions 6-6

journaux 7-8

liste des profils 2-5

liste des stratégies 2-5

moniteur d'activité virale du pare-feu 6-8

par défaut 6-5

stateful inspection 6-7

stratégies par défaut 6-5

stratégies, exceptions et profils 6-3

système de détection d'intrusion 6-7

vérification du déploiement 6-12

pare-feu stateful inspection

- définition E-5

PDA

- protection 1-17

périphérique d'accès au réseau (PAR)

- définition E-5

pilote du pare-feu commun 1-9

Ping

- définition E-5

Ping of Death

- définition E-5

plusieurs sources de mise à jour

- nouvelle fonctionnalité 1-5

Policy Server pour Cisco NAC

- affichage des journaux de validation du client B-33

aperçu du déploiement B-2

certificat ACS B-4

certificat CA A-18, B-8

certificat SSL du serveur de stratégie B-10

certificats A-16

Cisco Trust Agent (CTA) B-13

- mise à niveau vers la version 2.0 B-15

configuration de la synchronisation B-36

configuration des règles B-28

configuration des stratégies B-30

configuration du serveur de stratégie B-21

configuration serveur ACS B-19

création des règles A-10

création des stratégies A-14

définition du serveur de stratégie A-8

installation du serveur de stratégie B-16

- intervention du serveur ACS B-4
 - modification des mots de passe B-35
 - processus de validation du client A-6
 - règles par défaut A-12
 - stratégies et règles A-9
 - stratégies par défaut A-14
 - synchronisez le serveur de stratégie au serveur OfficeScan A-16
 - tâches administratives B-35
 - pourcentage de protection contre les programmes espions 3-11
 - prévention des épidémies 1-19, 5-2
 - accès en écriture interdit dans les fichiers et les dossiers 5-7
 - application 2-4
 - blocage des dossiers partagés 5-2
 - blocage des ports 5-4
 - restauration des paramètres initiaux du réseau 5-10
 - prévention manuelle des épidémies 2-6
 - configuration des notifications d'épidémies 5-9
 - problèmes connus avec OfficeScan 9-21
 - programme client 1-9
 - programme client OfficeScan 1-9
 - désinstallation 2-5
 - programme espion 1-8, 3-2
 - définition E-5
 - Programme international de pistage des virus 4-7
 - programmes espions et autres graywares
 - configuration des paramètres anti-programmes espions 3-9
 - envoi des fichiers suspects à Trend Micro 3-4
 - le pourcentage de protection contre les programmes espions 3-11
 - mode d'infiltration sur votre réseau 3-3
 - protection contre 3-12
 - risques et menaces 3-3
 - types 1-8, 3-2
 - utilisant ActiveX 3-5
 - vue d'ensemble 1-7, 3-2
 - protection
 - analyse 1-15
 - mise à jour 1-16
 - protection contre les graywares
 - nouvelle fonctionnalité 1-3
 - protocole Dynamic Host Control Protocol (DHCP)
 - définition E-5
 - protocole FTP (File Transfer Protocol)
 - définition E-5
 - protocole HTTP (Hyper Text Transfer Protocol)
 - définition E-4
 - protocole Hypertext Transfer (HTTP) 1-21
 - protocole ICMP (Internet Control Message Protocol)
 - définition E-4
 - protocole IP (Internet Protocol)
 - définition E-5
 - protocole Post Office 3 (POP 3)
 - définition E-5
 - protocole Simple Mail Transport Protocol (SMTP)
 - définition E-6
 - protocole Transmission Control (TCP)
 - définition E-6
 - protocole User Datagram (UDP)
 - définition E-6
 - proxy
 - Internet 2-20
 - intranet 4-3
 - proxy Internet
 - configuration des paramètres 2-20
 - proxy intranet 2-6
 - configuration 4-3
- ## R
- rapport hebdomadaire sur les virus 9-20
 - réalisation de scans 1-16
 - Remote Authentication Dial-In User Service (RADIUS)
 - définition E-6
 - renommer un domaine 2-12
 - restauration des paramètres initiaux du réseau 5-10
 - restaurer 2-4
 - rétrogradation des composants 2-7, 2-34
 - risques de sécurité
 - packers 1-6
 - RVP D-15

S

Safe Computing Guide 9-21

scan

- à partir d'un emplacement 1-16
- exclusion des fichiers et des dossiers 2-57
- exportation et importation des paramètres 2-4
- Foire aux questions (FAQ) 9-5
- options 2-4
- paramètres de scan 2-46
- scan en temps réel 2-51
- scan immédiat 2-5, 2-59
- scan manuel 2-48
- scan programmé 2-54

scan des fichiers adaptable

- nouvelle fonctionnalité 1-3

scan en temps réel 2-51

scan immédiat 2-5, 2-59

scan manuel 2-48, 2-54

scan programmé 2-54

secure Configuration Verification. *Consultez* SCV

Secure Socket Layer (SSL) 1-19

- définition E-6

SecureClient D-10

- Éditeur SCV D-10

- intégration avec OfficeScan D-11

- Serveurs de stratégie D-10

Server Tuner 8-9

serveur

- administration 2-4
- configuration des mises à jour automatiques programmées 2-18
- journaux de mise à jour 7-5
- mise à jour 2-17
- mise à jour manuelle 2-19
- mode fichier 1-22
- Mode HTTP 1-20
- nouvelles fonctionnalités 1-5

Serveur de stratégie 2-6

- affichage des journaux de validation du client B-33
- certificat SSL B-10
- définition E-2
- configuration B-21
- configuration de la synchronisation B-36
- configuration des stratégies B-28, B-30
- configuration minimale requise de la console Web A-19

configuration système requise A-19

définition E-6

définition de règle E-6

définition de stratégie E-6

inscription du serveur ACS sécurisé de Cisco B-4

journaux de validation du client B-33

modification des mots de passe B-35

routeurs Cisco pris en charge A-20

synchroniser avec le serveur OfficeScan A-16

serveur en mode fichier 1-22

serveur OfficeScan

- affichage des informations résumées 2-4

architecture 1-20

- synchroniser avec le serveur de stratégie A-16

serveurs de stratégie pour SecureClient D-10

service d'abonnement 9-21

service d'alertes virales 9-21

services Damage Cleanup 2-5

- exécution du nettoyage immédiat 3-8

signature de scan pour les programmes

espions/graywares 1-9

signature pour le nettoyage des programmes

espions/graywares 1-9, 3-7

Sites hameçon

- définition E-6

SOCKS 4

- définition E-6

SolutionBank - consultez le point base de

connaissances 1-27

source de mise à jour 2-25

SSL 1-19

stratégies antivirus et anti-programmes espions

- mise en oeuvre 1-15

soutien technique 9-1, 9-22

suppression

- Agent Control Manager C-9

- clients inactifs 4-5

suppression d'un domaine 2-11

SYN Flood

- définition E-7

synchronisation

- configuration du serveur de stratégie B-36

système de détection d'intrusion (IDS) 6-7

- définition E-4

T

- tâches administratives 4-1
- TCP/IP 1-21
- Teardrop
 - définition E-7
- Telnet
 - définition E-7
- Terminal Access Controller Access Control System (TACACS+)
 - définition E-7
- traduction d'adresses réseau
 - définition E-7
- Trend Micro
 - contacter 9-20
- TrendLabs 9-21, 9-24
 - définition E-7

U

- URL
 - base de connaissances 1-27
 - Cisco NAC A-2
 - version du moteur de scan 1-13
- utilitaire de création d'image 8-10

V

- validation du client
 - définition E-7
- vérification
 - mises à jour 2-33
- vers 1-6
 - définition E-7
- virus
 - « dans la nature » 1-11
 - « en cage » 1-11
 - contrôle des épidémies 1-16
 - définition E-7
 - scan de 1-16
- virus de macro 1-6
 - définition E-8
- virus de réseau 1-7
 - définition E-8
- virus de test
 - définition E-8

- virus du secteur d'amorçage 1-6
 - définition E-8
- virus HTML, VBScript ou JavaScript 1-6, E-8
- virus Primer 9-21
- virus qui infectent les fichiers COM et EXE 1-6
 - définition E-8
- Vulnerability Scanner (Scanner de faille) 8-3

W

- Windows
 - prise en charge des plates-formes serveur pour les clients 1-3
- Wireless Protection Manager 1-17