F-Secure Client Security

Guide de l'administrateur

Sommaire

Chapitre 1: Présentation....9

Configuration système requise....10
Policy Manager Server....10
Policy Manager Console....10
Principaux composants....12
Fonctions....13
Enregistrement du produit....14
Gestion des applications....15
Terminologie de base....16

Chapitre 2: Installation du produit....17

Procédure d'installation....18
Télécharger et exécuter le package d'installation....18
Sélection des composants à installer....18
Réalisation de l'installation du produit....19
Exécuter Policy Manager Console....19
Modification du chemin d'accès au navigateur Web....22
Désinstallation du produit....23

Chapitre 3: Interface utilisateur en Mode antivirus 25

Onglet Domaines de stratégie....26
Onglets de gestion....27
Onglet Résumé....27
Onglet Paramètres....29
Onglet Etat....38
Onglet Alertes....40
Onglet Rapports....40
Onglet Installation....41
Onglet Opérations....41
Barre d'outils....42
Options des menus....43
Héritage des paramètres....45
Affichage de l'héritage des paramètres dans l'interface utilisateur....45
Verrouillage et déverrouillage simultanés de tous les paramètres d'une page....46
Héritage des paramètres dans les tables....46

Chapitre 4: Configuration du réseau géré....47

Ouverture de session....48

Propriétés de connexion 48
Modification des préférences de communication....48
Administration des domaines et des hôtes....50
Ajout de domaines de stratégie....50
Ajout d'hôtes....51
Ajout d'hôtes à des domaines Windows....51
Importation d'hôtes auto-enregistrés....51
Installations distantes....53
Installation par stratégies....56
Installations et mises à jour locales à l'aide de packages préconfigurés....58
Installation locale et Policy Manager....60
Configuration système requise....60
Désinstallation d'autres programmes antivirus....60
Procédure d'installation....61
Installation sur un hôte infecté....62
Vérification du fonctionnement des connexions de gestion 63

Chapitre 5: Configuration de la protection contre les virus et les logiciels espions. 65

Configuration des mises à jour automatiques....66
Comment fonctionnent les mises à jour automatiques ?....66
Paramètres de la mise à jour automatique....66
Configuration des mises à jour automatiques à partir de Policy Manager Server....66
Configuration de Policy Manager Proxy....67
Configuration des clients de sorte qu'ils téléchargent des mises à jour entre eux....68
Configuration de l'analyse en temps réel....69
Paramètres d'analyse en temps réel....69
Activation de l'analyse en temps réel pour l'ensemble du domaine....70
Activation forcée de l'analyse en temps réel sur tous les hôtes....71
Exclusion du fichier .pst de Microsoft Outlook de l'analyse en temps réel....71
Configuration de DeepGuard....72
Paramètres DeepGuard....72
Requêtes serveur DeepGuard....72
Configuration de la recherche de rootkits (Blacklight)....74
Paramètres de la recherche de rootkits....74
Lancement de la recherche de rootkits dans l'ensemble du domaine....74
Configuration de l'analyse du courrier électronique....75
Paramètres d'analyse du courrier électronique....75
Activation de l'analyse du courrier électronique pour les messages entrants et sortants.76
Configuration de l'analyse du trafic Web (HTTP)....77
Paramètres d'analyse du trafic Web....77
Activation de l'analyse du trafic Web pour l'ensemble du domaine....77
Exclusion d'un site Web de l'analyse HTTP....77
Configuration de la recherche de logiciels espions....79
Paramètres de contrôle des logiciels espions....79

Configuration du contrôle des logiciels espions pour l'ensemble du domaine.....80
Lancement de la recherche de logiciels espions dans l'ensemble du domaine.....81
Autorisation de l'utilisation d'un composant de logiciel espion ou de riskware.....81
Gestion des objets en quarantaine.....82
Suppression des objets en quarantaine.....82
Libération d'objets en quarantaine.....82
Interdiction de modification des paramètres par les utilisateurs.....84
Marquage de tous les paramètres de protection antivirus comme finaux.....84
Configuration de l'envoi d'alertes.....85
Configuration de Client Security de façon à envoyer les alertes de virus à une adresse électronique.85
Désactivation des fenêtres indépendantes d'alerte de Client Security.....85
Surveillance des virus sur le réseau.....86
Test de la protection antivirus.....87

Chapitre 6: Configuration de la protection Internet.....89
Niveaux de sécurité globale de pare-feu.....90
Elaboration des principes des niveaux de sécurité.....92
Configuration des niveaux et des règles de sécurité.....93
Sélection d'un niveau de sécurité actif pour un poste de travail.....93
Configuration d'un niveau de sécurité par défaut pour les hôtes administrés.....93
Ajout d'un nouveau niveau de sécurité pour un domaine particulier.....94
Configuration de la quarantaine réseau.....96
Paramètres de quarantaine réseau.....96
Activation de la quarantaine réseau à l'échelle du domaine.....96
Réglage de la quarantaine réseau.....96
Configuration des alertes de règle.....97
Ajout d'une nouvelle règle avec alerte.....97
Configuration du contrôle des applications.....100
Paramètres de contrôle des applications.....100
Première configuration du contrôle des applications.....101
Création d'une règle pour une application inconnue au niveau racine.....102
Modification d'une règle de contrôle des applications existante.....103
Désactivation des fenêtres contextuelles de contrôle des applications.....104
Utilisation d'alertes pour vérifier le fonctionnement de la protection Internet.....105
Configuration de la prévention des intrusions.....106
Paramètres de la prévention des intrusions.....106
Configuration d'IPS pour les ordinateurs de bureau et les portables.....107

Chapitre 7: Comment vérifier la protection de l'environnement réseau.109
Vérifier que tous les hôtes utilisent la dernière stratégie.....110
Vérifier que le serveur utilise les définitions de virus les plus récentes 111
Vérifier que les hôtes ont les définitions de virus les plus récentes.....112
Vérifier qu'aucun hôte n'est déconnecté.....113
Affichage des rapports d'analyse.....114

Affichage des alertes....115
Création d'un rapport d'infection hebdomadaire....116
Surveillance d'une attaque réseau potentielle....117

Chapitre 8: Mise à jour du logiciel....119
Utilisation de l'éditeur d'installation....120

Chapitre 9: Opérations sur les hôtes locaux....123
Analyse manuelle....124
Comment sélectionner le type d'analyse manuelle....124
Nettoyer automatiquement les programmes malveillants....125
Afficher les résultats de l'analyse manuelle....126
Analyse à heures fixes....127
Planifier une analyse....127
Annuler une analyse planifiée....127
Afficher les résultats de l'analyse planifiée....128
Où trouver des alertes de pare-feu et des fichiers journal ?....129
Afficher les alertes du pare-feu....129
Afficher le journal des actions....130
Gestion du trafic réseau à l'aide de la consignation de paquets....130
Connexion à Policy Manager et importation manuelle d'un fichier de stratégie....133
Suspension des téléchargements et mises à jour....134
Autoriser les utilisateurs à décharger les produits F-Secure....135

Chapitre 10: Informations sur les virus....137
Informations sur les antiprogrammes et les outils sur les pages Web F-Secure....138
Comment envoyer un échantillon de virus à F-Secure....139
Comment préparer un échantillon de virus ?....139
Quels fichiers envoyer ?....139
Comment envoyer un échantillon de virus ?....140
Que faire en cas d'apparition d'un virus ?....142

Chapitre 11: Configuration du plug-in Cisco NAC....145
Installation du plug-in Cisco NAC....146
Importations de définitions d'attributs de validation de posture....147
Utiliser des attributs pour un jeton de posture d'application....148

Chapitre 12: Fonctions avancées : protection contre les virus et les logiciels espions....149
Configuration de l'analyse planifiée....150
Paramètres DeepGuard avancés....151
Notification d'un utilisateur d'un événement de refus....151

Permettre à un administrateur d'autoriser ou de refuser des événements provenant de programmes d'autres utilisateurs 151
Autorisation ou refus des événements requis automatiquement par une application spécifique. 151
Configuration de Policy Manager Proxy 153
Configuration des mises à jour automatiques sur les hôtes à partir de Policy Manager Proxy. 154
Exclure une application de l'analyseur du trafic Web 155

Chapitre 13: Fonctions avancées : protection Internet 157

Gestion à distance des propriétés de la protection Internet 158
Utilisation de la consignation des paquets 158
Utilisation de l'interface approuvée 158
Utilisation du filtrage des paquets 158
Configuration de la sélection automatique du niveau de sécurité 160
Dépannage de problèmes de connexion 161
Ajout de nouveaux services 162
Création d'un service Internet basé sur le protocole HTTP par défaut 162
Installation de Dialup Control 164
Autorisation et blocage des numéros de téléphone 164
Utilisation de l'enregistrement des appels 165

Chapitre 14: Modification de prodsett.ini 167

Paramètres prodsett.ini configurables 168

Chapitre 15: Messages d'alerte et d'erreur de l'analyse du courrier électronique. 177

Messages d'erreur et d'alerte 178

Chapitre 16: Produits détectés ou supprimés lors de l'installation du client. 181

Liste de produits 182

Chapitre

1

Présentation

Sujets :

- *Configuration système requise*
- *Principaux composants*
- *Fonctions*
- *Enregistrement du produit*
- *Gestion des applications*
- *Terminologie de base*

Policy Manager offre les fonctionnalités suivantes :

- définir des stratégies de sécurité ;
- distribuer des stratégies de sécurité ;
- installer des applications sur les systèmes locaux et distants ;
- surveiller des activités de tous les systèmes dans l'entreprise afin d'assurer la conformité avec les stratégies de l'entreprise et le contrôle centralisé.

Une fois le système configuré, vous pouvez afficher des informations d'état de l'ensemble du domaine géré en un seul et même endroit. De cette façon, vous pouvez facilement vous assurer que l'ensemble du domaine est protégé et modifier les paramètres de protection lorsqu'il y a lieu. Vous pouvez également empêcher les utilisateurs de modifier les paramètres de sécurité et être sûr que la protection est toujours à jour.

Configuration système requise

Cette section indique la configuration requise pour Policy Manager Server et Policy Manager Console.

Policy Manager Server

Pour installer Policy Manager Server, votre système doit correspondre à la configuration requise suivante.

Système d'exploitation :	Microsoft Windows • Microsoft Windows Server 2003 SP1 ou ultérieur (32 bits) ; éditions Standard, Enterprise, Web Edition ou Small Business Server • Windows Server 2003 SP1 ou ultérieur (64 bits) ; éditions Standard ou Enterprise • Windows Server 2008 SP1 (32 bits) ; éditions Standard, Enterprise ou Web Server • Windows Server 2008 SP1 (64 bits) ; éditions Standard, Enterprise, Web Server, Small Business Server ou Essential Business Server • Windows Server 2008 R2 ; éditions Standard, Enterprise ou Web Server
Processeur :	Processeur P4 2 GHz ou plus rapide. La gestion de plus de 5 000 hôtes ou l'utilisation de Web Reporting exige un processeur P4 à 3 GHz ou plus rapide.
Mémoire :	512 Mo de RAM, 1 Go de RAM recommandé. La gestion de plus de 5 000 hôtes ou l'utilisation de Web Reporting exige 1 Go de RAM.
Espace disque :	5 Go d'espace disque libre ; au moins 8 Go sont recommandés. La quantité d'espace requis sur le disque dur dépend de la taille de l'installation. Outre la configuration décrite ci-dessus, il est recommandé d'allouer environ 1 Mo par hôte pour les alertes et les stratégies. Il est difficile de prévoir la quantité réelle d'espace occupé sur le disque par chaque hôte, puisqu'elle dépend de la manière dont les stratégies sont utilisées ainsi que du nombre de fichiers d'installation stockés.
Réseau :	Réseau 10 Mbits La gestion de plus de 5 000 hôtes nécessite un réseau à 100 mégabits.

Policy Manager Console

Pour installer Policy Manager Console, votre système doit correspondre à la configuration requise indiquée ici.

Système d'exploitation :	Microsoft Windows : • Windows XP Professionnel (SP2 ou version ultérieure) • Windows Vista (32 ou 64 bits) avec ou sans SP1 ; éditions Business, Enterprise ou Intégrale • Windows 7 (32 ou 64 bits) ; éditions Professionnel, Entreprise ou Intégrale • Microsoft Windows Server 2003 SP1 ou ultérieur (32 bits) ; éditions Standard, Enterprise, Web Edition ou Small Business Server editions • Windows Server 2003 SP1 ou ultérieur (64 bits) ; éditions Standard ou Enterprise • Windows Server 2008 SP1 (32 bits) ; éditions Standard, Enterprise ou Web Server • Windows Server 2008 SP1 (64 bits) ; éditions Standard, Enterprise, Web Server, Small Business Server ou Essential Business Server • Windows Server 2008 R2 ; éditions Standard, Enterprise ou Web Server
Processeur :	Processeur P4 2 GHz ou plus rapide. La gestion de plus de 5 000 hôtes exige un processeur P4 3 GHz ou plus rapide.
Mémoire :	512 Mo de RAM. La gestion de plus de 5 000 hôtes exige 1 Go de mémoire.
Espace disque :	200 Mo espace libre sur le disque dur.
Affichage :	Ecran 16 bits minimum d'une résolution de 1 024 x 768 : écran 32 bits et résolution de 1 280 x 1 024 ou supérieure).
Réseau :	Réseau 10 La gestion de plus de 5 000 hôtes exige un réseau 100 Mbits.

Principaux composants

La puissance de Policy Manager repose sur l'architecture d'administration F-Secure, qui offre une grande évolutivité pour le personnel disséminé et itinérant.

Policy Manager Console

Policy Manager Console fournit une console de gestion centralisée pour assurer la sécurité des hôtes administrés du réseau. Cette console permet à l'administrateur d'organiser le réseau en unités logiques pour partager les stratégies. Ces stratégies sont définies dans Policy Manager Console puis sont diffusées aux postes de travail via Policy Manager Server. Policy Manager Console est une application *Java* qui peut être exécutée sur différentes plates-formes. Elle permet notamment d'installer Management Agent à distance sur d'autres postes de travail sans utiliser de scripts de connexion locaux, sans redémarrer l'ordinateur et sans aucune intervention de l'utilisateur final.

Policy Manager Console comporte deux interfaces utilisateur différentes :

- **Mode antivirus** : interface utilisateur optimisée pour la gestion de Client Security et Anti-virus for Workstations.
- **Mode avancé** : interface utilisateur qui peut être utilisée pour la gestion d'autres produits F-Secure.

Policy Manager Server

Policy Manager Server est le référentiel des stratégies et des packages logiciels distribués par l'administrateur, et des informations et alertes d'état envoyées par les hôtes administrés. La communication entre Policy Manager Server et les hôtes administrés s'établit via le *protocole HTTP* standard, qui assure un fonctionnement optimal aussi bien sur les réseaux locaux (*LAN*) que sur les réseaux étendus (*WAN*).

Management Agent

Management Agent met en application les stratégies de sécurité définies par l'administrateur sur les hôtes administrés et fournit l'interface utilisateur ainsi que d'autres services. Il gère toutes les fonctions d'administration sur les postes de travail locaux, fournit une interface commune à toutes les applications F-Secure et s'articule autour d'une infrastructure de gestion par stratégies.

Web Reporting

Web Reporting est un système Web de création de rapports graphiques à l'échelle de l'entreprise inclus dans Policy Manager Server. Il permet de créer rapidement des rapports graphiques basés sur les tendances passées et d'identifier les ordinateurs qui ne sont pas protégés ou qui sont vulnérables aux attaques de nouveaux virus.

Update Server & Agent

Update Server & Agent sont utilisés pour la mise à jour des définitions de virus et logiciels espions sur les hôtes administrés et sont inclus à Policy Manager Server. Automatic Update Agent permet aux utilisateurs d'obtenir les mises à jour des bases de données de définitions de virus ainsi que des données sans avoir à interrompre leur travail pour télécharger les fichiers à partir d'Internet. Il télécharge les fichiers automatiquement en tâche de fond en utilisant la bande passante non utilisée par les autres applications Internet. Si Automatic Update Agent est connecté en permanence à Internet, il reçoit automatiquement les mises à jour de définitions de virus après leur publication par F-Secure.

Fonctions

Certaines fonctions de Policy Manager sont décrites dans la présente section.

Distribution des logiciels

- Installation des produits F-Secure sur des hôtes à partir d'un emplacement central et mise à jour de fichiers exécutables et fichiers de données, y compris les mises à jour de définitions de virus.
- Les mises à jour peuvent s'effectuer de différentes manières
  - A partir d'un CD F-Secure.
  - Sur le poste client à partir du site Web F-Secure. Ces mises à jour peuvent être automatiquement distribuées par Automatic Update Agent, ou récupérées à la demande sur le site Web de F-Secure.
- Policy Manager Console peut être utilisé pour exporter des packages d'installation préconfigurés, qu'il est également possible de transmettre à l'aide d'un logiciel tiers, tel que SMS, ou des outils similaires.

Gestion de la configuration et des stratégies

- Configuration centralisée des stratégies de sécurité. L'administrateur distribue les stratégies sur le poste de travail de l'utilisateur à partir de Policy Manager Server. L'intégrité des stratégies est assurée par l'utilisation de signatures numériques.

Gestion des événements

- Rapports à Event Viewer (journaux locaux et distants), courrier électronique, fichiers de rapport et création de statistiques des événements. .

Gestion des performances

- Création de rapports et gestion des statistiques et des données relatives aux performances.

Gestion des tâches

- Gestion de la détection de virus et autres tâches.

Enregistrement du produit

Vous pouvez fournir à F-Secure des informations relatives à l'utilisation de Policy Manager en enregistrant votre produit.

Les questions et réponses suivantes offrent davantage d'informations sur l'enregistrement de votre installation de Policy Manager. Vous devez également consulter les termes de la licence F-Secure (*http://www.f-secure.com/en_EMEA/estore/license-terms/*) et la politique de confidentialité (*http://www.f-secure.com/en_EMEA/privacy.html*).

Pourquoi F-Secure collecte des données ?

Nous collectons des informations statistiques sur l'utilisation des produits F-Secure afin d'améliorer notre service. Pour un meilleur service et support F-Secure, vous pouvez nous autoriser à lier ces informations à vos informations de contact. Pour ce faire, veuillez saisir le numéro de client figurant sur votre certificat de licence lors de l'installation de Policy Manager.

Quelles sont les informations envoyées ?

Nous collectons des informations qui ne peuvent pas être liés à l'utilisateur final ou à l'utilisation de l'ordinateur. Les informations collectées incluent les versions du produit F-Secure, les versions du système d'exploitation, le nombre d'hôtes gérés et le nombre d'hôtes déconnectés. Ces informations sont ensuite transférées dans un format sécurisé et crypté.

Quel est l'avantage d'envoyer les informations à F-Secure ?

Lorsque vous contactez notre support, celui-ci pourra vous fournir une solution à votre problème plus rapidement grâce aux informations collectées. En outre, elles nous permettent également de développer davantage nos produits et services afin qu'ils répondent encore mieux aux besoins de nos clients.

Où sont stockées les informations et qui peut y accéder ?

Le données sont stockées dans un centre de données F-Secure hautement sécurisé. Et seul le personnel F-Secure habilité peut accéder aux données.

Gestion des applications

Policy Manager inclut plusieurs composants permettant de gérer les applications de votre réseau.

Management Agent

Management Agent met en application les stratégies de sécurité définies par l'administrateur sur les hôtes administrés.Il sert de composant de configuration central sur les hôtes et, par exemple, il interprète les fichiers de stratégie, envoie les demandes d'auto-enregistrement et les informations sur l'état des hôtes à Policy Manager, et effectue des installations basées sur la stratégie.

Prise en charge NAC (Cisco Network Admission Control)

F-Secure Corporation participe au programme *NAC* (*Network Admission Control*) animé par Cisco Systems®. Cisco NAC peut être utilisé pour restreindre l'accès réseau des hôtes ayant des bases de données de définitions de virus, ou des modules antivirus ou pare-feu trop anciens.

Terminologie de base

Vous trouverez dans cette section des descriptions relatives aux termes fréquemment utilisés dans ce guide.

Hôte

Hôte fait référence à un ordinateur qui est géré de manière centralisée avec Policy Manager.

Stratégie

Une stratégie de sécurité peut être définie comme l'ensemble des règles précises édictées dans le but de définir les modalités d'administration, de protection et de distribution des informations confidentielles et autres ressources. L'architecture d'administration de F-Secure exploite les stratégies configurées de manière centralisée par l'administrateur pour un contrôle total de la sécurité dans un environnement d'entreprise.

L'échange d'informations entre Policy Manager Console et les hôtes s'effectue via le transfert des fichiers de stratégie.

Domaine de stratégie

Les domaines de stratégie sont des groupes d'hôtes ou de sous-domaines disposant d'une stratégie de sécurité similaire.

Transmission des stratégies

La transmission des stratégies simplifie la définition d'une stratégie commune. Dans Policy Manager Console, chaque domaine de stratégie hérite automatiquement des paramètres de son domaine parent, ce qui permet une administration aisée et efficace des réseaux de grande taille. Vous pouvez modifier ces paramètres pour des hôtes ou des domaines individuels. Lorsque vous modifiez les paramètres hérités d'un domaine, ces modifications sont transmises à tous les hôtes et sous-domaines contenus dans ce domaine.

La stratégie peut être davantage affinée pour des sous-domaines, voire des hôtes individuels. La granularité de définitions de stratégie peut varier considérablement d'une installation à l'autre. Certains administrateurs peuvent ne vouloir définir que quelques stratégies différentes pour des domaines étendus, tandis que d'autres préféreront associer les stratégies directement à chaque hôte, obtenant ainsi la granularité la plus fine.

Chapitre
2

Installation du produit

Sujets :

- *Procédure d'installation*
- *Modification du chemin d'accès au navigateur Web*
- *Désinstallation du produit.*

Vous y trouverez des instructions pour installer les principaux composants du produit : Policy Manager Server et Policy Manager Console.

Procédure d'installation

Suivez les étapes suivantes dans l'ordre indiqué pour installer Policy Manager Server et Policy Manager Console sur le même ordinateur.

Télécharger et exécuter le package d'installation

La première étape d'installation de Policy Manager consiste à télécharger et à exécuter le package d'installation.

Pour commencer l'installation du produit :

1. Téléchargez le package d'installation sur le site *www.f-secure.com/webclub*.
   Vous trouverez le fichier dans la section **Téléchargement** de la page **Policy Manager**.
2. Cliquez deux fois sur le fichier exécutable pour lancer l'installation.
   L'installation démarre.
3. Sélectionnez la langue d'installation dans le menu déroulant, puis cliquez sur **Suivant** pour continuer.
4. Prenez connaissance du contrat de licence, puis sélectionnez **J'accepte le contrat** et cliquez sur **Suivant** pour poursuivre.

Sélection des composants à installer

La prochaine étape consiste à sélectionner les composants du produit à installer.

Pour continuer l'installation du produit :

1. Sélectionnez les composants à installer et cliquez sur **Suivant** pour poursuivre.
   - Sélectionnez Policy Manager Server et Policy Manager Console pour les installer sur le même ordinateur.
   - Sélectionnez Policy Manager Server si vous voulez installer Policy Manager Console sur un autre ordinateur.
2. Choisissez le dossier de destination, puis cliquez sur **Suivant**.
   Nous vous recommandons d'utiliser le répertoire d'installation par défaut. Si vous souhaitez installer le produit dans un répertoire différent, utilisez la fonction **Parcourir** et sélectionnez un nouveau répertoire.

   
   Remarque: Si Management Agent est installé sur le même ordinateur, cette fenêtre ne s'affichera pas.
3. Entrez votre numéro de client et cliquez sur **Suivant**.
   Vous trouverez ce numéro sur le certificat de licence fourni avec le produit.
4. Si le programme d'installation ne détecte aucune installation précédente de Policy Manager lors de la configuration, un message vous demande de confirmer qu'une installation précédente du produit existe :
   - Si une version précédente a été installée, sélectionnez **Une installation de F-Secure Policy Manager existe déjà**. Saisissez le chemin du répertoire de communication du programme Policy Manager installé. Le contenu de ce répertoire est copié sous le `<répertoire d'installation du serveur>\commdir\` (répertoire de communication sous le répertoire d'installation de Policy Manager Server), et ce répertoire sera utilisé par Policy Manager Server comme référentiel. Vous pouvez utiliser le répertoire `commdir` précédent comme sauvegarde, ou vous pouvez le supprimer une fois que vous avez vérifié que Policy Manager Server est correctement installé.
   - Si aucune version précédente n'a été installée, sélectionnez **Je n'ai pas déjà installé F-Secure Policy Manager**. Aucun répertoire `commdir` ne sera requis, et un répertoire `commdir` sera créé dans l'emplacement par défaut (sous `<répertoire d'installation de F-Secure Policy Manager 5>\commdir`).

5. Cliquez sur **Suivant** pour poursuivre.
6. Indiquez si vous souhaitez conserver les paramètres existants ou les modifier :

   Remarque: Cette boîte de dialogue s'affiche uniquement si une installation précédente de Policy Manager Server a été détectée sur l'ordinateur.

   - Par défaut, le programme d'installation conserve les paramètres existants. Sélectionnez cette option si vous avez manuellement mis à jour la configuration de Policy Manager Server. Cette option conserve automatiquement les ports d'administration, d'hôte et de génération de rapports Web existants.
   - Si vous souhaitez changer les ports d'une installation précédente, sélectionnez l'option **Modifier les paramètres**. Cette option remplace la configuration modifiée et restaure les valeurs par défaut des paramètres.
7. Cliquez sur **Suivant** pour poursuivre.
8. Sélectionnez les modules Policy Manager Server à activer :
   - Le module **Hôte** est utilisé pour la communication avec les hôtes. Le port par défaut est 80.
   - Le module **Administration** est utilisé pour la communication avec Policy Manager Console. Le port HTTP par défaut est 8080.

     Remarque: Si vous voulez modifier le port de communication par défaut, vous devez également modifier le paramètre **Numéro de port HTTP** dans Policy Manager Console.

     Par défaut, l'accès au module **Administration** est restreint à l'ordinateur local. C'est le mode d'utilisation du produit le plus sécurisé. En cas de connexion via un réseau, il est conseillé d'envisager de sécuriser la communication à l'aide de F-Secure SSH.
   - Le module **Web Reporting** est utilisé pour la communication avec Web Reporting. Indiquez si vous souhaitez l'activer. Web Reporting se connecte au module **Administration** via un socket local pour rechercher les données du serveur. Le port par défaut est 8081.

     Par défaut, l'accès à Web Reporting est également autorisé depuis les autres ordinateurs. Si vous souhaitez uniquement un accès depuis cet ordinateur, sélectionnez **Restreindre l'accès à l'ordinateur local**.
9. Cliquez sur **Suivant** pour poursuivre.
10. Sélectionnez le(s) module(s) d'installation de produits dans la liste des modules disponibles, puis cliquez sur **Suivant** pour poursuivre.

Réalisation de l'installation du produit

La prochaine étape consiste à effectuer l'installation du produit.

1. Examinez les modifications que le programme d'installation va apporter, puis cliquez sur **Démarrer** pour lancer l'installation des composants sélectionnés.
   Lorsque le programme d'installation est terminé, il indique si tous les composants ont été installés correctement.
2. Cliquez sur **Terminer** pour finaliser l'installation.
3. Redémarrez votre ordinateur si un message vous invite à le faire.

Exécuter Policy Manager Console

La dernière étape de l'installation du produit consiste à exécuter Policy Manager Console la première fois.

Pour ce faire Policy Manager Console :

1. Exécutez Policy Manager Console en sélectionnant **Démarrer** ➤ **Programmes** ➤ **F-Secure Policy Manager Console** ➤ **F-Secure Policy Manager Console**.

   Lorsque l'application Policy Manager Console est exécutée pour la première fois, l'**Assistant d'installation de la console** collecte les informations requises pour créer une connexion initiale au serveur. La première page de l'Assistant d'installation de Policy Manager Console résume le processus d'installation.
2. Cliquez sur **Suivant** pour poursuivre.
3. Sélectionnez le mode d'utilisation correspondant à vos besoins :

   - **Mode Administrateur** : active toutes les fonctions d'administration.
   - **Mode Lecture seule** : permet de consulter les données d'administration, mais pas d'apporter des modifications. Si vous sélectionnez le **Mode Lecture seule**, vous ne pourrez pas administrer les hôtes. Pour passer en **Mode Administrateur**, vous devrez disposer des clés d'administration `admin.pub` et `admin.prv`.
4. Cliquez sur **Suivant** pour poursuivre.
5. Saisissez l'adresse du serveur Policy Manager Server utilisé pour la communication avec les hôtes gérés, puis cliquez sur **Suivant** pour poursuivre.
6. Entrez le chemin d'accès au répertoire où vous souhaitez stocker les fichiers de clé privée et de clé publique de l'administrateur.

   Par défaut, les fichiers de clé sont enregistrés dans le répertoire d'installation de Policy Manager Console : `Program Files\F-Secure\Administrator`.
7. Cliquez sur **Suivant** pour poursuivre.

   Remarque: Si la paire de clés n'existe pas encore, elle sera créée plus tard, au cours du processus d'installation.
8. Déplacez votre curseur dans la fenêtre afin d'initialiser le facteur aléatoire utilisé par le générateur du jeu de clés d'administration.

   L'utilisation des déplacements de la souris assure que le facteur de l'algorithme de génération de jeu de clés est suffisamment aléatoire.

   Lorsque l'indicateur de progression atteint 100 %, la boîte de dialogue **Phrase de cryptage** s'affiche automatiquement.
9. Entrez une phrase de cryptage qui protège votre clé privée d'administration.
10. Confirmez cette phrase dans la zone **Confirmer la phrase de cryptage** et cliquez sur **Suivant**.
11. Cliquez sur **Terminer** pour terminer le processus de configuration.
    Policy Manager Console génère la paire de clés d'administration. Une fois le jeu de clés créé, Policy Manager Console démarre.

    L'assistant d'installation crée le groupe d'utilisateurs `FSPM users`. L'utilisateur qui avait ouvert une session et qui a procédé à l'installation est automatiquement ajouté à ce groupe. Pour autoriser un autre utilisateur à exécuter Policy Manager, vous devez l'ajouter manuellement au groupe d'utilisateurs `FSPM users`.

Policy Manager Consoledémarre en mode **antivirus**, qui constitue une interface utilisateur optimisée pour la gestion de Client Security, de Anti-virus for Workstations et de Anti-virus for Windows Servers. Si vous comptez utiliser Policy Manager Console pour gérer un autre produit F-Secure, vous devez utiliser l'interface utilisateur en **Mode avancé**. Vous pouvez y accéder en sélectionnant **Affichage** ➤ **Mode avancé** dans le menu.

Lorsque vous configurez les stations de travail, vous devez y installer une copie du fichier de clé `admin.pub` (ou leur donner l'accès à ce fichier). Si vous installez à distance les produits F-Secure sur des postes de travail, à l'aide de Policy Manager, une copie du fichier de clé `admin.pub` y est automatiquement installée. Par contre, si vous effectuez l'installation à partir d'un CD, vous devez transférer manuellement une copie du fichier de clés `admin.pub` sur les postes de travail. La méthode la plus avantageuse et la plus sûre consiste à copier le fichier `admin.pub` sur une disquette, puis à l'installer sur les postes de travail à partir

de cette disquette. Vous pouvez également placer le fichier `admin.pub` dans un répertoire accessible à tous les hôtes qui seront configurés avec des produits F-Secure administrés à distance.

Modification du chemin d'accès au navigateur Web

Policy Manager Console obtient le chemin d'accès au navigateur Web par défaut lors du processus d'installation.

Si vous voulez modifier ce chemin d'accès :

1. Sélectionnez **Outils** ➤ **Préférences** dans le menu.
2. Sélectionnez l'onglet **Emplacements** et entrez le nouveau chemin d'accès au fichier.

Désinstallation du produit.

Suivez les étapes ci-dessous pour désinstaller des composants Policy Manager.

Pour désintaller des composants Policy Manager :

1. Ouvrez le menu **Démarrer** Windows et accédez au **Panneau de configuration**.
2. Sélectionnez **Ajout/Suppression de programmes**.
3. Choisissez le composant à désinstaller (Policy Manager Console ou Policy Manager Server), puis cliquez sur **Ajouter/Supprimer**.
   La boîte de dialogue **Désinstallation** de F-Secure s'affiche.
4. Cliquez sur **Démarrer** pour lancer la désinstallation.
5. Au terme de la désinstallation, cliquez sur **Fermer**.
6. Recommencez les étapes ci-dessus si vous voulez désinstaller d'autres composants Policy Manager.
7. Une fois que vous avez désinstallé les composants, quittez **Ajout/Suppression de programmes**.
8. Il est recommandé de redémarrer l'ordinateur après la désinstallation.

   Le redémarrage est nécessaire pour nettoyer les fichiers restant sur l'ordinateur après la désinstallation et avant les installations suivantes des mêmes produits F-Secure.

Chapitre

3

Interface utilisateur en Mode antivirus

Sujets :

- *Onglet Domaines de stratégie*
- *Onglets de gestion*
- *Barre d'outils*
- *Options des menus*
- *Héritage des paramètres*

Cette section fournit une référence des paramètres disponibles sur les différentes pages de l'interface utilisateur en **Mode antivirus**.

Remarque: Policy Manager comprend également une autre interface utilisateur, l'interface utilisateur en **Mode avancé**. Il permet de gérer des produits autres que Client Security et Anti-virus for Workstations. Il permet également de modifier les paramètres avancés de Client Security. Vous pouvez basculer entre les deux modes en sélectionnant **Mode avancé** ou **Mode antivirus** dans le menu **Affichage**.

Les principaux composants du **Mode antivirus** sont les suivants :

- L'onglet **Domaines de stratégie** qui affiche la structure des domaines de stratégie gérés.
- Les onglets de gestion : **Synthèse**, **Paramètres**, **Etat**, **Alertes**, **Rapports**, **Installation** et **Opérations** qui peuvent être utilisés pour configurer et surveiller Client Security installé sur les hôtes ainsi que pour effectuer des opérations.
- L'écran **Message** en bas de la fenêtre affichant des messages d'information de Policy Manager, par exemple lorsque les définitions de virus ont été mises à jour sur le serveur.

Onglet Domaines de stratégie

Vous pouvez effectuer des actions pour les domaines de stratégie et des hôtes dans l'onglet **Domaines de stratégie**.

Vous pouvez effectuer les opérations suivantes dans l'onglet **Domaines de stratégie** :

- Ajouter un nouveau domaine de stratégie en cliquant sur l'icône  icône de la barre d'outils. Vous ne pouvez créer un nouveau domaine de stratégie que si vous avez sélectionné un domaine parent.
- Ajouter un nouvel hôte en cliquant sur l'icône  .
- Rechercher un hôte.
- Afficher les propriétés d'un domaine ou d'un hôte. Les noms attribués à chaque hôte et domaine doivent être sans ambiguïté.
- Importer des hôtes auto-enregistrés.
- Détecter automatiquement des hôtes d'un domaine Windows.
- Supprimer des hôtes ou des domaines.
- Déplacer des hôtes ou des domaines à l'aide des fonctions Couper et Coller.
- Exporter un fichier de stratégie.

Une fois le domaine ou l'hôte sélectionné, vous pouvez accéder à ces commandes depuis le menu **Edition**. Vous pouvez également y accéder en cliquant avec le bouton droit de la souris sur l'hôte ou le domaine. Les fonctions **Autodécouvrir** et **Importer des hôtes auto-enregistrés** sont également disponibles dans l'onglet **Installation**.

Remarque: Les domaines désignés dans ces commandes ne sont pas des domaines Windows NT ni DNS. Les domaines de stratégie sont des groupes d'hôtes ou de sous-domaines disposant d'une stratégie de sécurité similaire.

Onglets de gestion

Cette section décrit les onglets de gestion (**Résumé**, **Paramètres**, **Etat**, **Alertes**, **Rapports**, **Installation** et **Opérations**), et les différentes pages sur chaque onglet.

Onglet Résumé

L'onglet **Résumé** est conçu pour afficher les informations les plus importantes concernant le ou les domaines ou hôtes sélectionnés.

Lorsqu'un hôte individuel est sélectionné, l'onglet **Résumé** affiche des informations sur l'ensemble du domaine. Lorsqu'un hôte individuel est sélectionné, vous pouvez voir des informations détaillées concernant cet hôte.

Si certains des paramètres affichés dans l'onglet **Résumé** exigent votre attention ou une action immédiate, une icône s'affiche à côté de ces paramètres. Les icônes s'interprètent comme suit :

	Avertit d'une situation d'erreur exigeant votre intervention. L'erreur ne peut pas être corrigée automatiquement. L'icône s'affiche par exemple lorsque les stratégies les plus récentes n'ont pas été distribuées ou lorsque les définitions de virus des hôtes ne sont pas à jour.
	Avertit d'une situation pouvant exiger votre intervention. La situation ne crée pas encore de problèmes de sécurité, mais elle pourrait le faire plus tard si le problème n'est pas résolu maintenant. L'icône s'affiche par exemple lorsque des hôtes sont déconnectés.

Les informations affichées dans l'onglet **Résumé** dépendent de ce qui est sélectionné dans l'onglet **Domaines de stratégie** :

- Lorsqu'un domaine est sélectionné, l'onglet **Résumé** affiche des informations réparties en plusieurs sections comme suit : **Policy Manager**, **Domaine**, **Protection antivirus pour postes de travail** et **Protection Internet**.
- Lorsqu'un hôte est sélectionné, les sections sont : **Policy Manager**, **Hôte**, **Protection antivirus** et **Protection Internet**.

Onglet Résumé lorsqu'un domaine est sélectionné

Les informations décrites dans la présente section sont affichées dans l'onglet **Résumé** quand un domaine est sélectionné dans l'onglet **Domaines de stratégie**.

Policy Manager

Dans la section **Policy Manager**, vous pouvez :

- Voir l'état actuel de distribution des **stratégies** sous (**enregistrées**/**non enregistrées**, **distribuées**/**non distribuées**) et, si nécessaire, enregistrer les données de stratégie et distribuer les nouvelles stratégies aux hôtes.
- Voir l'état des définitions de virus sur le serveur.
- Voir l'état des définitions de logiciels espions sur le serveur.
- Voir l'état des mises à jour **DeepGuard** sur le serveur.
- Voir le nombre de nouveaux hôtes auto-enregistrés. S'il y a de nouveaux hôtes, vous pouvez les ajouter au domaine en cliquant sur **Ajouter ces hôtes à un domaine**.

- Découvrir automatiquement les hôtes d'un domaine Windows en cliquant sur **Autodécouvrir hôtes Windows**.

Domaine

Dans la section **Domaine**, vous pouvez :

- Voir le nombre d'hôtes ayant la stratégie la plus récente et accéder à une synthèse de la mise à jour de cette stratégie en cliquant sur **Afficher la mise à jour de stratégie la plus récente des hôtes**. L'onglet **Etat** et la page **Gestion centralisée** s'affichent.
- Voir le nombre d'hôtes déconnectés. Vous pouvez également accéder à une liste détaillée affichant l'état de connexion des hôtes en cliquant sur **Afficher les hôtes déconnectés...**. L'onglet **Etat** et la page **Gestion centralisée** s'affichent.
- Voir une synthèse des nouvelles alertes. Si vous souhaitez obtenir des informations plus détaillées sur les alertes, vous pouvez cliquer sur le lien **Afficher les alertes par gravité** pour accéder à l'onglet **Alertes**.

  La gravité des alertes est indiquée par les icônes suivantes

Icône	Référence	Description
	Info	Informations de fonctionnement normal émises par un hôte.
	Avertissement	Avertissement émanant de l'hôte.
	Erreur	Erreur non fatale survenue sur l'hôte.
	Erreur fatale	Erreur fatale survenue sur l'hôte.
	Alerte de sécurité	Incident lié à la sécurité survenu sur l'hôte.

Protection antivirus pour postes de travail

Dans la section **Protection antivirus pour postes de travail**, vous pouvez :

- Voir sur combien d'hôtes du domaine est installée la **protection antivirus**.
- Voir sur combien d'hôtes du domaine est activée l'**Analyse en temps réel**. Si vous souhaitez voir sur quels hôtes elle est activée ou non, cliquez sur **Afficher la protection globale des hôtes...** pour accéder à des informations plus détaillées sur l'onglet **Etat** et la page **Protection globale**.
- Voir combien d'infections ont été détectées dans le domaine. Si vous souhaitez voir des informations d'infection spécifiques à l'hôte, cliquez sur **Afficher l'état d'infection des hôtes** pour accéder à l'onglet **Etat** et à la page **Protection globale**.
- Voir combien d'hôtes disposent des définitions de virus les plus récentes et voir si les définitions de virus de certains hôtes sont récentes ou obsolètes.
  - **Récente** signifie que les définitions de virus sont les plus récentes.
  - **Obsolète** signifie que les définitions de virus sont plus anciennes que la limite de temps configurée.

    Remarque: Si F-Secure AntiVirus 5.40 est installé sur certains hôtes, la version des définitions de virus de ces hôtes est marquée comme étant **Inconnu**.

  Si vous devez mettre à jour les définitions de virus sur certains hôtes, cliquez sur **Mettre à jour les définitions de virus** pour accéder à l'onglet **Opérations**.

Protection Internet

Dans la section **Protection Internet**, vous pouvez :

- Voir sur combien d'hôtes du domaine est installé la protection Internet.
- Voir l'attaque récente la plus courante et le pourcentage du domaine affecté. Si vous souhaitez obtenir des informations plus détaillées sur les attaques les plus récentes, vous pouvez cliquer sur le lien **Afficher l'état de la protection Internet** pour accéder à l'onglet **Etat** et à la page **Protection Internet**.

Onglet Résumé lorsqu'un hôte est sélectionné

Lorsqu'un hôte est sélectionné dans l'onglet **Domaines de stratégie**, l'onglet **Résumé** affiche des informations plus détaillées dans la section **Hôte**.

Hôte

Dans la section **Hôte**, vous pouvez :

- Voir le nom de l'hôte sélectionné, affiché en regard de **Identité de l'ordinateur**. Vous pouvez également accéder à des informations plus détaillées sur l'hôte en cliquant sur **Afficher les propriétés de l'hôte**. L'onglet **Etat** et la page **Propriétés de l'hôte**.
- Voir quel est le protocole actif (HTTP ou Partage de fichiers), l'adresse de Policy Manager Server auquel est connecté l'hôte, ainsi que la date et l'heure de la dernière connexion.
- Voir si le fichier de stratégie utilisé par l'hôte est le plus récent ou non.
- Voir si l'hôte est déconnecté ou non.
- Voir une synthèse des nouvelles alertes. Si vous souhaitez obtenir des informations plus détaillées sur les alertes, cliquez sur **Afficher les alertes par gravité** pour accéder à l'onglet **Alertes**.

Protection antivirus pour postes de travail

Outre les informations affichées quand un domaine est sélectionné, la section **Protection antivirus pour postes de travail** affiche également le numéro de version des définitions de virus.

Protection Internet

Outre les informations affichées quand un domaine est sélectionné, la section **Protection Internet** affiche également le niveau de sécurité en cours de la Protection Internet pour l'hôte.

Onglet Paramètres

L'onglet **Paramètres** contient 12 pages servant à configurer les composants de Client Security, qui sont brièvement décrits dans cette section.

Menu contextuel des pages Paramètres

En cliquant avec le bouton droit sur un paramètre des pages de l'onglet **Paramètres**, vous pouvez accéder à un menu contextuel contenant les options suivantes :

Effacer	Cette option efface un paramètre redéfini au niveau actuel.
Forcer la valeur	La commande **Forcer la valeur** n'est disponible que si un domaine de stratégie est sélectionné. Vous pouvez utiliser cette commande pour forcer l'application du paramètre de domaine en cours dans tous les sous-domaines et hôtes. En pratique, cette action efface le paramètre correspondant dans tous les sous-domaines et les hôtes sous le domaine actuel, afin de leur permettre d'hériter de la valeur actuelle. Utilisez cette option avec prudence : toutes les valeurs définies dans le sous-domaine ou les hôtes

	sous le domaine sélectionné sont effacées et il est impossible de les rétablir.
Afficher les valeurs du domaine	La commande **Afficher les valeurs du domaine** n'est disponible que si un domaine de stratégie est sélectionné. Vous utiliser cette commande pour afficher la liste de tous les domaines de stratégie et des hôtes sous le domaine de stratégie sélectionné, ainsi que la valeur de la zone sélectionnée. Cliquez sur le nom d'un domaine ou d'un hôte pour le sélectionner dans l'onglet **Domaines de stratégie**. Il est possible d'ouvrir simultanément plusieurs boîtes de dialogue de **valeur de domaine**.
Localiser en mode avancé	Cette option est destinée aux utilisateurs avancés. Elle vous mène à l'interface utilisateur en **Mode avancé** et y sélectionne le paramètre.

Mises à jour automatiques.

La page **Mises à jour automatique** est divisée en deux parties : **Mises à jour automatiques** et **Neighborcast**.

Mises à jour automatiques

Dans la section **Mises à jour automatiques**, vous pouvez :

- activer ou désactiver les mises à jour automatiques. Notez que la désactivation de ce paramètre annule pour l'hôte toutes les possibilités d'obtenir des mises à jour automatiques ;
- spécifier l'intervalle d'interrogation des mises à jour en provenance de Policy Manager Server ;
- voir une liste des serveurs de Policy Manager Proxy. Vous pouvez également ajouter de nouveaux serveurs à la liste, supprimer des serveurs de la liste et modifier leurs adresses et priorités ;
- choisir si un proxy HTTP peut être utilisé et est spécifié l'adresse du proxy HTTP.
- Choisir si les clients doivent télécharger des mises à jour entre eux, en plus de celles fournies sur les serveurs ou les proxys.

Neighborcast

Neighborcast permet aux clients de télécharger des mises à jour entre eux, ainsi qu'à partir de tout serveur ou proxy disponible. Dans cette section, vous pouvez :

- Désigner un client qui distribuera les mises à jour aux autres clients.
- Désigner un client qui téléchargera les mises à jour depuis d'autres clients qui distribuent des mises à jour.
- Choisir le port à utiliser.

Analyse en temps réel

Les paramètres affichés sur cette page affectent l'analyse en temps réel des hôtes dans le domaine sélectionnée.

Sauf mention contraire, les paramètres indiqués sur cette page sont valables pour toutes les versions de Client Security. Pour afficher et configurer les paramètres qui ne sont plus valables pour Client Security 9 ou versions supérieures et Anti-virus for Windows Servers 9 ou versions supérieures , mais qui le sont toujours pour les anciennes versions du produit, cliquez sur **Paramètres pour les anciens clients (7.x, 8.x)...**.

Généralités

Cette section vous permet d'activer ou de désactiver l'analyse en temps réel.

Analyse des fichiers

Dans cette section, vous pouvez :

- Sélectionner quels fichiers seront analysés et définir les extensions incluses.
- Sélectionner si certaines extensions seront exclues de l'analyse et définir lesquelles.
- Sélectionner si les utilisateurs peuvent exclure des objets de l'analyse en temps réel.
- Sélectionner si des lecteurs réseau sont inclus dans l'analyse en temps réel.
- Définir l'action à effectuer lorsqu'un fichier infecté est détecté (pour Client Security 9 ou ultérieur et Anti-virus for Windows Servers 9 ou ultérieur).
- Activer ou désactiver la protection du fichier « Hôtes ».
- Sélectionner si les cookies de suivi sont inclus à l'analyse.

DeepGuard

Dans cette section, vous pouvez :

- Activer ou désactiver DeepGuard.
- Sélectionner l'action à effectuer lorsqu'une tentative de modification du système est détectée.
- Sélectionner si une requête doit être envoyée à un serveur distant pour améliorer la précision de la détection.
- Activer ou désactiver le contrôle avancé des processus.

Analyse manuelle

Les paramètres affichés sur cette page affecte les analyses manuelles effectuées par les utilisateurs de l'hôte.

Analyse manuelle de fichiers

Dans cette section, les options suivantes sont disponibles pour la sélection des éléments à analyser :

- Sélectionner quels fichiers seront analysés et définir les extensions incluses.
  - **Tous les fichiers** : tous les fichiers sont analysés, quelle que soit leur extension. Cette option est déconseillée car elle risque de ralentir considérablement les performances du système.
  - **Fichiers avec ces extensions** : seuls les fichiers portant les extensions définies sont analysés. Pour indiquer des fichiers sans extension, tapez `.`. Vous pouvez également utiliser le caractère générique `?` pour représenter une lettre quelconque. Séparez chaque extension de fichier par un espace.
- Indiquer si les fichiers compressés doivent être analysés. Cochez cette case pour analyser les fichiers compressés `ZIP`, `ARJ`, `LZH`, `RAR`, `CAB`, `TAR`, `BZ2`, `GZ`, `JAR` et `TGZ`. L'analyse de fichiers compressés volumineux sollicite de nombreuses ressources système et risque donc de ralentir le système.
- Sélectionner si certaines extensions seront exclues de l'analyse et définir lesquelles. Vous pouvez spécifier si certains fichiers ne doivent pas être analysés et entrer les extensions à exclure de l'analyse dans le champ **Extensions exclues**.
- Sélectionner si les utilisateurs peuvent exclure des objets de l'analyse en temps réel. Lorsque l'option **Activer les objets exclus** est sélectionnée, les utilisateurs peuvent spécifier des fichiers ou dossiers individuels qui ne seront pas analysés.
- Dans la liste déroulante **Action en cas d'infection**, vous pouvez sélectionner l'action que devra exécuter Client Security lors de la détection d'un fichier infecté. Sélectionnez l'une des actions suivantes :

Action	Définition
Interroger l'utilisateur après analyse	Démarre l'**Assistant de nettoyage** quand un fichier infecté est détecté.

Action	Définition
Nettoyer automatiquement	Nettoie le fichier automatiquement lorsqu'un virus est détecté.
Renommer automatiquement	Renomme le fichier automatiquement lorsqu'un virus est détecté.
Supprimer automatiquement	Supprime le fichier automatiquement lorsqu'un virus est détecté. Notez que cette option supprime également l'objet infecté par le virus. Cette option est donc déconseillée.
Signaler uniquement	Indique qu'un virus a été détecté et vous empêche d'ouvrir l'objet infecté. Cette option se contente de vous signaler la présence du virus. Elle n'entreprend aucune action à son encontre.

Analyse des rootkits

Dans cette section, vous pouvez

- Activez ou désactivez la recherche de rootkits.
- Inclure ou exclure l'analyse des rootkits dans l'analyse complète de l'ordinateur.
- Spécifier si les éléments suspects détectés doivent être affichés dans l'assistant de nettoyage et dans le rapport d'analyse après une vérification complète de l'ordinateur.

Analyse planifiée

Le lien **Configurer le partage de fichiers en mode avancé...** ouvre l'interface utilisateur en **Mode avancé** qui permet la configuration du partage de fichiers.

Analyse manuelle du secteur d'amorçage

Dans cette section, vous pouvez

- Activer ou désactiver l'analyse manuelle des secteurs d'amorçage des disquettes.
- Sélectionner l'action à effectuer lorsqu'une infection est détectée.

Contrôle des logiciels espions

Les paramètres affichés sur cette page sont spécifiques aux logiciels espions. Ces paramètres sont destinés à une analyse en temps réel et manuelle.

Applications exclues de la recherche manuelle

Cette table affiche une liste des logiciels espions et riskwares que les administrateurs ont autorisé à exécuter sur les hôtes.

Logiciels espions et riskwares rapportés par les hôtes

Cette table affiche les logiciels espions et riskwares que les hôtes ont signalé et ceux mis en quarantaine sur l'hôte ou les hôtes. La table affiche le type et la gravité pour chaque application logicielle espion ou riskware détectée. Tout logiciel espion ou riskware ayant l'état **Potentiellement actif** a été autorisé de s'exécuter sur l'hôte par l'administrateur.

Si vous voulez que les utilisateurs puissent être capables de décider d'autoriser certains logiciels espions et riskwares, cela est possible à l'aide de la liste déroulante **Autoriser les utilisateurs à définir les éléments de logiciels espions autorisés**.

Gestion de la quarantaine

Cette page permet de gérer les antiprogrammes qui ont été mis en quarantaine sur les hôtes administrés.

Contenu de la quarantaine

Ce table affiche des éléments en quarantaine sur les hôtes. Chaque ligne de la table affiche le type d'objet, le nom, le chemin d'accès au fichier et le nombre d'hôtes sur lesquels l'objet a été mis en quarantaine.

Actions à effectuer sur les objets en quarantaine

Cette table affiche une liste des objets en quarantaine qui ont été traités. Les objets en quarantaine sont soit libérés (autorisés) soit supprimés. L'action indiquée ici est distribuée aux hôtes administrés. Ainsi, dès que l'antiprogramme est détecté sur un hôte, l'action sélectionnée est appliquée. Quand l'action est définie sur **Libérer**, une règle d'exclusion appropriée doit exister sur la page **Contrôle des logiciels espions** ou **Analyse en temps réel**, en fonction du type d'objet afin d'empêcher une nouvelle mise en quarantaine de l'objet dans le futur.

Les actions appliquées sont automatiquement effacées de cette table dès qu'il ne reste plus d'actions en attente pour les hôtes correspondants (aucun hôte ne signale cet objet come étant en quarantaine).

Analyse du courrier électronique

Cette page comporte des paramètres distincts pour l'analyse des messages entrants et sortants. Les paramètres de la section **Généralités** sont communs aux deux types de messages.

Analyse du courrier électronique entrant

Dans cette section, vous pouvez

- Activer ou désactiver l'analyse du courrier électronique entrant.
- Sélectionner l'action à exécuter si une pièce jointe entrante est infectée.
- Sélectionner l'action à exécuter en cas d'échec de l'analyse.
- Sélectionner l'action à exécuter si des parties du message sont déformées.

Analyse du courrier électronique sortant

Dans cette section, vous pouvez

- Activer ou désactiver l'analyse du courrier électronique sortant.
- Sélectionner l'action à exécuter si une pièce jointe sortante est infectée.
- Sélectionner l'action à exécuter en cas d'échec de l'analyse.
- Sélectionner l'action à exécuter si des parties du message sont déformées.
- Choisir d'enregistrer les messages bloqués dans la boîte d'envoi de l'utilisateur.

Généralités

Dans cette section, vous pouvez

- Sélectionner si l'analyse du courrier électronique porte également sur les pièces jointes compressées.
- Sélectionner si la progression de l'analyse est affichée et définir après combien de temps elle s'affiche.
- Sélectionner si le rapport d'analyse est affiché lorsque des messages infectés sont détectés ou lorsque l'analyse échoue.

Analyse du trafic Web

Les paramètres affichés sur cette page sont liés à l'analyse du trafic Web, par exemple les fichiers téléchargés.

Généralités

Dans cette section, vous pouvez activer ou désactiver HTTP.

Analyse HTTP

- Sélectionner l'action à prendre en cas d'infection.
- Sélectionner l'action à prendre en cas d'échec de l'analyse.
- Choisir si les fichiers compressés doivent être inclus dans l'analyse.

Sites HTTP approuvés

Cette table affiche la liste des sites HTTP qui sont définis comme étant approuvés. Les téléchargements effectués à partir de ces sites ne sont pas analysés pour rechercher des virus.

Niveaux de sécurité du pare-feu

Les paramètres de cette page permettent de déterminer le niveau de sécurité globale sur l'hôte ou le domaine sélectionné.

Généralités

Dans cette section, vous pouvez :

- Sélectionner le niveau de sécurité prédéfini pour l'hôte.
- Configurer la sélection automatique du niveau de sécurité en cliquant sur **Configurer la sélection automatique du niveau de sécurité en mode avancé**. L'interface utilisateur en **Mode avancé** s'affiche.
- Activer les règles de pare-feu du niveau de sécurité actuel à appliquer aux paquets entrants et sortants en sélectionnant **Activer le moteur pare-feu**.
- Activer l'utilisation de l'interface approuvée.
- Activer ou désactiver la fonction de contrôle des applications.

Table des niveaux de sécurité du pare-feu (globale)

Cette table indique les niveaux de sécurité disponibles globalement dans le système. La table des niveaux de sécurité est la même pour tous les domaines de stratégie, mais l'activation et la désactivation de niveaux de sécurité individuels peuvent être effectuées au niveau de chaque domaine de stratégie.

Quarantaine réseau

Dans cette section, vous pouvez :

- Activer ou désactiver la quarantaine réseau.
- Spécifier l'âge des définitions de virus après lequel la **quarantaine réseau** est activée.
- Spécifier si la désactivation de l'analyse en temps réel sur l'hôte active la **quarantaine réseau**.

Prévention des intrusions

Dans cette section, vous pouvez :

- Activer ou désactiver la prévention des intrusions.
- Sélectionner l'action à exécuter en cas de détection d'un paquet malveillant. Les options disponibles sont les suivantes :
  - Consigner et supprimer.

  - Consigner sans éliminer.
- Définir la gravité d'alerte centralisée.
- Définir le niveau d'alerte et de performances.

Règles de pare-feu

Cette page permet de définir les règles appliquées aux différents niveaux de sécurité du pare-feu.

Tableau des règles de firewall

Cette table répertorie les règles définies pour les différents niveaux de sécurité. Vous pouvez sélectionner le niveau dans le menu déroulant **Niveau de sécurité de protection Internet en cours de modification**. Lorsque le niveau de sécurité sélectionné est modifié, les règles associées au nouveau niveau de sécurité s'affichent dans le tableau.

Lorsque le pare-feu est utilisé, les règles de celui-ci sont vérifiées dans l'ordre où elles s'affichent dans la table, de haut en bas. Pour les niveaux de sécurité munis d'un mode de filtrage **Normal**, il est possible de définir des règles spécifiques aux domaines ou aux hôtes. Lorsque l'option **Autoriser les utilisateurs à définir des nouvelles règles** est sélectionnée, les utilisateurs finaux sont également autorisés à définir de nouvelles règles pour le niveau de sécurité en question. La table indique également l'emplacement de ces règles.

La table des **règles de pare-feu** affiche les informations suivantes pour chaque règle :

- Que la règle soit activée ou non
- Le nom et le commentaire associés à la règle.
- Le type de règle (autoriser/refuser).
- Le service et la direction associés : **<=** pour un service entrant, **=>** pour un service sortant et **<=>** pour un service bidirectionnel.
- Les hôtes distants affectés.
- Que l'envoi des alertes soit activé ou non
- Si la règle s'applique uniquement lorsqu'une liaison d'accès à distance est utilisée.

Pour modifier l'emplacement des nouvelles règles définies par l'utilisateur dans le tableau, cliquez sur **Les règles définis par l'utilisateur vont ici**. Ensuite, vous pouvez utiliser les boutons **Déplacer vers le haut** et **Déplacer vers le bas** pour aller à l'emplacement des règles des utilisateurs dans la table.

En outre, le **Contrôle des applications** créera automatiquement des règles sur l'hôte pour les applications qui ont été autorisées. Les règles sont placées juste avant la première règle **Refuser l'accès** dans la table de règles, qui est la première règle de refus avec le service **Tout le trafic** et l'hôte distant **Tout**. Les règles permettent les paquets entrants aux applications serveur, et un pare-feu autorise ensuite les paquets de réponse sortants à partir des applications serveur. Les paquets sortants des applications ordinaires doivent être autorisés par les règles de la table des règles de pare-feu.

Services de pare-feu

Un service (abréviation de service de réseau) correspond à un service disponible sur le réseau, par exemple, le partage de fichiers, l'accès distant à la console ou la navigation sur le Web. Il est généralement décrit par le protocole et le port qu'il utilise.

Table des services de pare-feu (globale)

Cette table affiche une liste de services définis pour le pare-feu. Il est également possible de créer ou de permettre aux utilisateurs finaux de créer de nouveaux services pour le pare-feu.

Vous pouvez également empêcher les utilisateurs d'ajouter de nouveaux services en cliquant sur **Limité**, puis en sélectionnant **Taille fixe** dans la boîte de dialogue qui s'affiche. Une fois cette option sélectionnée, les utilisateurs ne peuvent pas ajouter ou supprimer des lignes des tableaux.

Contrôle des applications

Les paramètres de cette page permettent de contrôler les applications qui utilisent des connexions réseau entrantes et sortantes.

Règles d'application pour les applications connues

Cette section affiche la liste des applications connues et des règles qui leur sont associées pour les tentatives de connexion entrantes et sortantes.

Applications inconnues rapportées par les hôtes

Cette liste répertorie les applications que les hôtes ont signalées et pour lesquelles il n'existe pas encore de règles.

Dans cette section, vous pouvez aussi :

- Sélectionner l'action par défaut pour les applications clientes.
- Sélectionner l'action par défaut pour les applications serveur.
- Choisir si les nouvelles applications doivent vous être signalées en cochant la case Répertorier les nouvelles applications inconnues.

Décisions automatiques

Cette section vous permet de choisir si l'utilisateur est invité à prendre une décision quand l'application a été identifiée par DeepGuard ou par le réseau de protection en temps réel.

Message pour les utilisateurs

Cette section contient les options suivantes :

- Choisissez si les utilisateurs peuvent voir les messages par défaut en cas de tentatives de connexion par une application inconnue.
- L'option **Définir les messages par défaut** ouvre la fenêtre **Définir les messages**, où vous pouvez définir les messages affichés en cas d'autorisation, refus, ou décision de l'utilisateur pour les applications connues et inconnues.

Protection de la navigation

Les paramètres de cette page définissent les paramètres de protection de la navigation pour les hôtes qui intègrent Client Security 9 ou une version supérieure.

Exploit Shield

Dans cette section, vous pouvez sélectionner si la protection de la navigation utilise Exploit Shield pour bloquer l'accès aux sites Web qui contiennent des exploits.

Exploit Shield identifie et empêche les sites Web malveillants d'utiliser les vulnérabilités pour, par exemple, forcer un téléchargement non autorisé qui contient un antiprogramme. Il ne vous protège pas contre les fichiers que vous avez intentionnellement téléchargé et qui peuvent contenir des antiprogrammes ; ce type de menace est gérée par la recherche de virus et de logiciels espions.

Protection basée sur la réputation

Les paramètres de cette section définissent l'affichage des évaluations des sites Web et si ces derniers seront bloqués ou non pour les utilisateurs s'ils sont reconnus comme nuisibles. Ces évaluations de sécurité sont fondées sur des informations provenant de sources diverses, telles que les analystes d'antiprogrammes F-Secure et les partenaires F-Secure, ainsi que d'autres évaluations fournies par d'autres utilisateurs de la protection de la navigation.

Sites approuvés

Si la protection de la navigation bloque l'accès à une page que vous considérez comme saine et à laquelle les utilisateurs doivent pouvoir accéder, vous pouvez toujours définir cette page comme site approuvé. Tous les sites approuvés seront répertoriés ici.

Paramètres avancés

Vous pouvez cliquer sur **Configurer les paramètres avancés** pour accéder aux paramètres de la protection de la navigation dans le **Mode avancé**.

Envoi d'alertes

Les paramètres de cette page définissent l'affichage des alertes et l'envoi de celles-ci aux administrateurs.

Généralités

Cette section permet de sélectionner la langue des alertes.

Envoi d’alertes par courrier électronique

- Définir l'adresse du serveur de messagerie (SMTP).
- Définir l'adresse d'expéditeur et l'objet à utiliser lors de la transmission d'alertes par courrier électronique.

Transmission des alertes

Cette table permet de configurer la destination des alertes d'une certaine gravité.

Gestion centralisée

Cette page inclut des paramètres qui contrôlent l'application des paramètres Client Security sur le réseau.

Généralités

Cette section contient les options suivantes :

- **Autoriser les utilisateurs à modifier tous les paramètres...**

  Cette option détermine comme non finaux tous les paramètres des interfaces utilisateur **Antivirus** et **Mode avancé**, ce qui signifie que les utilisateurs sont autorisés à modifier tous les paramètres.
- **N'autoriser aucun utilisateur à changer les paramètres**

  Cette option détermine comme finaux tous les paramètres des interfaces utilisateur **Antivirus** et **Mode avancé**, ce qui signifie que les utilisateurs ne sont pas autorisés à modifier tous les paramètres.
- **Effacer tous les paramètres**

  Cette option rétablit les paramètres par défaut pour tous les composants de Client Security.
- **Autoriser les utilisateurs à suspendre tous les téléchargements et mises à jour**

  Cette option définit si l'utilisateur est autorisé à suspendre temporairement les communications réseau, telles que l'interrogation automatique de stratégies et l'envoi de statistiques et de mises à jour automatiques.

  Elle est utile pour les hôtes qui utilisent parfois une ligne d'accès à distance lente.
- **Autoriser les utilisateurs à désinstaller les produits F-Secure**

  Lorsque cette option est désactivée, les utilisateurs ne peuvent pas désinstaller le logiciel F-Secure de leur ordinateur. La désinstallation exige toujours des droits administratifs. Cette option s'applique à tous les systèmes d'exploitation Windows, y compris Windows NT/2000/XP où l'utilisateur final possède des droits d'administrateur.

Pour désinstaller le logiciel localement, vous devez soit sélectionner cette option, soit arrêter d'abord le service Management Agent avant de procéder à la désinstallation.

- **Autoriser l'utilisateur à décharger des produits**

  Les valeurs possibles sont : **Toujours autorisé**, **Autorisé sur les installations autonomes seulement**, **Non autorisé**.

  Cette option indique si l'utilisateur est autorisé à décharger temporairement tous les produits F-Secure, par exemple pour libérer de la mémoire pour un jeu ou une application similaire. Notez que les fonctions principales des produits sont désactivées aussi longtemps que le produit est déchargé et que l'ordinateur devient donc vulnérable aux virus et aux attaques.

- **Définition de connexion lente**

  Cette variable définit quelles connexions réseau sont considérées comme lentes. L'unité est le kilobit par seconde. Notez que la vitesse nominale de la connexion n'est pas significative, mais que la vitesse réelle de la connexion est mesurée. La valeur par défaut `0` (zéro) signifie que toutes les connexions sont considérées comme rapides.

Paramètres de Policy Manager Server

- **Policy Manager Server**

  Adresse URL de Policy Manager Server.

- **Intervalle de récupération des packages entrants**

  Définit la fréquence à laquelle l'hôte essaie de récupérer les packages entrants depuis Policy Manager Server, par exemple les fichiers de stratégie de base. La valeur par défaut de l'intervalle est fixée à 10 minutes.

- **Intervalle de mise à jour des packages sortants**

  Définit la fréquence à laquelle l'hôte tente d'envoyer à Policy Manager Server des nouvelles versions des informations envoyées périodiquement, par exemple des statistiques. La valeur par défaut de l'intervalle est fixée à 10 minutes.

Onglet Etat

Les différentes pages de l'onglet **Etat** affichent des informations détaillées sur l'état de certains composants d'applications Client Security gérées de façon centralisée.

Si vous sélectionnez un domaine dans l'onglet **Domaines de stratégie**, l'onglet **Etat** affiche l'état de tous les hôtes de ce domaine. Si un seul hôte est sélectionné, l'onglet **Etat** affiche l'état de cet hôte.

👉 **Remarque:** En cliquant avec le bouton droit sur les en-têtes de colonne des pages **Etat**, vous pouvez déterminer quelles colonnes doivent être affichées sur cette page.

Menu contextuel de l'onglet Etat

En cliquant avec le bouton droit sur une ligne de la page de l'onglet **Etat**, vous pouvez accéder à un menu contextuel contenant les options suivantes :

- **Copier comme texte** copie les lignes actuellement sélectionnées et les en-têtes de colonne de la table sous forme de texte.
- **Sélectionner tout** sélectionne toutes les lignes du tableau.
- **Sélectionner les hôtes dans l'arborescence du domaine** peut être utilisée pour sélectionner les hôtes et afficher leur emplacement dans l'arborescence du domaine.

Protection globale

La page **Protection globale** affiche un récapitulatif des fonctions de protection activées sur chaque hôte :

- Si l'analyse en temps réel est activée ou non.
- Niveau de sécurité de la protection Internet actuellement utilisé.
- Si l'analyse du courrier électronique des messages entrants et sortants est activée ou désactivée.
- Si la protection basée sur la réputation est utilisée ou non.
- Si la protection contre les exploits est utilisée ou non.

Mises à jour automatiques.

La page Mises à jour automatiques affiche un récapitulatif des bases de données de définition des virus pour les produits installés sur les hôtes :

- La date et l'heure de la dernière mise à jour des définitions de virus.
- Version des définitions de virus.
- La date et l'heure de la dernière mise à jour des définitions de virus sur des produits F-SecureGateway.
- Delta de mise à jour est l'écart de temps entre la dernière mise à jour des définitions de virus sur l'hôte et la dernière fois que l'hôte a envoyé des statistiques à Policy Manager.
- Version des définitions de virus sur les produits Gateway.
- La date et l'heure de la dernière mise à jour des définitions de logiciels espions.
- Version de définitions de logiciels espions.
- La date et l'heure de la dernière mise à jour de définitions de courrier indésirable sur des produits Gateway.
- Version des définitions de courrier indésirable sur les produits Gateway.

Les informations de date et de version des définitions de virus sont également affichées pour les hôtes sur lesquels Anti-virus for Citrix Servers, Anti-virus for Windows Servers, Internet Gatekeeper ou Anti-virus for Microsoft Exchange sont installés.

Protection antivirus

La page **Protection antivirus** affiche les informations suivantes :

- Date de la dernière infection.
- Nom de la dernière infection.
- Dernier objet infecté.
- Dernière action après infection.
- Nombre total d'infections.

Protection Internet

La page **Protection Internet** affiche les informations suivantes :

- Date et heure de la dernière attaque dans la colonne **Horodatage de la dernière attaque**.
- Service de la dernière attaque.
- Source de la dernière attaque.
- Attaques récentes (vous pouvez trier cette colonne en cliquant sur son en-tête).
- Réinitialisation des attaques récentes

Logiciels installés

La page **Logiciels installés** affiche une synthèse des logiciels installés sur les hôtes :

- Client Security - version du logiciel (y compris le numéro de compilation et correctifs possibles).
- Liste de correctifs anti-logiciels espions.
- Si la protection Internet est installée.

- Si l'analyse du courrier électronique est installée.
- Si l'analyse du trafic Web est installée.
- Si la protection de la navigation est installée.
- Si DeepGuard est installé.
- Policy Manager Proxy - version du logiciel.

Gestion centralisée

La page **Gestion centralisée** affiche un résumé des informations relatives à la gestion centralisée :

- Horodateur du fichier de stratégie.
- Compteur du fichier de stratégie (numéro du fichier de stratégie actuellement utilisé sur l'hôte).
- La date à laquelle la dernière mise à jour des statistiques a été envoyée à Policy Manager.
- Si l'hôte est déconnecté (vous pouvez trier cette colonne en cliquant sur son en-tête).
- Le nombre de nouvelles alertes de sécurité.
- Le nombre de nouvelles erreurs fatales.

Propriétés hôtes

La page **Propriétés hôtes** affiche les informations suivantes sur chaque hôte :

- Le nom WINS de l'hôte.
- L'adresse IP de l'hôte.
- Le nom DNS de l'hôte.
- Le système d'exploitation de l'hôte.

Onglet Alertes

L'onglet **Alertes** affiche les alertes des hôtes et domaines sélectionnés. Il peut également être utilisé pour gérer les rapports d'alerte.

L'onglet **Alertes** affiche les informations suivantes pour chaque alerte :

- la gravité,
- la date et l'heure,
- la description,
- l'hôte et l'utilisateur et
- produit sur lequel porte l'alerte.

Lorsque vous sélectionnez une alerte dans la liste, la partie inférieure de la page affiche des informations spécifiques sur celle-ci : produit, gravité, hôte d'origine, etc. Les alertes d'analyse émises par Client Security peuvent être associées à un rapport. Ce report sera affiché dans la partie inférieure de la page.

En cliquant sur **Configurer la transmission des alertes**, vous pouvez accéder à l'onglet **Paramètres** et la page **Alertes**, où vous pouvez configurer la transmission d'alertes.

Onglet Rapports

L'onglet **Rapports** affiche des rapports d'analyse antivirus des hôtes et domaines sélectionnés. Il peut également être utilisé pour gérer les rapports d'analyse.

L'onglet **Rapports** affiche les informations suivantes sur chaque rapport :

- la gravité,
- la date et l'heure,
- la description,
- l'hôte et l'utilisateur, et
- le produit concerné.

Lorsqu'une ligne est sélectionnée dans la liste des rapports, le rapport d'analyse correspondant s'affiche dans la partie inférieure de la page.

Onglet Installation

L'onglet **Installation** est le premier qui s'ouvre quand Policy Manager Console est installé.

L'onglet **Installation** contient des raccourcis vers toutes les fonctions liées à l'installation. Il affiche également une liste des packages d'installation de logiciel disponibles.

Autodécouvrir hôtes Windows...	La fonction de découverte automatique détecte automatiquement les domaines et hôtes de Windows, charge le logiciel d'installation et importe de nouveaux hôtes dans l'arborescence des domaines de stratégie.
Distribuer l'installation aux hôtes Windows...	L'installation de type « push » permet une installation directe sur des hôtes Windows spécifiques d'après leur adresse IP ou leur nom d'hôte. Cette fonction permet d'installer le logiciel sur les hôtes même s'ils n'apparaissent pas dans la liste de domaines NT de l'écran **Autodécouvrir**.
Importer des hôtes auto	Les hôtes envoient des messages d'enregistrement automatique à Policy Manager lorsque le premier produit est installé sur les hôtes. Ces nouveaux hôtes sont intégrés dans la gestion des stratégies par leur importation dans l'arborescence des domaines de stratégie.
Packages d'installation	L'écran **Packages d'installation** affiche les modules d'installation disponibles et des informations détaillées sur leur contenu.

Remarque: En raison de modifications apportées dans Mises à jour automatiques, les définitions de virus sur le serveur ne peuvent plus être mises à jour manuellement en demandant l'opération depuis Policy Manager Console. Il est uniquement possible de les mettre à jour manuellement sur Policy Manager Server à l'aide d'un outil spécial.

Onglet Opérations

Nous vous conseillons d'utiliser les opérations disponibles dans cet onglet après l'apparition d'un virus sur le réseau local.

L'onglet **Opérations** contient deux opérations :

Opération de mise à jour des définitions de virus	Cette opération permet d'ordonner aux hôtes sélectionnés ou à tous les hôtes du domaine sélectionné d'aller chercher immédiatement de nouvelles définitions de virus.
Opération de recherche de virus et de logiciels espions	Cette opération permet d'ordonner aux hôtes sélectionnés ou à tous les hôtes du domaine sélectionné de commencer immédiatement à chercher des virus et des logiciels espions.

L'emploi de ces deux opérations est recommandé après l'apparition d'un virus sur le réseau local.

Barre d'outils

La barre d'outils contient des boutons pour les tâches de Policy Manager Console

	Enregistre les données de stratégie.
	Distribue la stratégie.
	Accède au domaine ou à l'hôte précédent dans l'historique de sélection de l'arborescence.
	Accède au domaine ou à l'hôte suivant dans l'historique de sélection de l'arborescence.
	Accède au domaine parent.
	Coupe un hôte ou un domaine.
	Colle un hôte ou un domaine.
	Ajoute un domaine au domaine actuellement sélectionné.
	Ajoute un hôte au domaine actuellement sélectionné.
	Affiche la boîte de dialogue **Propriétés** d'un domaine ou d'un hôte.
	Démarre l'outil **Autodécouvrir hôtes Windows**. De nouveaux hôtes vont être ajoutés au domaine de stratégie actuellement sélectionné.
	Démarre l'installation distante sur les hôtes Windows.
	Importe des hôtes auto-enregistrés dans le domaine actuellement sélectionné. Si cette icône est verte, cela signifie que l'hôte a envoyé une demande d'auto-enregistrement.
	Affiche les packages d'installation disponibles.
 ou 	Affiche toutes les alertes. L'icône est mise en surbrillance s'il existe de nouvelles alertes. Lorsque vous démarrez Policy Manager Console, l'icône est toujours mise en surbrillance.

Options des menus

Cette section fournit une référence pour les options de menus disponibles dans Policy Manager Console.

Menu	Commande	Action
Fichier	Nouvelle stratégie	Crée une instance de données de stratégie à l'aide des paramètres par défaut de la base d'informations de gestion (MIB). Cette option est rarement utilisée car les données de stratégie existantes sont généralement modifiées, puis enregistrées à l'aide de l'option **Enregistrer sous**.
	Ouvrir une stratégie	Ouvre les données d'une stratégie précédemment enregistrée.
	Enregistrer les modifications de stratégie	Enregistre les données de stratégie actuelles.
	Enregistrer la stratégie sous	Enregistre les données de stratégie sous le nom spécifié.
	Distribuer des stratégies	Distribue les fichiers de stratégie.
	Exporter le fichier de stratégie de l'hôte	Exporte les fichiers de stratégie.
	Quitter	Ferme Policy Manager Console.
Edition	Couper	Coupe l'élément sélectionné.
	Coller	Colle l'élément à l'emplacement sélectionné.
	Supprimer	Supprime l'élément sélectionné.
	Nouveau domaine de stratégie	Ajoute un nouveau domaine.
	Nouvel hôte	Ajoute un nouvel hôte.
	Importer des hôtes auto-enregistrés	Importe les hôtes qui ont envoyé une demande d'auto
	Autodécouvrir hôtes Windows	Importe des hôtes à partir de la structure de domaine Windows.
	Distribuer l'installation aux hôtes Windows	Installe le logiciel à distance et importe les hôtes définis par l'adresse IP ou le nom WINS.
	Rechercher	Recherche une chaîne dans les propriétés de l'hôte. La recherche est effectuée sur tous les hôtes du domaine sélectionné.
	Propriétés de domaine/d'hôte	Affiche la page des **propriétés** de l'hôte ou du domaine de stratégie sélectionné.
Affichage	Editeurs de restriction intégrés	Bascule entre l'éditeur de restriction intégré et la boîte de dialogue des restrictions.
	Volet Messages	Affiche ou masque le volet **Message** en bas de l'écran.
	Ouvrir pour un nouveau message	S'il est sélectionné, le volet **Message** s'ouvre automatiquement quand un nouveau message est reçu.
	Retour	Accède au domaine ou à l'hôte précédent dans l'historique de sélection de l'arborescence.
	Suivant	Accède au domaine ou à l'hôte suivant dans l'historique de sélection de l'arborescence.

Menu	Commande	Action
	Domaine parent	Accède au domaine parent.
	Toutes les alertes	Ouvre la page **Alertes** pour afficher toutes les alertes.
	Mode avancé	Active l'interface utilisateur en **Mode avancé**.
	Mode antivirus	Active l'interface utilisateur en **Mode antivirus**, qui est optimisée pour une gestion centralisée de Client Security.
	Actualiser <Elément>	Permet d'actualiser manuellement l'affichage du rapport, de l'état ou de l'alerte. L'élément de menu varie en fonction de l'onglet ou de la page sélectionné.
	Actualiser tout	Permet d'actualiser manuellement toutes les données concernant l'interface : stratégie, état, alertes, rapports, packages d'installation et demandes d'auto-enregistrement.
Outils	Packages d'installation	Affiche dans une boîte de dialogue les informations relatives aux packages d'installation.
	Modifier la phrase de cryptage	Change la phrase de cryptage de connexion (la phrase de cryptage protégeant la clé privée de Policy Manager Console.
	Transmission des rapports	Vous permet de sélectionner les méthodes de transmission de rapports, les domaines/hôtes et les produits inclus dans les rapports.
	Préférences	Définit les propriétés locales de Policy Manager Console. Ces propriétés concernent uniquement l'installation locale de Policy Manager Console.
Aide	Sommaire	Affiche l'index de l'**Aide**.
	Enregistrer	Ouvre une boîte de dialogue qui vous permet d'enregistrer le produit.
	Contacts	Affiche les coordonnées des contacts de la société F-Secure.
	A propos de F-Secure Policy Manager Console	Affiche les informations de version.

Héritage des paramètres

Cette section explique comment fonctionne l'héritage des paramètres et comment les paramètres hérités et les paramètres redéfinis au niveau actuel sont affichés dans l'interface utilisateur.

Les paramètres de Policy Manager Console peuvent soit être hérités d'un niveau supérieur dans la structure des domaines de stratégie, soit avoir été changés au niveau actuel. Lorsqu'un paramètre redéfini localement est effacé (en cliquant sur le lien **Effacer** qui lui correspond), la valeur d'un niveau de domaine supérieur ou la valeur par défaut du paramètre est rétablie.

Au besoin, les paramètres peuvent être définis comme finaux, ce qui signifie que les utilisateurs ne sont pas autorisés à les modifier. Cela force toujours l'application de la stratégie : la variable de stratégie écrase toutes les valeurs de l'hôte local et l'utilisateur final ne peut modifier ces valeurs tant que la restriction **Final** est définie. Si les paramètres n'ont pas été définis comme étant finaux, les utilisateurs sont autorisés à les modifier.

Affichage de l'héritage des paramètres dans l'interface utilisateur

Les paramètres hérités et les paramètres redéfinis au niveau actuel sont affichés différemment dans l'interface utilisateur de Policy Manager.

Non hérité	Hérité	Description
		Un cadenas fermé signifie que l'utilisateur ne peut pas changer ce paramètre parce qu'il a été défini comme final. Si le symbole est bleu, le paramètre a été redéfini au niveau actuel. S'il est gris, le paramètre est hérité.
		Un verrou ouvert signifie que l'utilisateur est autorisé à modifier le paramètre au niveau actuel. Si le symbole est bleu, le paramètre a été redéfini au niveau actuel. S'il est gris, le paramètre est hérité.
Effacer		Si le lien **Effacer** s'affiche à côté d'un paramètre, le paramètre a été redéfini au niveau actuel et peut être effacé. Lorsque le paramètre est effacé, sa valeur par défaut ou la valeur héritée est rétablie. Si rien n'est affiché à côté d'un paramètre, c'est que le paramètre est hérité.
Zones de texte		Les valeurs héritées sont affichées en gris. Les paramètres qui ne sont pas hérités sont affichés en noir sur blanc.

Non hérité	Hérité	Description
Cases à cocher		Les valeurs héritées sont affichées en grisé sur fond gris. Les valeurs qui ne sont pas héritées sont affichées sur un fond blanc.

Verrouillage et déverrouillage simultanés de tous les paramètres d'une page

Vous pouvez choisir de verrouiller ou de déverrouiller les paramètres d'une page.

Les liens suivants peuvent être utilisés pour verrouiller et déverrouiller tous les paramètres d'une page :

Autoriser les modifications utilisateur	Déverrouille tous les paramètres auxquels est associé un verrou sur la page actuelle. Après cela, les utilisateurs peuvent modifier les paramètres en question.
Interdire les modifications utilisateur	Verrouille tous les paramètres auxquels est associé un verrou sur la page actuelle. Après cela, les utilisateurs ne peuvent pas modifier les paramètres en question.
Effacer tout...	Efface tous les paramètres qui ont été redéfinis sur la page actuelle et rétablit les valeurs par défaut ou héritées.

Héritage des paramètres dans les tables

L'héritage de paramètres s'affiche aussi sur les tables des pages de paramètres.

La table des **niveaux de sécurité de pare-feu** et la table des **services de pare-feu** sont des tables dites « globales », ce qui signifie que tous les ordinateurs du domaine utilisent les mêmes valeurs. Cependant, différents sous-domaines et différents hôtes peuvent avoir des niveaux de sécurité différents.

Dans les tables, les valeurs par défaut dérivées des bases MIB sont affichées en gris. Les valeurs qui ont été modifiées au niveau actuel sont affichées en noir.

Chapitre

4

Configuration du réseau géré

Sujets :

- *Ouverture de session*
- *Administration des domaines et des hôtes*
- *Ajout d'hôtes*
- *Installation locale et Policy Manager*
- *Installation sur un hôte infecté*
- *Vérification du fonctionnement des connexions de gestion*

Policy Manager vous offre plusieurs manières de déployer Client Security dans votre entreprise :

- Dans un domaine Windows, vous pouvez utiliser les fonctions **Autodiscover** et **Autoregistration** pour automatiser la création du domaine géré.
- S'il y a beaucoup d'ordinateurs tournant sous Unix ou Linux, ou s'il existe également des serveurs à gérer, il est possible de tous les connecter à Policy Manager, et leurs applications de sécurité peuvent être administrées à partir d'un endroit centralisé.

Il existe également certains aspects à prendre en considération pour, ensuite, exploiter au mieux la gestion centralisée des applications de sécurité. Un de ces aspects est, par exemple, la planification minutieuse de la structure du domaine géré.

Lors de la planification de la structure du domaine géré, envisagez de regrouper dans le même sous-domaine les utilisateurs finaux ayant des besoins de sécurité similaires et de regrouper les ordinateurs portables et de bureaux dans leurs propres sous-domaine. De cette manière, vous définissez les paramètres de sécurité optimaux pour les ordinateurs pouvant être connectés à différents réseaux ou utilisant des connexions commutées, ainsi que pour les ordinateurs qui sont toujours connectés au réseau de l'entreprise.

Ouverture de session

Lorsque vous démarrez Policy Manager Console, la bôite de dialogue **Ouverture de session** s'affiche.

👉 **Astuce:** Vous pouvez cliquer sur **Options** pour agrandir la boîte de dialogue et afficher davantage d'options.

Vous pouvez utiliser la boîte de dialogue **Ouverture de session** pour sélectionner des connexions définies. Chaque connexion s'accompagne de ses propres préférences, ce qui facilite l'administration de plusieurs serveurs avec une seule instance de Policy Manager Console.

Il est également possible de définir plusieurs connexions multiples à un seul serveur. Une fois la connexion sélectionnée, entrez la phrase de cryptage de Policy Manager Console. Il s'agit de la phrase de cryptage définie lors de l'installation du programme, et non de votre mot de passe d'administrateur réseau.

Vous pouvez démarrer le programme en mode Lecture seule, auquel cas vous n'avez pas besoin d'entrer une phrase de cryptage. Le cas échéant, cependant, vous ne pourrez effectuer aucune modification.

L'assistant d'installation crée la connexion initiale, qui figure par défaut dans la zone **Connexions :**. Pour ajouter d'autres connexions, cliquez sur **Ajouter** ou pour modifier une connexion existante, cliquez sur **Modifier**. Ces deux options sont disponibles quand la boîte de dialogue est agrandie.

Notez qu'il est possible de copier des connexions existantes. Vous pouvez ainsi définir aisément plusieurs connexions au même serveur, en employant des paramètres légèrement différents en vue d'utilisations diverses. Par exemple, vous pouvez utiliser une connexion existante comme modèle, puis tester différents paramètres de connexion sur la nouvelle copie, sans influer sur les paramètres d'origine.

Propriétés de connexion

Les propriétés de connexion sont définies lors de l'ajout d'une nouvelle connexion ou de la modification d'une connexion existante.

La liaison au référentiel de données est définie comme l'URL HTTP de Policy Manager Server.

Le champ **Nom** permet de définir le nom que portera la connexion dans le champ **Connexion :** de la boîte de dialogue **Connexion**. Si le champ **Nom** reste vide, l'URL ou le chemin d'accès s'affiche.

Les chemins **Fichier de clé publique** et **Fichier de clé privée** indiquent quel jeu de clés d'administration doit être utilisé pour la connexion en question. Si les fichiers de clé spécifiés n'existent pas, Policy Manager Console génère un nouveau jeu de clés.

Modification des préférences de communication

Dans les préférences de communication, vous pouvez définir la fréquence d'interrogation du serveur pour obtenir des informations sur son état, ainsi qu'une limite après laquelle les hôtes sont considérés comme déconnectés.

La boîte de dialogue **Propriétés de connexion** s'ouvre (par exemple en cliquant sur **Options** sur la boîte de dialogue **Ouverture de session**).

Pour modifier les préférences de communication :

1. Sélectionnez l'onglet **Communication**.
2. Modifiez l'**Etat de connexion de l'hôte** si nécessaire.

   Etat de connexion de l'hôte contrôle quand les hôtes sont considérés comme déconnectés de Policy Manager. Tous les hôtes qui n'ont pas contacté Policy Manager Server dans l'intervalle défini sont considérés comme déconnectés. Les hôtes déconnectés sont signalés par une icône de notification dans l'arborescence, et ils sont placés dans la liste **Hôtes déconnectés** de la vue de l'état du **domaine**.

> 👉 **Remarque:** Il est possible de définir un intervalle de moins d'un jour en entrant un nombre à décimales dans le champ de saisie. Par exemple, si vous entrez une valeur de `0,5`, tous les hôtes qui n'ont pas contacté le serveur dans les 12 heures sont considérés comme déconnectés. Les valeurs inférieures à un jour ne servent normalement qu'à des fins de dépannage. Dans un environnement traditionnel, certains hôtes sont naturellement déconnectés du serveur de temps à autre. Par exemple, il se peut qu'un ordinateur portable soit incapable d'accéder quotidiennement au serveur, mais dans la plupart des cas, ce comportement est tout à fait acceptable.

3. Cliquez sur **Options d'intervalles d'interrogation** pour modifier les intervalles d'interrogation. La boîte de dialogue **Intervalles d'interrogation** s'affiche.
4. Modifiez les intervalles d'interrogation de sorte qu'ils correspondent à votre environnement.

   Le choix du protocole de communication affecte les intervalles d'interrogation par défaut. Si vous ne souhaitez pas recevoir certaines informations d'administration, désactivez complètement les récupérations inutiles. Pour ce faire, décochez l'élément de récupération que vous souhaitez désactiver. Cependant, l'interrogation automatique ne doit être désactivée qu'en cas de problèmes de performances. L'option **Désactiver toutes les interrogations** permet de désactiver l'ensemble des éléments d'interrogation. Que l'interrogation automatique soit désactivée ou non, les opérations d'actualisation manuelle peuvent servir à actualiser les informations sélectionnées.

Après le démarrage de Policy Manager Console, ces paramètres peuvent être modifiés normalement depuis la vue **Préférences**.

Administration des domaines et des hôtes

Si vous souhaitez utiliser des stratégies de sécurité différentes pour différents types d'hôtes (portables, ordinateurs de bureau, serveurs), pour différents services de l'entreprise ou pour des utilisateurs ayant des connaissances différentes en informatique, il est judicieux de planifier la structure du domaine en fonction de ces critères.

Cela facilitera la gestion des hôtes. Si vous avez conçu au préalable la structure du domaine de stratégie, vous pouvez importer les hôtes directement dans cette structure. Si vous souhaitez démarrer rapidement, vous pouvez également commencer par importer tous les hôtes dans le domaine racine et créer la structure du domaine plus tard, lorsque le besoin s'en fait sentir. Les hôtes peuvent alors êtres coupés et collés dans leur nouveau domaine.

Chaque domaine ou hôte de cette structure doit disposer d’un nom unique.

Il est également possible de créer les différents bureaux nationaux en tant que sous-domaines.

Ajout de domaines de stratégie

Cette rubrique décrit comment ajouter des nouveaux domaines de stratégie.

Pour ajouter un nouveau domaine de stratégie :

1. Sélectionnez **Edition** ➤ **Nouveau domaine de stratégie** dans le menu.
   Alternativement :
   - Cliquez sur  dans la barre d'outils.
   - Appuyez sur Ctrl + Insert.

   Le nouveau domaine de stratégie est un sous
2. Entrez un nom pour le domaine de stratégie.
   Une icône représentant le domaine est créée.

Ajout d'hôtes

Cette section décrit les différentes méthodes d'ajout d'hôtes à un domaine de stratégie.

Les principales méthodes d'ajout d'hôtes dans votre domaine de stratégie, selon le système d'exploitation utilisé, sont les suivantes :

- Importer des hôtes directement à partir de votre domaine Windows.
- Importer des hôtes par auto-enregistrement (nécessite que Management Agent soit installé sur les hôtes importés). Vous pouvez également utiliser d'autres critères pour importer les hôtes auto-enregistrés dans différents sous-domaines.
- Créez des hôtes manuellement à l'aide de la commande **Nouvel hôte**.

Ajout d'hôtes à des domaines Windows

Dans un domaine Windows, la méthode la plus pratique pour ajouter des hôtes dans votre domaine de stratégie consiste à importer ceux-ci à l'aide du composant d'installation intelligente.

Notez que cela installe également Management Agent sur les hôtes importés. Pour importer des hôtes depuis un domaine Windows :

1. Sélectionnez le domaine cible.
2. Sélectionnez **Edition** ➤ **Autodécouvrir hôtes Windows** dans le menu.
   Au terme de l'opération de découverte automatique, le nouvel hôte est automatiquement ajouté à l'arborescence du **Domaine de stratégie**.

Importation d'hôtes auto-enregistrés

Il est également possible d'importer les hôtes dans Policy Manager Console en utilisant la fonction d'*auto-enregistrement*.

Cette opération n'est réalisable qu'une fois Management Agent installé sur les hôtes et après l'envoi d'une demande d'auto-enregistrement par les hôtes. Management Agent devra être installé à partir d'un CD-ROM, d'un script de connexion ou d'une autre manière.

Pour importer des hôtes auto-enregistrés :

1. Cliquez sur  dans la barre d'outils.
   Autre possibilité :
   - Sélectionnez **Edition** ➤ **Importer des hôtes auto-enregistrés** dans le menu.
   - Sélectionnez **Importer des hôtes auto-enregistrés** dans la vue **Installation**.

   Une fois l'opération terminée, l'hôte est ajouté à l'arborescence du domaine. Les hôtes auto-enregistrés peuvent être importés dans différents domaines en fonction de différents critères, tels que l'IP ou l'adresse DNS de l'hôte. La vue **Auto-enregistrement** présente les données envoyées par l'hôte dans le message d'auto-enregistrement sous forme de tableau. Ces données comprennent les propriétés d'auto-enregistrement personnalisées éventuellement incluses dans le package d'installation distante lors de l'installation.
2. Vous pouvez effectuer les opérations suivantes dans la vue **Auto-enregistrement** :
   - Vous pouvez trier les messages d'auto-enregistrement selon les valeurs de n'importe quelle colonne. Pour ce faire, cliquez sur son en-tête dans le tableau.
   - Vous pouvez modifier l'ordre des colonnes en les faisant glisser à l'emplacement souhaité. La largeur des colonnes peut également être modifiée.

- Vous pouvez utiliser le menu contextuel de la table (cliquez avec le bouton droit de la souris sur la barre d'en-tête de la table) pour spécifier les propriétés d'auto-enregistrement à afficher dans la table.

Utilisation des règles d'importation de l'auto-enregistrement

Vous pouvez définir les règles d'importation des hôtes auto-enregistrés dans l'onglet **Règles d'importation** de la boîte de dialogue **Importer les hôtes auto-enregistrés**.

Les critères d'importation suivants peuvent être utilisés dans les règles :

- Nom WINS, nom DNS, nom DNS dynamique, propriétés personnalisées
  - L'astérisque (`*`) peut être utilisé comme caractère générique. Le caractère `*` peut remplacer n'importe quel nombre de caractères. Par exemple : `test_hôte*` ou `*.exemple.com`.
  - La correspondance n'est pas sensible à la casse : les caractères en majuscule et en minuscule sont donc traités de la même façon.
- Adresse IP, adresse IP dynamique
  - Ces critères prennent en charge la correspondance exacte d'adresse IP (par exemple : `192.1.2.3`) et la correspondance de sous-domaines IP (par exemple : `10.15.0.0/16`).

1. Vous pouvez masquer et afficher des colonnes de la table à l'aide du menu contextuel qui apparaît lorsque vous cliquez avec le bouton droit de la souris sur n'importe quel en-tête de colonne de la fenêtre **Importer des règles**.

   Seules les valeurs contenues dans les colonnes actuellement visibles sont utilisées comme critères de correspondance lors de l'importation des hôtes dans le domaine de stratégie. Les valeurs contenues dans les colonnes masquées sont ignorées.

2. Il est également possible d'ajouter de nouvelles propriétés personnalisées à utiliser comme critères lors de l'importation des hôtes.

   Les propriétés personnalisées peuvent également être utilisées pour créer des packages d'installation indépendants pour différents services devant être regroupés dans des domaines de stratégie spécifiques. Dans ce cas, il est possible d'utiliser le nom du service comme propriété personnalisée, puis de créer des règles d'importation qui utilisent le nom des services comme critère d'importation. Notez que les noms de propriété personnalisée masqués ne sont conservés en mémoire que jusqu'à la fermeture de Policy Manager Console. Pour ajouter une nouvelle propriété personnalisée :

   a) Cliquez avec le bouton droit sur un en-tête de colonne et sélectionnez **Ajouter une propriété personnalisée**.
   La boîte de dialogue **Nouvelle propriété personnalisé** s'ouvre.
   b) Saisissez le nom de la propriété personnalisée (par exemple, le nom du service), puis cliquez sur **OK**.
   La nouvelle propriété personnalisée apparaît dans le tableau. Elle peut désormais être utilisée comme critère d'importation dans de nouvelles règles d'importation d'auto-enregistrement.

3. Créer une nouvelle règle d'importation d'auto-enregistrement :

   a) Cliquez sur **Ajouter** dans l'onglet **Règles d'importation**.
   La boîte de dialogue **Sélectionner le domaine de stratégie de destination pour la règle** s'ouvre et affiche les domaines et sous-domaines existants.
   b) Sélectionnez le domaine pour lequel vous créez la règle et cliquez sur **OK**.
   c) Sélectionnez la ligne que vous venez de créer, cliquez dans la cellule à renseigner, puis cliquez sur **Modifier**.
   d) Saisissez la valeur dans la cellule.
   Le critère d'importation est défini.

   - Lors de l'importation d'hôtes auto-enregistrés, les règles sont vérifiées de haut en bas. La première règle correspondante est appliquée. Il est possible de changer l'ordre des règles en cliquant sur **Déplacer vers le bas** ou **Déplacer vers le haut**.

- Si vous souhaitez créer plusieurs règles pour un domaine, vous pouvez utiliser l'option **Cloner**. Commencez par créer une règle pour le domaine. Sélectionnez ensuite la ligne et cliquez sur **Cloner**. Vous pouvez désormais modifier les critères dans la ligne dupliquée.

4. Lorsque vous voulez débuter l'importation, sélectionnez l'onglet **Hôtes auto-enregistrés** et cliquez sur **Importer**.

   Les règles d'importation définies seront validées avant le début de l'importation.

   Une fois les hôtes importés, une boîte de dialogue récapitulative s'ouvre et affiche le nombre d'hôtes importés avec succès et le nombre d'importations échouées. Notez qu'un ensemble de conditions vide est traité comme une correspondance absolue.

Création manuelle d'hôtes

Cette rubrique décrit comment créer des hôtes manuellement.

Pour créer un hôte manuellement :

1. Sélectionnez le domaine cible.
2. Sélectionnez **Edition** ➤ **Nouvel hôte** dans le menu.

   Autre possibilité :

   - Cliquez sur  dans la barre d'outils.
   - Appuyez sur Insérer.

   Cette opération est utile dans les cas suivants :

   - Apprentissage et test : vous pouvez essayer un sous-ensemble des fonctions de Policy Manager Console sans installer de logiciel en complément de Policy Manager Console.
   - Définition des stratégies en avance : vous pouvez définir et générer une stratégie pour un hôte avant d'installer le logiciel sur l'hôte.
   - Cas particuliers : vous pouvez générer des stratégies pour des hôtes qui n'accèderont jamais directement au serveur (c'est-à-dire lorsqu'il est impossible d'importer l'hôte). Il est, par exemple, possible de générer des fichiers de stratégie de base pour un ordinateur n'ayant pas accès à F-Secure Policy Manager Server. Vous devez transférer le fichier de stratégie de base soit manuellement, soit en utilisant un autre mode de transport externe. Pour ce faire, choisissez la commande **Edition** ➤ **Exporter le fichier de stratégie** dans le menu.

   Remarque: Les hôtes non équipés de Management Agent ne peuvent pas être administrés par Policy Manager Console, car ils n'ont aucun moyen de rechercher les stratégies. De plus, ils ne disposent d'aucune information d'état. Toutes les modifications apportées à la structure du domaine sont appliquées, même si vous fermez Policy Manager Console sans les enregistrer dans les données de stratégies en cours.

Installations distantes

Cette section décrit comment effectuer une installation distante sur les hôtes.

La seule différence entre les fonctions **Autodécouvrir hôtes Windows** et **Distribuer l'installation aux hôtes Windows** réside dans la manière dont les hôtes de destination sont sélectionnés. La fonction de découverte automatique examine les domaines Windows, et l'utilisateur peut sélectionner les hôtes de destination dans une liste. La fonction de distribution de l'installation permet pour sa part de définir directement les hôtes de destination à l'aide d'adresses IP ou de noms d'hôte. Une fois les hôtes de destination sélectionnés, les deux opérations d'installation distante se déroulent de la même manière.

Remarque: Avant de commencer l'installation de produits F-Secure sur les hôtes, vous devez vous assurer qu'aucun programme antivirus ou de pare-feu n'entre en conflit avec les programmes installés.

Autodécouvrir hôtes Windows

Les hôtes cibles peuvent être sélectionnés avec la fonction *Autodécouvrir*.

Pour sélectionner des hôtes cibles :

1. Sélectionnez le domaine cible.
2. Sélectionnez **Edition** ➤ **Autodécouvrir hôtes Windows** dans le menu.

   Vous pouvez également cliquer sur le bouton  .
3. Dans la liste des **Domaines NT**, sélectionnez l'un des domaines et cliquez sur **Actualiser**.

   La liste des hôtes est actualisée lorsque vous cliquez sur le bouton **Actualiser**. Afin d'optimiser les performances, seules les informations stockées en mémoire cache apparaissent à l'écran. Avant de cliquer sur **Actualiser**, vous pouvez modifier les options suivantes :

   - **Masquer les hôtes déjà administrés**. Cochez cette case afin d'afficher uniquement les hôtes ne disposant pas d'applications F-Secure.
   - **Identifier les hôtes en détail (plus lent)**. Cette option affiche tous les détails relatifs aux hôtes, comme les versions du système d'exploitation et de Management Agent.
   - **Identifier les noms d'hôtes et les commentaires uniquement (plus rapide)**. Cette option peut être utilisée lorsque tous les hôtes n'apparaissent pas de façon détaillée ou que la récupération de la liste prend trop de temps. Notez qu'il peut parfois s'écouler un petit moment avant que le **Navigateur principal** affiche un hôte récemment installé sur le réseau.
4. Sélectionnez les hôtes sur lesquels effectuer l'installation.

   Appuyez sur la barre d'espace pour vérifier les hôtes sélectionnés. Plusieurs hôtes peuvent être facilement sélectionnés en maintenant appuyée la touche Maj. et en effectuant l'une des tâches suivantes :

   - cliquer sur plusieurs lignes d'hôtes ;
   - faire glisser la souris au-dessus de plusieurs lignes d'hôtes ;
   - utiliser les touches portant une flèche vers le haut ou vers le bas.

   Vous pouvez également cliquer à l'aide du bouton droit de la souris. Dans le menu contextuel de la liste des hôtes, utilisez l'une des commandes suivantes :

   - **Activer** : active la case à cocher de l'hôte sélectionné (équivaut à appuyer sur la barre d'espacement).
   - **Désactiver** : désactive la case à cocher de l'hôte sélectionné (équivaut à appuyer sur la barre d'espacement).
   - **Tout activer** : active les cases à cocher de tous les hôtes du domaine Windows sélectionné.
   - **Désactiver tout** : désactive les cases à cocher de tous les hôtes du domaine Windows sélectionné.
5. Cliquez sur **Installer** pour continuer.

Lorsque vous avez sélectionné les hôtes cibles, vous devez tout de même installer à distance les applications sur les hôtes.

Distribuer l'installation aux hôtes Windows

Vous pouvez également sélectionner les hôtes cibles à l'aide de la fonction **Distribuer l'installation aux hôtes Windows**.

Pour sélectionner des hôtes cibles :

1. Sélectionnez le domaine cible.
2. Sélectionnez **Edition** ➤ **Distribuer l'installation aux hôtes Windows** dans le menu.

   Vous pouvez également cliquer sur le bouton  .

3. Entrez le nom des hôtes de destination sur lesquels démarrer l'installation, puis cliquez sur **Suivant** pour continuer.

   Vous pouvez cliquer sur **Parcourir** pour vérifier les versions de Management Agent sur les hôtes.

Lorsque vous avez sélectionné les hôtes cibles, vous devez installer à distance les applications sur les hôtes.

Installation distante après la sélection de l'hôte cible

Lorsque vous avez sélectionné les hôtes cibles, vous devez exécuter à distance les packages d'installation.

Pour exécuter à distance des packages d'installation sur les hôtes cibles sélectionnés :

1. Sélectionnez le package d'installation de votre choix, puis cliquez sur **Suivant** pour continuer.
2. Sélectionnez les produits à installer et cliquez sur **Suivant** pour continuer.

   Vous pouvez forcer la réinstallation s'il existe déjà des applications portant le même numéro de version.
3. Acceptez la stratégie par défaut ou choisissez la stratégie d'hôte ou de domaine à employer comme stratégie anonyme, puis cliquez sur **Suivant**.
4. Choisissez le compte d'utilisateur et le mot de passe pour l'installation à distance en sélectionnant soit **Ce compte** (le compte actuel) ou **Un autre utilisateur**.

   Remarque: Durant l'installation, la fonction d'installation distante doit disposer des droits d'accès administrateur sur le poste de destination. Si le compte que vous avez sélectionné ne dispose pas de droits d'accès administrateur sur l'un des hôtes distants, le message d'erreur **Accès refusé** apparaît pour l'hôte concerné, tandis que l'installation se poursuit pour les autres hôtes.

   Lorsque vous sélectionnez **Ce compte**, vous disposez des droits de sécurité du compte auquel vous êtes connecté. Utilisez cette option dans les cas suivants :

   - Vous êtes déjà connecté en tant qu'administrateur de domaine.
   - Vous êtes connecté en tant qu'administrateur local avec un mot de passe qui correspond à celui de l'administrateur local sur l'hôte de destination.

   Un autre utilisateur : entrez le compte et le mot de passe. L'administrateur peut saisir n'importe quels compte et mot de passe corrects d'administrateur de domaine afin d'effectuer l'installation distante sur les hôtes sélectionnés.

   - En cas d'installation sur des domaines approuvés et non approuvés à l'aide d'un compte de domaine, veillez à entrer le compte avec le format`DOMAINE\\COMPTE`.
   - Lorsque vous utilisez un compte d'administrateur local, utilisez le format `COMPTE`. N'ajoutez pas le nom d'hôte à celui du compte, faute de quoi ce compte ne sera accepté que par l'hôte en question.

   Remarque: Lors de l'installation, si l'ordinateur de l'administrateur a ouvert des connexions réseau avec l'ordinateur de destination à l'aide d'un autre compte d'utilisateur, le message d'erreur NT **1219** (conflit d'identification) s'affiche. Dans ce cas, interrompez les connexions actives avant de lancer l'**installation distante**.
5. Prenez connaissance du résumé de l'installation.
6. Pour démarrer l'**Assistant d'installation distante**, cliquez sur **Démarrer**.

   L'**Assistant d'installation distante** affiche une série de boîtes de dialogue dans lesquelles vous devez répondre à des questions pour permettre la réalisation de l'installation. Dans la dernière boîte de dialogue, cliquez sur **Terminer** puis passez à l'étape suivante.

   Policy Manager installe Management Agent et les produits sélectionnés sur les hôtes. Durant cette opération, la ligne d'**état** affiche l'avancement de la procédure. Vous pouvez cliquer à tout moment sur **Annuler** pour interrompre l'installation.
7. Quand la ligne d'**état** affiche terminé, le processus est terminé et vous pouvez sélectionner le domaine dans lequel inclure les nouveaux hôtes à l'aide des paramètres d'importation.
8. Cliquez sur **Terminer**.

Policy Manager Console place les nouveaux hôtes dans le domaine sélectionné, sauf si vous avez entré un domaine différent dans cette boîte de dialogue. Vous pouvez également décider de ne pas placer automatiquement les hôtes dans un domaine. Les nouveaux hôtes enverront des demandes d'enregistrement automatique qui permettront de les importer.

Après quelques minutes, la liste des produits installés s'affiche.

9. Afin de visualiser cette liste, sélectionnez l'onglet **Installation**. Vous pouvez également sélectionner le domaine principal sur l'arborescence du **Domaine de stratégie**).

Installation par stratégies

Des fichiers de stratégie de base sont utilisés pour démarrer des installations sur les hôtes où Management Agent est installé.

Policy Manager Console crée un package d'installation spécifique d'une opération, qu'il stocke sur Policy Manager Server, puis écrit une tâche d'installation dans les fichiers de stratégie de base (une distribution de stratégie est donc nécessaire pour démarrer les installations). Les fichiers de stratégie de base et le package d'installation sont signés par la paire de clés d'administration, si bien que les hôtes n'accepteront que des informations authentiques.

Management Agent charge les nouvelles stratégies à partir de Policy Manager Server et recherche la tâche d'installation. Management Agent récupère, à partir du serveur, le package d'installation indiqué dans les paramètres de la tâche, puis démarre le programme d'installation.

Au terme de l'installation, Management Agent envoie le résultat de l'opération au serveur, dans un fichier de stratégie incrémentiel. Policy Manager Console recherche les nouvelles informations d'état et présente le résultat.

La désinstallation s'effectue à l'aide des mêmes mécanismes de remise. Les résultats de la désinstallation ne seront pas signalés.

Utilisation de l'éditeur d'installation

L'éditeur d'installation doit être utilisé sur les hôtes équipés de Management Agent.

Pour utiliser l'éditeur d'installation :

1. Ouvrez l'onglet **Stratégie** et sélectionnez le nœud racine (l'arborescence secondaire **F-Secure**).

   Vous pouvez également ouvrir l'onglet **Installer**.

   L'**Editeur d'installation** s'affiche.
2. Dans l'**Editeur d'installation**, sélectionnez les produits à installer sur l'hôte ou le domaine de stratégie actuellement sélectionné.

   L'**Editeur d'installation** contient les informations suivantes relatives aux produits installés sur l'hôte ou un domaine de stratégie de destination :

Nom de produit	Nom du produit déjà installé sur un hôte ou un domaine ou qui peut être installé à l'aide d'un package d'installation disponible.
Version installée	Numéro de version du produit. Si plusieurs versions du produit sont installées, tous les numéros de version correspondants s'affichent. Pour les hôtes, il s'agit toujours d'un numéro de version unique.
Version à installer	Numéros de version des packages d'installation disponibles pour le produit.
Version actuelle	Version actuelle, en cours d'installation sur un hôte ou un domaine.

En cours	Progression de l'installation. Le champ **En cours** affiche des informations différentes pour les hôtes et pour les domaines.

- Lorsqu'un hôte est sélectionné, le champ **En cours** affiche l'un des messages suivants :

En cours	L'installation a démarré (et a été ajoutée aux données de stratégie), mais l'hôte n'a pas encore signalé le succès ou l'échec de l'opération.
Échec	L'installation ou la désinstallation a échoué. Cliquez sur le bouton du champ **En cours** pour afficher des informations d'état détaillées.
Terminé	L'installation ou la désinstallation est achevée. Ce message disparaît lorsque vous fermez l'**Editeur d'installation**.
(Zone vide)	Aucune opération n'est en cours. Le champ **Version installée** affiche le numéro de version des produits actuellement installés.

- Lorsqu'un domaine est sélectionné, la zone **En cours** contient l'une des informations suivantes :

<nombre> hôtes restants - **<nombre> installations ayant échoué**	Nombre d'hôtes restants et nombre d'installations qui ont échoué. Cliquez sur le bouton de la zone **En cours** pour afficher des informations d'état détaillées.
Terminé	L'installation ou la désinstallation est achevée sur tous les hôtes.
(Zone vide)	Aucune opération n'est en cours. La **version installée** affiche le numéro de version des produits actuellement installés.

3. Lorsque tous les numéros de version requis sont sélectionnés, cliquez sur **Démarrer**. L'**Editeur d'installation** lance l'**Assistant d'installation**, qui invite l'utilisateur à configurer les paramètres de l'installation. L'**Editeur d'installation** prépare ensuite un package personnalisé de distribution de l'installation pour chaque opération d'installation. Ce package est sauvegardé sur Policy Manager Server.

   
   Remarque: Le bouton **Démarrer** permet à l'administrateur de démarrer les opérations d'installation sélectionnées dans la zone **Version à installer**. Si vous fermez l'**Editeur d'installation** sans cliquer sur le bouton **Démarrer**, toutes les modifications sont annulées.

4. L'installation étant déclenchée par une stratégie, vous devez distribuer les nouveaux fichiers de stratégie.

   Le fichier de stratégie contient une entrée qui invite l'hôte à rechercher le package d'installation et à démarrer l'installation.

   Notez qu'une installation peut prendre énormément de temps, notamment lorsqu'un hôte concerné n'est pas connecté au réseau lors de l'installation ou si l'opération activée requiert que l'utilisateur redémarre son poste de travail avant que l'installation soit terminée. Si les hôtes sont connectés au réseau et qu'ils n'envoient ou ne reçoivent pas correctement les fichiers de stratégie, cela signifie qu'il peut y avoir un problème important. Il est possible que l'hôte ne confirme pas correctement la réception de l'installation. Dans tous les cas, vous pouvez supprimer l'opération d'installation de la stratégie en cliquant sur le bouton **Tout arrêter**. Toutes les opérations d'installation définies pour le domaine de stratégie ou l'hôte sélectionné seront alors annulées. Vous pouvez arrêter toutes les tâches d'installation dans le domaine sélectionné et tous ses sous-domaines en choisissant l'option **Annuler de façon récurrente les installations pour les sous-domaines et les hôte** dans la boîte de dialogue de confirmation.

Le bouton **Tout arrêter** est activé uniquement si une opération d'installation est définie pour l'hôte ou le domaine actuel. Les opérations définies pour les sous-domaines ne modifient pas son état. **Tout arrêter** supprime uniquement l'opération de la stratégie. Si un hôte a déjà récupéré le fichier de stratégie précédent, il est possible qu'il tente d'exécuter l'installation même si elle n'est plus visible dans l'**Editeur d'installation**.

Désinstallation à distance :

La désinstallation d'un produit peut s'exécuter aussi facilement qu'une mise à jour. Le système crée un fichier de diffusion contenant uniquement le logiciel nécessaire à la désinstallation du produit. Si ce dernier ne prend pas en charge la désinstallation à distance, l'**Editeur d'installation** n'affiche aucune option de désinstallation.

Si vous sélectionnez **Réinstaller**, la version actuelle sera à nouveau installée. Utilisez cette option uniquement pour résoudre certains problèmes. En règle générale, il n'est pas nécessaire de réinstaller un produit.

Lors de la désinstallation de Management Agent, aucune information statistique indiquant que la désinstallation a réussi n'est envoyée car Management Agent a été supprimé et ne peut pas envoyer d'informations. Si vous désinstallez par exemple F-Secure Anti-Virus et Management Agent :

1. Désinstaller F-Secure Anti-Virus
2. Attendez que Policy Manager Console signale le succès ou l'échec de la désinstallation.
3. Si F-Secure Anti-Virus a été désinstallé correctement, désinstallez Management Agent.
4. Si la désinstallation de Management Agent a échoué, Policy Manager Console affiche un rapport statistique de l'échec. La réussite ne peut pas être signalée, mais elle se remarque à la coupure des communications, le rapport final de Management Agent contenant la mention « `en cours` ».

Installations et mises à jour locales à l'aide de packages préconfigurés

Vous pouvez exporter des packages pré-configurés dans un format JAR ou MSI (programme d'installation Microsoft).

Les packages MSI peuvent être distribués, par exemple, en utilisant la stratégie de groupe Windows dans l'environnement Active Directory.

La procédure d'exportation dans les deux formats est la même (voir ci-dessous). Vous pouvez sélectionner le format de fichier pour le package personnalisé dans la boîte de dialogue **Exporter le package d'installation**.

Utilisation du package d'installation à distance personnalisé

L'utilisation du script de connexion peut se faire de deux façons sur les plates-formes Windows : à l'aide d'un fichier d'installation distante personnalisé ou à l'aide d'un fichier MSI personnalisé.

Pour utiliser le fichier JAR d'installation distante personnalisé :

1. Exécutez Policy Manager Console.
2. Sélectionnez **Outils** ➤ **Packages d'installation**.
   La boîte de dialogue **Packages d'installation** s'ouvre.
3. Sélectionnez le package d'installation contenant les produits que vous souhaitez installer, puis cliquez sur **Exporter**.
4. Indiquez le format, JAR ou MSI, et l'emplacement où vous souhaitez enregistrer le package d'installation, puis cliquez sur **Exporter**.
5. Indiquez l'emplacement où vous souhaitez enregistrer le package d'installation JAR personnalisé, puis cliquez sur **Enregistrer**.
6. Sélectionnez les composants à installer et cliquez sur **Suivant** pour continuer.
7. Acceptez la stratégie par défaut ou choisissez la stratégie d'hôte ou de domaine à employer comme stratégie anonyme, puis cliquez sur **Suivant** pour continuer.
8. Sélectionnez le type d'installation.

   Le choix par défaut, **Installation avec administration centralisée**, est recommandé. Vous pouvez également préparer un package pour un hôte autonome.

Une page récapitulative présente les options choisies pour l'installation.

9. Consultez le récapitulatif, puis cliquez sur **Démarrer** pour continuer l'installation de l'assistant.

   Policy Manager Console affiche les **Assistants d'installation à distance** qui collectent toutes les informations nécessaires à l'installation des produits sélectionnés. Vous pouvez inclure autant de propriétés d'auto-enregistrement personnalisées que vous le voulez dans le fichier d'installation. Les hôtes ajouteront ces propriétés personnalisées au message d'auto-enregistrement qu'ils envoient à Policy Manager après l'installation locale. Les propriétés spécifiques des clients s'affichent avec les propriétés standard d'identification d'hôte de la vue d'**auto-enregistrement**. Le nom de la propriété personnalisée est utilisé comme nom de colonne, et sa valeur comme valeur de cellule.

   Vous pouvez par exemple utiliser des propriétés personnalisées pour créer un fichier d'installation distinct destiné à des unités d'exploitation différentes qui doivent être regroupées dans des domaines de stratégie spécifiques. Le nom de la propriété peut être `Unité`, sa valeur différant pour chaque fichier d'installation. Il est désormais possible de distinguer les hôtes de chaque unité dans la vue d'auto-enregistrement. Vous pouvez importer tous les hôtes d'une unité dans leur domaine de destination à l'aide des fonctions de tri des colonnes et de sélection multiple. Notez que le domaine de destination peut être modifié directement depuis la vue d'**auto-enregistrement**. Après quoi, les hôtes d'une autre unité peuvent être importés dans le domaine de destination approprié.

10. Lorsque vous atteignez la dernière page de l'assistant, cliquez sur **Terminer** pour continuer.
11. Vous pouvez installer le package JAR exporté sur les hôtes en exécutant l'outil `ilaunchr.exe`.

    L'outil `ilaunchr.exe` se trouve dans le répertoire d'installation de Policy Manager Console sous `...\Administrator\Bin`. Pour ce faire :

    a) Copiez `ilaunchr.exe` et le package JAR exporté à un emplacement où le script de connexion peut accéder à ceux-ci.
    b) Entrez la commande :`ilaunchr <nom de package>.jar` où `<nom de package>` est remplacé par le nom réel du package JAR installé.

       Lors de l'installation, l'utilisateur voit une boîte de dialogue affichant l'avancement de l'installation. Si un redémarrage s'impose après l'installation, un message invite l'utilisateur à redémarrer l'ordinateur de la manière définie lors de l'exportation du package d'installation. Si vous souhaitez que l'installation s'exécute en mode silencieux, utilisez la commande suivante :`ilaunchr <nom de package>.jar /Q`. Dans ce cas, l'utilisateur peut être invité à redémarrer l'ordinateur après l'installation, et si une erreur fatale se produit pendant l'installation, un message s'affiche.

       ILAUNCHR comporte les paramètres de ligne de commande suivants :

       `/U` — Aucune assistance. Aucun message ne s'affiche, même lorsqu'une erreur fatale se produit.

       `/F` — Installation forcée. Complète l'installation même si Management Agent est déjà installé.

       Tapez `ILAUNCHR /?` à l'invite de commande afin d'afficher la totalité de l'aide.

       Lorsque vous effectuez une installation sur XP (ou version plus récente), vous pouvez également utiliser les paramètres suivants :

       - `/user:domaine\nom_utilisateur` (variation : `/user:nom_utilisateur`) : spécifie le compte utilisateur et le nom de domaine. Le nom de domaine est facultatif.
       - `/password:secret` (variation : `/password:"secret avec espaces"`) : spécifie le mot de passe du compte utilisateur.

       La fonctionnalité de l'utilitaire ilaunchr reste la même si aucun de ces deux paramètres n'est fourni. Si un seul des paramètres est fourni, ilaunchr renvoie un code d'erreur. Si les deux paramètres sont fournis, llaunchr démarre le programme**d'installation**. Exemple de la commande :

       ```
       ILaunchr <fichier jar> /user:domaine\nom_utilisateur /password:mot_secret
       ```

Installation locale et Policy Manager

L'installation locale est recommandée si vous devez installer Client Security localement, sur une station de travail par ailleurs gérée de manière centralisée par Policy Manager.

Policy Manager doit déjà être installé pour que vous puissiez poursuivre l'installation.

Remarque: Lors de l'installation de Client Security devant être géré par Policy Manager, sélectionnez **Gestion centrale avec F-Secure Policy Manager** pendant l'affichage de l'étape de sélection de la gestion lors de l'installation. Vous devrez également indiquer l'emplacement de la clé publique Policy Manager (`admin.pub`, créée lors de l'installation de Policy Manager Console) et l'adresse réseau du Policy Manager Server en cours d'utilisation. Ces informations sont requises pour garantir des communications sécurisées avec Policy Manager.

Configuration système requise

Avant d'utiliser le produit, veuillez lire les informations ci-après.

Configuration système recommandée pour une utilisation optimale du produit sur votre ordinateur : Configuration système requise

Processeur :	• Sur Windows Vista et Windows 7 : Intel Pentium 4 2 GHz ou supérieur • Sur Windows XP : Intel Pentium III 1 GHz ou supérieur
Système d'exploitation :	• Windows 7 32 bits et 64 bits • Windows Vista 32 bits et 64 bits • Windows XP SP2 ou ultérieur
Mémoire :	• Sur Windows Vista et Windows 7 : 1 Go de RAM ou plus • Sur Windows XP : 512 Mo de RAM ou plus
Espace disque :	800 Mo espace libre sur le disque dur
Affichage :	• Sur Windows Vista et Windows 7 : 16 bits ou plus (65 000 couleurs) • Sur Windows XP : 16 bits, 65 000 couleurs ou plus
Connexion Internet :	Requise pour la validation de votre abonnement et la réception de mises à jour

Désinstallation d'autres programmes antivirus

Avant de commencer l'installation de Client Security, vous devez supprimer tous les autres programmes antivirus installés sur les stations de travail.

Pour désinstaller d'autres programmes antivirus :

1. Sélectionnez les programmes installés dans la boîte de dialogue **Démarrer** ➤ **Paramètres** ➤ **Panneau de configuration** ➤ **Ajout/Suppression de programmes**.
2. Supprimez tous les composants liés.

   Certains programmes peuvent avoir plusieurs composants liés, qui devront probablement être désinstallés séparément. Si vous rencontrez des problèmes, consultez la documentation utilisateur du programme antivirus installé.

3. Redémarrez votre ordinateur.

Procédure d'installation

Vous devez disposer du CD du produit, d'une clé d'abonnement valide et d'une connexion Internet. Si plusieurs utilisateurs partagent et utilisent l'ordinateur, ouvrez une session avec des droits d'administration pour procéder à l'installation du produit.

Installation du logiciel :

1. Insérez le CD d'installation.

   L'installation devrait démarrer automatiquement. Si tel n'est pas le cas, double-cliquez sur l'icône du CD-ROM, puis sur le fichier `setup.exe` pour lancer l'installation.

   La première boîte de dialogue de l'installation s'affiche.
2. Sélectionnez la langue d'installation de votre choix, puis cliquez sur **Suivant** pour continuer.
3. Lisez le contrat de licence. Pour l'accepter et poursuivre, cliquez sur **Accepter**.
4. Saisissez votre clé d'abonnement, puis cliquez sur **Suivant** pour continuer.

   Remarque: Si vous souhaitez utiliser une version d'évaluation du produit, ne renseignez pas le champ **Ma clé d'abonnement est** et cliquez sur **Suivant**. Sélectionnez le service à évaluer dans la boîte de dialogue **Options d'évaluation**.

   - Si vous avez acheté le produit dans un magasin sur support CD, vous trouverez la clé d'abonnement sur la page de couverture du guide d'installation rapide.
   - Si vous avez téléchargé le produit depuis l'eStore de F-Secure, la clé d'abonnement vous a été fournie dans le message de confirmation du bon de commande.

   Remarque: Utilisez uniquement la clé d'abonnement fournie avec le produit. Vous pouvez utiliser la clé d'abonnement pour le nombre de copies prévu par votre licence (reportez-vous à l'avis "Licence F-Secure" du présent guide). Si vous rencontrez des difficultés lors de votre enregistrement, veuillez contacter l'assistance technique de F-Secure.
5. Sélectionnez le type d'installation :

   - Installation automatique : l'installation du produit s'effectue automatiquement. Les produits de sécurité existants peuvent être automatiquement remplacés. Le produit est installé dans le répertorie par défaut.
   - Installation étape par étape : vous pouvez sélectionner vos propres options pendant l'installation. Vous pouvez par exemple modifier le répertoire d'installation. Nous vous recommandons toutefois d'utiliser le répertoire par défaut.
6. Cliquez sur **Suivant**.
7. Retirez le CD d'installation lorsque l'installation est terminée.
8. L'ordinateur redémarre automatiquement. Pour redémarrer immédiatement, sélectionnez **Redémarrer maintenant**.
9. Après le redémarrage, le produit tente de se connecter à Internet afin de valider votre abonnement et télécharger les mises à jour disponibles. Vérifiez que vous êtes bien connecté à Internet. Le téléchargement de ces mises à jour importantes peut prendre quelques minutes. Après ce téléchargement, votre protection est actualisée. Grâce au téléchargement des dernières mises à jour, vous bénéficiez d'une protection optimisée.

   Astuce: Pour plus d'informations concernant le produit, vous pouvez cliquer sur le bouton **Aide** du produit et accéder ainsi aux ressources d'aide en ligne. L'aide en ligne est également disponible sur le CD d'installation.

Installation sur un hôte infecté

Si l'hôte sur lequel vous allez installer Client Security est infecté par une variante du virus Klez, exécutez l'outil d'élimination de Klez sur l'hôte avant de démarrer l'installation.

L'outil d'installation `Ilaunchr.exe` ne peut pas fonctionner sur un ordinateur infecté par Klez.

Vous pouvez télécharger l'outil Klezt à l'adresse ftp://ftp.europe.f-secure.com/anti-virus/tools/kleztool.zip.

Le package `kleztool.zip` contient un fichier `kleztool.txt` dans lequel vous trouverez les instructions relatives à l'exécution de Kleztool sur l'ordinateur infecté. Lisez attentivement ces instructions avant de continuer.

Vérification du fonctionnement des connexions de gestion

Vous pouvez vérifier le bon fonctionnement des connexions de gestion en suivant les étapes indiquées ci-dessous.

1. Vérifiez l'**Etat de distribution des stratégies** dans l'onglet **Résumé**.
2. Enregistrez et distribuez les stratégies si nécessaire.
3. Accédez à l'onglet **Etat** et sélectionnez la page **Gestion centralisée**.
4. Vérifiez la date, l'heure et le compteur du fichier de stratégies utilisé actuellement.

Chapitre

5

Configuration de la protection contre les virus et les logiciels espions

Sujets :

- *Configuration des mises à jour automatiques*
- *Configuration de l'analyse en temps réel*
- *Configuration de DeepGuard*
- *Configuration de la recherche de rootkits (Blacklight)*
- *Configuration de l'analyse du courrier électronique*
- *Configuration de l'analyse du trafic Web (HTTP)*
- *Configuration de la recherche de logiciels espions*
- *Gestion des objets en quarantaine*
- *Interdiction de modification des paramètres par les utilisateurs*
- *Configuration de l'envoi d'alertes*
- *Surveillance des virus sur le réseau*
- *Test de la protection antivirus*

La protection contre les virus et les logiciels espions protège les ordinateurs contre les virus incorporés dans des fichiers, les logiciels espions, les riskwares, les rootkits et les virus diffusés par des pièces jointes de courrier électronique et dans du trafic Web.

Les mises à jour automatiques garantissent une protection contre les virus et les logiciels espions toujours actualisée. Une fois que vous avez installé la protection antivirus et contre les logiciels espions, ainsi que les mises à jour automatiques en diffusant les paramètres appropriés dans le cadre d'une stratégie de sécurité, vous pouvez être sûr que le réseau géré est protégé. Vous pouvez également surveiller les résultats d'analyse et d'autres informations que les hôtes gérés renvoient à Policy Manager Console.

Lorsqu'un virus est détecté sur un ordinateur, une des actions suivantes est effectuée :

- Le fichier infecté est nettoyé.
- Le fichier infecté est renommé.
- Le fichier infecté est supprimé.
- Le fichier infecté est mis en quarantaine.
- L'utilisateur est invité à décider de ce qu'il faut faire du fichier infecté.
- La pièce jointe ou le fichier infecté (dans une analyse du courrier électronique) sont uniquement signalé, ou
- La pièce jointe infectée (dans une analyse du courrier électronique) est nettoyée, supprimée ou bloquée.

Configuration des mises à jour automatiques

Cette section explique les différents paramètres de configuration disponibles pour les mises à jour automatiques dans Policy Manager et fournit quelques exemples de configuration pratiques pour des hôtes présentant des besoins de protection différents.

Ces instructions vous permettront de maintenir à jour les définitions de virus sur les hôtes et de choisir la meilleure source pour les mises à jour en fonction des besoins des utilisateurs.

Comment fonctionnent les mises à jour automatiques ?

Automatic Update Agent installé avec Client Security télécharge les mises à jour automatiques à partir des sources de mise à jour configurée.

Automatic Update Agent tente de télécharger les mises à jour automatiques dans l'ordre suivant :

1. Si Policy Manager Proxy est utilisé dans le réseau de l'entreprise, le client tente de se connecter à Policy Manager Server par l'intermédiaire de chaque Policy Manager Proxy à tour de rôle.
2. Si le client est configuré pour utiliser le proxy HTTP, il tente de télécharger les mises à jour par le biais du proxy HTTP à partir de Policy Manager Server.
3. Ensuite, le client tente de télécharger les mises à jour directement depuis Policy Manager Server.
4. Si Policy Manager Proxy est utilisé dans le réseau de l'entreprise, le client tente de se connecter au serveur de mises à jour F-Secure par l'intermédiaire de chaque Policy Manager Proxy à tour de rôle.
5. Si le client est configuré pour utiliser le proxy HTTP, il tente de télécharger les mises à jour par le biais du proxy HTTP à partir du serveur de mise à jour F-Secure.
6. Le client tente ensuite de télécharger les mises à jour directement depuis le serveur de mise à jour de F-Secure.

👉 **Remarque:** Si Client Security est configuré pour télécharger des mises à jour Neighborcast, il pourra également télécharger des mises à jour depuis d'autres installations de Client Security pour lesquelles l'option Neighborcast a été activée.

Paramètres de la mise à jour automatique

Dans la page **Mises à jour automatiques** de l'onglet **Paramètres**, vous pouvez spécifier si vous souhaitez que Client Security reçoive automatiquement des mises à jour de définitions de virus et de logiciels espions.

Pour autoriser les mises à jour automatiques, cochez la case **Activer les mises à jour automatiques**. Vous devriez toujours activer les mises à jour automatiques.

Spécifiez l'intervalle d'interrogation des mises à jour dans le champ **Intervalle d'interrogation des mises à jour à partir de F-Secure Policy Manager Server**.

La liste **Proxies Policy Manager** est une liste de serveurs Policy Manager Proxy disponibles. Automatic Update Agent installé avec Client Security se connecte à ceux-ci dans l'ordre de priorité spécifié dans cette table.

Si vous souhaitez utiliser HTTP Proxy, sélectionnez **A partir des paramètres du navigateur** ou **Défini par l'utilisateur** dans le menu déroulant **Utiliser le proxy HTTP**. Spécifiez ensuite l'**Adresse du proxy HTTP**.

Configuration des mises à jour automatiques à partir de Policy Manager Server

Lorsque l'administration est centralisée, tous les hôtes peuvent aller chercher leurs mises à jour de définitions de virus et de logiciels espions sur Policy Manager Server.

La configuration s'effectue comme suit :

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Mises à jour automatiques**.
3. Assurez-vous que l'option **Activer les mises à jour automatiques** est sélectionnée.
4. Assurez-vous que l'intervalle d'interrogation défini dans **Intervalle d'interrogation des mises à jour à partir de F-Secure Policy Manager** convient à votre environnement.
5. Si vous souhaitez utiliser des proxies HTTP, vérifiez que les paramètres **Utiliser le proxy HTTP** et **Adresse du proxy HTTP** conviennent à votre environnement.
6. Si vous voulez que le système utilise Policy Manager Server ou le serveur de mises à jour F-Secure comme méthode de repli quand aucun Policy Manager Proxy n'est accessible, sélectionnez **Autoriser le repli sur Policy Manager Server si les proxies Policy Manager sont inaccessibles** ou **Autoriser le repli sur le serveur de mises à jour F-Secure si les proxies Policy Manager sont inaccessibles** en conséquence.
7. Si vous souhaitez empêcher les utilisateurs de changer ces paramètres, cliquez sur le symbole de cadenas en regard des paramètres.
8. Cliquez sur pour enregistrer et distribuer la stratégie.

Configuration de Policy Manager Proxy

Si chaque bureau d'une entreprise a son propre Policy Manager Proxy, il est souvent judicieux de configurer les portables que l'utilisateur emporte d'un bureau à l'autre pour qu'ils utilisent un Policy Manager Proxy comme source de mise à jour principale.

Remarque: Policy Manager Proxy est un nouveau produit qu'il ne faut pas confondre avec F-Secure Anti-Virus Proxy.

Dans cet exemple de configuration, on suppose que les portables ont été importés dans un sous-domaine dans l'onglet **Domaines de stratégie**, que les différents bureaux de l'entreprise ont leur propre Policy Manager Proxy et que tous seront inclus dans la liste des serveurs Policy Manager Proxy.

1. Sélectionnez le sous-domaine dans lequel utiliser le Policy Manager Proxy dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Mises à jour automatiques**.
3. Assurez-vous que l'option **Activer les mises à jour automatiques** est sélectionnée.
4. Cliquez sur **Ajouter** pour ajouter de nouveaux serveurs à la liste de serveurs proxy disponibles. La fenêtre **Propriétés de serveurs proxy Policy Manager** s'ouvre.
5. Entrez un numéro de priorité pour le Policy Manager Proxy dans la zone de texte **Priorité**.

   Ces numéros sont utilisés pour définir l'ordre dans lequel les hôtes tentent de se connecter au Policy Manager Proxy. Utilisez, par exemple, `10` pour le Policy Manager Proxy situé dans le bureau où l'hôte se trouve normalement et `20`, `30` etc. pour les autres proxies.
6. Entrez l'adresse URL du serveur Policy Manager Proxy dans la zone de texte **Addresse**, puis cliquez sur **OK**.
7. Répétez les étapes ci-dessus pour ajouter les autres serveurs à la liste.
8. Une fois tous les proxies ajoutés à la liste, vérifiez que l'ordre est correct

   Au besoin, vous pouvez modifier l'ordre des proxies en changeant leur numéro de priorité.
9. Si vous souhaitez empêcher les utilisateurs de changer ces paramètres, cliquez sur le symbole de cadenas en regard des paramètres.
10. Cliquez sur pour enregistrer et distribuer la stratégie.

Remarque: Les utilisateurs finaux peuvent également ajouter un Policy Manager Proxy à la liste via l'interface utilisateur locale ; l'hôte utilise une combinaison de ces deux listes lors du téléchargement des

mises à jour de définitions de virus et de logiciels espions. Un Policy Manager Proxy ajouté par les utilisateurs finaux est tenté avant ceux ajoutés par l'administrateur.

Configuration des clients de sorte qu'ils téléchargent des mises à jour entre eux

Vous pouvez configurer les clients Automatic Update Agent de sorte qu'ils téléchargent les mises à jour entre eux, outre le téléchargement depuis les serveurs ou proxys existants.

Cette fonctionnalité est appelée Neighborcast. Le téléchargement des mises à jour peut se faire à partir des sources suivantes :

- un Policy Manager Server
- un Policy Manager Proxy
- un proxy HTTP
- un serveur de mise à jour F-Secure
- un autre Automatic Update Agent (par exemple Client Security) avec la fonctionnalité Neighborcast activé.

Pour activer Neighborcast, procédez comme suit

1. Sélectionnez le domaine cible.
2. Sélectionnez l'onglet **Paramètres** puis la page **Mises à jour automatiques**.
   a) Pour configurer des clients du domaine sélectionné, de sorte qu'ils téléchargent des mises à jour depuis d'autres clients, sélectionnez **Activer le client Neighborcast**.
   b) Pour configurer des clients du domaine sélectionné de sorte qu'ils distribuent des mises à jour vers d'autres clients, sélectionnez **Activer le serveur Neighborcast**.
3. Pour modifier le port utilisé pour la fonction Neighborcast, saisissez un nombre dans **Port Neighborcast**.

Configuration de l'analyse en temps réel

L'analyse en temps réel assure une protection permanente de l'ordinateur en analysant les fichiers lors de tout accès, ouverture ou fermeture.

Le processus tourne en tâche de fond et est donc transparent pour l'utilisateur une fois qu'il a été configuré.

Paramètres d'analyse en temps réel

Les paramètres disponibles sur la page **Paramètres** ➤ **Analyse en temps réel** sont décrits ici.

Pour activer l'analyse en temps réel, cochez la case **Activer l'analyse en temps réel**. Pour la désactiver, décochez cette même case.

Les options suivantes sont disponibles pour la sélection des éléments à analyser :

- **Tous les fichiers**

  Tous les fichiers sont analysés, quelle que soit leur extension. Cette option est déconseillée pour un usage général, car elle risque de ralentir considérablement les performances du système.

- **Fichiers avec ces extensions**

  Seuls les fichiers portant les extensions définies sont analysés. Pour indiquer des fichiers sans extension, tapez . . Vous pouvez également utiliser le caractère générique ? pour représenter une lettre quelconque. Séparez chaque extension de fichier par un espace. Cette option est recommandée pour la protection en temps réel. De nouvelles extensions de fichiers sont automatiquement ajoutées à la liste lors de la mise à jour de définitions de virus.

- **Activer les extensions exclues**

  Vous pouvez spécifier si certains fichiers ne doivent pas être analysés et entrer les extensions à exclure de l'analyse dans le champ **Extensions exclues**. C'est surtout utile lorsque l'analyse est définie sur **Tous les fichiers**.

- **Activer les objets exclus**

  Les objets exclus sont des fichiers ou dossiers individuels, qui sont normalement définis localement. Ils peuvent également être définis à partir de Policy Manager Console en cliquant avec le bouton droit sur la case à cocher **Activer les objets exclus** et en sélectionnant **Localiser en mode avancé**.

- **Analyser les lecteurs réseau**

  Cochez cette case pour analyser les fichiers auxquels vous accédez sur les lecteurs réseau.

  Important: Dans Client Security, le paramètre **Analyser les lecteurs réseau** est désactivé par défaut.

- **Analyser les fichiers créés ou modifiés**

  Normalement, les fichiers sont analysés lorsqu'ils sont ouverts pour la lecture ou l'exécution. Lorsqu'un fichier est ouvert pour l'écriture ou qu'un nouveau fichier est créé, si ce paramètre est activé, le fichier est également analysé lors de sa fermeture. Une fois ce paramètre activé, les modifications se trouvant dans des nouveaux fichiers ou des fichiers modifiés sont détectées immédiatement après leur fermeture. Ce paramètre est activé par défaut et doit rester activé.

- **Déterminer automatiquement l'action en cas d'infection**

  Pour Client Security 9 ou ultérieur et Anti-virus for Windows Servers 9 ou ultérieur, vous pouvez sélectionner cette option pour laisser le programme déterminer automatiquement l'action à exécuter dès qu'une infection est détectée lors d'une analyse.

- **Action personnalisée en cas d'action**

Si les décisions automatiques sont désactivées, vous pouvez sélectionner l'action par défaut que le programme exécutera quand un fichier infecté est détecté dans ce menu déroulant. Choisissez l'une des actions suivantes :

Action	Définition
Interroger l'utilisateur après analyse	Démarre **Assistant de nettoyage** lorsqu'un fichier infecté est détecté.
Nettoyer automatiquement	Nettoie le fichier automatiquement lorsqu'un virus est détecté.
Renommer automatiquement	Renomme le fichier automatiquement lorsqu'un virus est détecté.
Supprimer automatiquement	Supprime le fichier automatiquement lorsqu'un virus est détecté. Notez que cette option supprime également le fichier infecté par le virus. Cette option est donc déconseillée.
Signaler uniquement	Indique qu'un virus a été détecté et vous empêche d'ouvrir l'objet infecté. Cette option se contente de vous signaler la présence du virus. Elle n'entreprend aucune action à son encontre.
Mettre en quarantaine automatiquement	Place automatiquement le fichier infecté en **quarantaine**.

- Protéger le fichier « Hôtes »

  Une fois cette option activée, le fichier « Hôtes » sera protégé contre les modifications effectuées par les logiciels espions. Il se peut que certains programmes malveillants essaient d'utiliser ce fichier pour remplacer l'adresse IP d'un nom DNS connu par l'adresse IP d'un site Web malveillant.
- **Rechercher des cookies de suivi**

  Quand ce paramètre est activé, les cookies de suivi seront détectés. L'analyse en temps réel détectera uniquement les cookies stockés sur un disque, non les cookies stockés dans le cache du navigateur Web. L'analyse manuelle détectera les cookies stockés sur un disque et dans le cache du navigateur Web.

Gestion des extensions de fichier

Client Security a une liste d'extensions incluses définies dans la stratégie (ceci peut correspondre à « tous les fichiers »). Les **extensions incluses** peuvent également faire partie d'une mise à jour de définitions de virus. Ces extensions incluses sont d'abord combinées par Client Security, puis toutes les extensions exclues sont supprimées de cette liste afin de déterminer la liste réelle des fichiers à analyser. Cette procédure s'applique à l'analyse en temps réel, l'analyse manuelle et l'analyse du courrier électronique.

Activation de l'analyse en temps réel pour l'ensemble du domaine

Dans cet exemple, l'analyse en temps réel est activée pour l'ensemble du domaine.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Analyse en temps réel**.
3. Cochez la case **Activer l'analyse en temps réel**.
4. Sélectionnez **Fichiers avec ces extensions** dans la liste déroulante **Fichiers à analyser**.

5. Sélectionnez l'action à exécuter lorsqu'un fichier infecté est détecté dans la liste déroulante **Analyse des fichiers : Action en cas d'infection**.
6. Vérifiez que les autres paramètres de cette page conviennent pour votre système et modifiez-les au besoin.
7. Cliquez sur pour enregistrer et distribuer la stratégie.

Activation forcée de l'analyse en temps réel sur tous les hôtes

Dans cet exemple, l'analyse en temps réel est configurée de sorte que les utilisateurs ne puissent pas la désactiver ; les hôtes restent ainsi protégés dans toutes les circonstances.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Analyse en temps réel**.
3. Cochez la case **Activer l'analyse en temps réel**.
4. Sélectionnez **Fichiers avec ces extensions** dans la liste déroulante **Fichiers à analyser**.
5. Sélectionnez l'action à exécuter lorsqu'un fichier infecté est détecté dans la liste déroulante **Action personnalisée en cas d'infection**.

   Sinon, sélectionnez **Déterminer automatiquement l'action en cas d'infection** afin que le produit décide automatiquement de l'action à exécuter.
6. Vérifiez que les autres paramètres de cette page conviennent pour votre système et modifiez-les au besoin.
7. Cliquez sur **Interdire les modifications utilisateur** afin d'empêcher les utilisateurs de désactiver l'analyse en temps réel sur leurs ordinateurs.
   Un symbole de cadenas fermé s'affiche alors en regard de tous les paramètres de cette page.
8. Cliquez sur pour enregistrer et distribuer la stratégie.

Exclusion du fichier .pst de Microsoft Outlook de l'analyse en temps réel

Si vous avez configuré une analyse en temps réel de tous les fichiers, vous souhaiterez peut-être exclure le fichier `.PST` de Microsoft Outlook de l'analyse afin de ne pas ralentir inutilement le système (les fichiers .PST sont généralement très volumineux et longs à analyser).

Le fichier `.PST` est exclu de l'analyse pour l'ensemble du domaine, comme suit :

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Analyse en temps réel.**.
3. Cochez la case **Activer les extensions exclues**.
4. Entrez l'extension `PST` dans la zone de texte **Extensions exclues**.

   Notez que l'extension doit être ajoutée sans le point qui précède (`.`).
5. Si vous souhaitez empêcher les utilisateurs de changer ces paramètres, cliquez sur le symbole de cadenas en regard des paramètres.
6. Cliquez sur pour enregistrer et distribuer la stratégie.

Configuration de DeepGuard

DeepGuard est un système de prévention des intrusions fondé sur les hôtes, qui analyse le comportement des fichiers et des programmes.

Il peut être utilisé pour bloquer les fenêtres publicitaires indépendantes intempestives et pour protéger les paramètres système importants, ainsi que les paramètres d'Internet Explorer, de toute modification non souhaitée.

Si une application essaie d'effectuer une action potentiellement dangereuse, le système vérifie si elle est fiable. Les applications sûres sont autorisées, tandis que les actions provenant d'applications non sûres sont bloquées.

Lorsque DeepGuard est activé, vous pouvez configurer le contrôle des applications de façon à ce qu'il demande aux utilisateurs l'action à effectuer lorsque DeepGuard n'approuve pas une application.

Paramètres DeepGuard

Les paramètres DeepGuard, affichés sur la page **Paramètres** ➤ **Analyse en temps réel**, sont décrits dans la présente section.

Pour activer DeepGuard, sélectionnez Activer DeepGuard.

Vous pouvez sélectionner l'action à exécuter lorsqu'une tentative de modification du système est détectée. Les actions possibles sont les suivantes :

Action	Définition
Toujours demander l'autorisation	DeepGuard demande aux utilisateurs s'ils souhaitent autoriser ou bloquer les actions surveillées, même lorsque l'application est identifiée comme sûre.
Demander en cas de doute	DeepGuard demande aux utilisateurs s'ils souhaitent autoriser ou bloquer les actions surveillées uniquement si DeepGuard ne peut pas identifier l'application comme sûre ou non sûre (option par défaut).
Automatique : ne pas demander	DeepGuard bloque les applications non sûres et autorise automatiquement les applications sûres sans poser aucune question à l'utilisateur.

Si vous rencontrez des problèmes avec des programmes légitimes bloqués par DeepGuard, vous pouvez essayer de désactiver l'option **Utiliser une surveillance de processus avancée**. Pour une protection optimale, DeepGuard modifie temporairement l'exécution des programmes. Certains programmes peuvent ne pas fonctionner à cause de cette surveillance de processus avancée. Cela concerne les programmes qui vérifient leur propre intégrité.

Requêtes serveur DeepGuard

Les requêtes serveur DeepGuard fournissent des informations à jour permettant de détecter des programmes malveillants et de réduire le nombre de fausses alertes détectées.

Sélectionnez **Utiliser les requêtes serveur pour améliorer la précision de détection** pour vérifier auprès des serveurs F-Secure quand DeepGuard détecte une application inconnue. Nous vous recommandons d'activer les requêtes serveur pour deux raisons :

- Un ordinateur avec requêtes serveur activées est mieux protégé. Moins de temps s'écoule entre la détection d'une nouvelle menace informatique et la protection contre cette menace.

- Un ordinateur avec requêtes serveur activées génère nettement moins de boîtes de dialogue demandant si un processus inconnu doit être autorisé à s'exécuter ou non. L'utilisateur a moins de risques de prendre une décision qui pourrait mettre en péril la sécurité de son ordinateur. L'utilisateur est aussi moins dérangé dans son travail.

Que dois-je connaître à propos des requêtes serveur ?

Les requêtes serveur nécessitent un accès à internet pour fonctionner. Si votre réseau n'autorise l'accès qu'à travers un proxy HTTP, définissez le paramètre de proxy HTTP Automatic Update Agent dans votre adresse de serveur proxy pour assurer le fonctionnement des requêtes réseau.

Configuration de la recherche de rootkits (Blacklight)

La recherche de rootkits peut être utilisée pour rechercher des fichiers et des lecteurs cachés par des rootkits.

Les rootkits servent typiquement à masquer les logiciels malveillants, tels que les logiciels espions, des utilisateurs, des outils systèmes et des scanneurs antivirus traditionnels. Les éléments cachés par des rootkits sont souvent infectés par des virus, des vers ou des chevaux de Troie.

Paramètres de la recherche de rootkits

Les paramètres de la recherche de rootkits sont affichés sur la page **Analyse manuelle** de l'onglet **Paramètres**.

La recherche de rootkits peut être exécutée manuellement ou dans le cadre d'une vérification complète de l'ordinateur.

Sélectionnez **Activer la recherche de rootkits** pour activer la recherche de fichiers et lecteurs cachés par des rootkits. Cette option permet également aux utilisateurs de lancer des analyses locales rapides afin de rechercher des rootkits et d'autres éléments cachés.

Sélectionnez **Inclure la recherche de rootkits dans l'analyse complète de l'ordinateur** pour rechercher des éléments cachés par des rootkits lors de l'exécution d'une analyse complète de l'ordinateur à partir de l'hôte local ou lors du lancement d'une analyse manuelle à partir de Policy Manager Console.

Sélectionnez **Signaler les éléments suspects après vérification complète de l'ordinateur** pour spécifier que les éléments suspects détectés doivent être affichés dans l'assistant de nettoyage et dans le rapport d'analyse après une analyse complète de l'ordinateur. Lorsque cette option est sélectionnée, les rapports d'analyse afficheront si certains éléments cachés par les rootkits ont été détectés sur les hôtes administrés.

Lancement de la recherche de rootkits dans l'ensemble du domaine

Dans cet exemple, une recherche de rootkits est lancée dans l'ensemble du domaine.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Analyse manuelle**.
3. Dans la section **Recherche de rootkits**, assurez-vous de bien cocher la case **Activer la recherche de rootkits**.
4. Cochez la case **Signaler les éléments suspects après vérification complète de l'ordinateur**.
5. Vérifiez que les autres paramètres de cette page conviennent et modifiez-les au besoin.
6. Accédez à l'onglet **Opérations** et cliquez sur le bouton **Recherche de virus et de logiciels espions**.

   Remarque: Vous devez distribuer la stratégie pour lancer l'opération.

7. Cliquez sur pour enregistrer et distribuer la stratégie.

Une fois la recherche terminée sur les hôtes locaux, vous pouvez voir si des rootkits ont été détectés à partir des **Rapports d'analyse** de l'onglet **Rapports**.

Configuration de l'analyse du courrier électronique

L'analyse du courrier électronique peut être utilisée pour protéger les messages électroniques entrants et sortants contre les virus.

L'activation de cette analyse en sortie vous évite en outre de diffuser sans le vouloir des pièces jointes infectées. Cette section décrit les paramètres d'analyse du courrier électronique et présente un exemple de configuration pratique.

L'analyse du courrier électronique analyse tout le trafic POP, IMAP et SMTP. Si le protocole SSL est utilisé, toutes les pièces jointes reçues via SSL sont également analysées lors de leur stockage dans le cache du courrier électronique local. Tous les fichiers envoyés sont traités par l'analyse en temps réel.

Paramètres d'analyse du courrier électronique

Les paramètres d'analyse du courrier électronique sont affichés sur la page **Analyse du courrier électronique** de l'onglet **Paramètres**.

Pour activer l'analyse des messages électroniques entrants et des pièces jointes (trafic POP3), sélectionnez **Activer l'analyse du courrier entrant**.

Pour activer l'analyse des messages électroniques sortants et des pièces jointes (trafic SMTP), sélectionnez **Activer l'analyse du courrier sortant**.

Vous pouvez sélectionner l'action à exécuter lorsqu'un message infecté est détecté. Les actions possibles sont les suivantes :

- Analyse du courrier électronique entrant :
  1. **Action à la réception d'une pièce jointe infectée** :
     - **Nettoyer pièce jointe** démarre l'Assistant de nettoyage chaque fois qu'une pièce jointe infectée est détectée.
     - **Supprimer pièce jointe** supprime la pièce jointe.
     - **Avertir uniquement** ignore la pièce jointe mais la signale à l'administrateur.
  2. **Action en cas d'échec de l'analyse** :
     - **Supprimer la pièce jointe** supprime la pièce jointe.
     - **Avertir uniquement** ignore l'échec de l'analyse mais le signale à l'administrateur.
  3. **Action si des parties de messages sont déformées** :
     - **Supprimer la partie de message** supprime le message.
     - **Avertir uniquement** ignore la partie déformée mais la signale à l'administrateur.

- Analyse du courrier électronique sortant :
  1. **Action à l'envoi d'une pièce jointe infectée** :
     - **Bloquer le courrier électronique** empêche d'envoyer le message électronique.
     - **Avertir uniquement** ignore la pièce jointe mais la signale à l'administrateur.
  2. **Action en cas d'échec de l'analyse** :
     - **Bloquer message électronique** empêche d'envoyer le message électronique.
     - **Avertir uniquement** ignore l'échec de l'analyse mais le signale à l'administrateur.
  3. **Action si des parties de messages sont déformées** :
     - **Supprimer la partie de message** supprime le message.

- **Avertir uniquement** ignore la partie déformée mais la signale à l'administrateur.

Avertissement: L'option **Avertir uniquement** est dangereuse et ne doit pas être utilisée dans des conditions normales.

Pour enregistrer les messages bloqués dans le dossier **Boîte d'envoi** des utilisateurs finaux, sélectionnez **Enregistrer les messages bloqués dans la boîte d'envoi**. L'utilisateur doit déplacer, supprimer ou modifier le message bloqué dans sa **Boîte d'envoi** pour pouvoir envoyer d'autres messages.

Les types de fichier inclus à l'analyse du courrier électronique et exclus de celle-ci sont déterminés en fonction des paramètres indiqués sur la page **Analyse en temps réel**.

Si vous souhaitez qu'une boîte de dialogue s'affiche lorsque des fichiers volumineux sont analysés, sélectionnez **Indiquer l'avancement en cas d'analyse de fichiers volumineux** et définissez la limite de temps dans le champ **Indiquer l'avancement après**.

Si vous souhaitez qu'un rapport s'affiche à la fin de l'analyse, sélectionnez **Afficher le rapport si des infections sont détectées**.

Activation de l'analyse du courrier électronique pour les messages entrants et sortants

Dans cet exemple, l'analyse du courrier électronique est activée pour les messages tant entrants que sortants.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Analyse du courrier électronique**.
3. Configuration de l'analyse du courrier électronique entrant :
   a) Sélectionnez **Activer l'analyse du courrier entrant**.
   b) Sélectionnez l'action à effectuer dans la liste déroulante **Action à la réception d'une pièce jointe infectée**.
   c) Sélectionnez l'action à effectuer dans la liste déroulante **Action en cas d'échec de l'analyse**.
   d) Sélectionnez l'action à effectuer dans la liste déroulante **Action si des parties de messages sont déformées**.
4. Configuration de l'analyse du courrier électronique sortant :
   a) Sélectionnez **Activer l'analyse du courrier sortant**.
   b) Sélectionnez l'action à effectuer dans la liste déroulante **Action à l'envoi d'une pièce jointe infectée**.
   c) Sélectionnez l'action à effectuer dans la liste déroulante **Action en cas d'échec de l'analyse**.
   d) Sélectionnez l'action à effectuer dans la liste déroulante **Action si des parties de messages sont déformées**.
5. Vérifiez les **paramètres généraux**.
   Vérifiez que les autres paramètres de cette page conviennent pour votre système et modifiez
6. Cliquez sur pour enregistrer et distribuer la stratégie.

Configuration de l'analyse du trafic Web (HTTP)

L'analyse du trafic Web peut être utilisée pour protéger l'ordinateur contre des virus dans du trafic HTTP.

Lorsqu'elle est activée, elle analyse les fichiers HTML, les fichiers images, les applications ou les fichiers exécutables téléchargés, ou d'autres types de fichiers téléchargés. Elle supprime les virus automatiquement des téléchargements. Vous pouvez également activer un panneau de notification présenté à l'utilisateur final chaque fois que l'analyse du trafic Web bloque des virus dans le trafic Web et des téléchargements.

Cette section décrit les paramètres d'analyse du trafic Web et présente des exemples de configuration pratiques.

Paramètres d'analyse du trafic Web

Les paramètres de l'analyse HTTP, qui sont affichés sur la page **Paramètres** ➤ **Analyse du trafic Web**, sont décrits dans cette section.

Pour activer l'analyse HTTP, sélectionnez **Activer l'analyse HTTP**.

Dans la liste déroulante **Action en cas d'infection**, vous pouvez sélectionner ce qu'il convient de faire lorsqu'une infection est détectée dans du trafic HTTP. Les actions disponibles sont les suivantes :

- **Bloquer** bloque l'accès au fichier infecté.
- **Avertir uniquement** ignore l'infection mais la signale à l'administrateur.

Dans la liste déroulante **Action en cas d'échec de l'analyse**, vous pouvez sélectionner ce qu'il convient de faire si un fichier dans du trafic HTTP ne peut pas être analysé. Ce paramètre est utilisé, par exemple, lors du traitement d'archives protégées par mot de passe. Les actions disponibles sont les suivantes :

- **Bloquer** bloque le fichier qui n'a pas pu être analysé.
- **Avertir uniquement** ignore le fichier mais le signale à l'administrateur.

Sélectionnez **Analyser les fichiers compressés** pour analyser les fichiers compressés `ZIP`, `ARJ`, `LZH`, `RAR`, `CAB`, `TAR`, `BZ2`, `GZ`, `JAR` et `TGZ`.

Vous pouvez spécifier une liste de sites fiables dans la table **Sites approuvés**. Le contenu des sites approuvés ne sera pas analysé à la recherche de virus.

Activation de l'analyse du trafic Web pour l'ensemble du domaine

Dans cet exemple, l'analyse HTTP est activée pour l'ensemble du domaine.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Analyse HTTP**.
3. Cochez la case **Activer l'analyse HTTP**.
4. Assurez-vous que **Action en cas d'infection** a la valeur **Bloquer**.
5. Vérifiez que **Action en cas d'échec de l'analyse** a la valeur **Bloquer**.
6. Vérifiez que les autres paramètres de cette page conviennent pour votre système et modifiez-les au besoin.
7. Cliquez sur pour enregistrer et distribuer la stratégie.

Exclusion d'un site Web de l'analyse HTTP

Vous pouvez exclure un site Web ou certaines pages Web de l'analyse HTTP en les définissant dans la table **Sites approuvés**.

L'exclusion d'un site Web pourrait être indiquée, par exemple, si le site contient du contenu à diffusion en continu non reconnaissable, pouvant imposer des attentes prolongées à l'utilisateur (voir le paramètre Dépassement du délai de téléchargement).

Dans cet exemple de configuration, l'ensemble d'un domaine (www.example.com) et un sous-répertoire d'un autre domaine (www.example2.com/news) sont exclus de l'analyse HTTP.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres**, puis sélectionnez la page **Analyse du trafic Web**.
3. Exclure un domaine de l'analyse HTTP :

   Pour exclure l'ensemble d'un domaine de l'analyse HTTP, entrez l'URL du domaine dans la table **Sites approuvés** de la façon suivante :

   a) Cliquez sur le bouton **Ajouter** sous la table **Sites approuvés**.
   Vous créez ainsi une nouvelle ligne dans la table.
   b) Cliquez sur la ligne que vous venez de créer afin qu'elle devienne active et saisissez `http://*.example.com/*`.
   Vous excluez ainsi tous les sous-domaines.
   c) Cliquez sur le bouton **Ajouter** sous la table **Sites approuvés**.
   Vous créez ainsi une ligne dans la table.
   d) Cliquez sur la ligne que vous venez de créer afin qu'elle devienne active et tapez `http://example.com/*`.
   Vos excluez ainsi le domaine de second niveau.
4. Exclure un sous-répertoire de l'analyse HTTP :

   Pour exclure un sous-répertoire de l'analyse HTTP, entrez l'URL du domaine avec le chemin du répertoire dans la table **Sites approuvés** de la manière suivante :

   a) Cliquez sur le bouton **Ajouter** sous la table **Sites approuvés**.
   Vous créez ainsi une nouvelle ligne dans la table.
   b) Cliquez sur la ligne que vous venez de créer afin qu'elle devienne active et tapez `http://www.example2.com/news/*`.
5. Cliquez sur  pour enregistrer et distribuer la stratégie.

Configuration de la recherche de logiciels espions

La recherche de logiciels espions protège les hôtes contre différents types de logiciels espions, par exemple des analyseurs de données, des outils de surveillance et des numéroteurs.

En mode de gestion centralisée, la recherche de logiciels espions peut être configurée, par exemple, pour signaler à l'administrateur les éléments de logiciels espions trouvés sur des hôtes ou pour mettre automatiquement en quarantaine tous les éléments de logiciels espions trouvés. Il est également possible de permettre l'utilisation de certaines applications de logiciels espions en les spécifiant comme logiciels espions autorisés sur la page Contrôle de logiciels espions.

Remarque à propos du nettoyage des logiciels espions et des riskwares

La notion de logiciels est relativement vague et recoupe toute une gamme de logiciels allant d'applications parfaitement légitimes aux virus/chevaux de Troie. Certains logiciels espions peuvent être nécessaires à l'exécution d'applications ordinaires, tandis que d'autres ne sont que des antiprogrammes dont l'exécution doit être rigoureusement interdite et rendue impossible. Par défaut, la recherche de logiciels espions est configurée de manière à permettre l'exécution de tous les logiciels espions.Vous pouvez vérifier s'il convient d'autoriser l'exécution de certains logiciels espions avant de renforcer la sécurité et d'interdire l'exécution de tous les nouveaux logiciels espions.

La recherche de logiciels espions détecte et signale également la présence de riskwares. Le riskware est un programme qui ne cause pas de dommage intentionnellement, mais qui peut être dangereux s'il est utilisé à mauvais escient, en particulier s' il n'est pas installé correctement. Ces programmes regroupent par exemple les logiciels de dialogue en direct (IRC) ou de transfert des fichiers.

Paramètres de contrôle des logiciels espions

Les paramètres de recherche de logiciels espions sont décrits ici.

La recherche de logiciels espions est fournie dans le cadre des analyses en temps réel et manuelle. Quand l'option **Analyse en temps réel activée** est sélectionnée sur la page **Analyse en temps réel**, la recherche de logiciels espions est activée. De la même façon, quand une analyse manuelle est exécutée, les logiciels espions sont automatiquement inclus dans l'analyse. L'action réalisée lors de la détection de logiciels espions est déterminée par l'action sélectionnée sur les pages **Analyse en temps réel** et **Analyse manuelle**.

La table **Applications exclues de la recherche de logiciels espions** affiche les logiciels espions et riskwares qui ont été autorisés par l'administrateur.

La table **Logiciels espions et riskwares signalés par les hôtes** contient les informations suivantes :

Logiciels espions et riskwares rapportés par les hôtes	
Nom du logiciel espion ou riskware	Affiche le nom du logiciel espion ou du riskware mis en quarantaine.
Type	Affiche le type de logiciel espion. Le type peut être logiciel publicitaire, analyseur de données, numéroteur, antiprogramme, outil de surveillance, numéroteur pornographique, riskware, vulnérabilité, ver, cookie (cookie de suivi) ou élément divers.
Gravité	Affiche la gravité de l'élément de logiciel espion. Il s'agit d'une valeur comprise entre 3 et 10.
Hôte	Affiche le nom de l'hôte sur lequel l'élément de logiciel espion a été trouvé.

Logiciels espions et riskwares rapportés par les hôtes	
Etat du logiciel espion	Affiche l'état actuel de l'élément de logiciel espion. Les états sont : **Potentiellement actif** : l'élément de logiciel espion est toujours potentiellement actif sur l'hôte. Aucune action n'a été prise sur l'hôte contre l'élément de logiciel espion. **Supprimé** : l'élément de logiciel espion a été supprimé de l'hôte. **Mis en quarantaine** - L'élément de logiciel espion a été mis en quarantaine sur l'hôte. **Actuellement en quarantaine** : l'élément de logiciel espion est actuellement en quarantaine sur l'hôte.
Tampon horodateur	Affiche la date et l'heure de découverte de l'élément de logiciel espion sur l'hôte.

Le logiciel espion signalé par les hôtes sera nettoyé si vous exécutez une recherche manuelle de logiciel espion sur les hôtes, mais aussi lorsque le logiciel espion mis en quarantaine est supprimé périodiquement sur les hôtes.

Configuration du contrôle des logiciels espions pour l'ensemble du domaine

Cet exemple indique comment configurer le contrôle des logiciels espions de telle sorte qu'il soit transparent pour les utilisateurs finals et qu'il les protège contre les logiciels espions et les cookies de suivi.

Lorsque vous configurez le contrôle des logiciels espions pour la première fois, il convient d'utiliser un environnement de test restreint composé d'hôtes sur lesquels sont installées les applications normalement utilisées dans votre entreprise. À ce stade, vous pouvez également autoriser certaines applications, si cela est nécessaire. Après la phase de test, vous pouvez distribuer la stratégie à l'ensemble du domaine géré.

Le contrôle des logiciels espions détecte les riskwares. Le riskware est un programme qui ne cause pas de dommage intentionnellement, mais qui peut être dangereux s'il est utilisé à mauvais escient, en particulier s'il n'est pas installé correctement. Ces programmes regroupent par exemple les programmes de dialogue en direct (IRC) ou encore des programmes destinés au transfert de fichiers. Si vous souhaitez autoriser l'utilisation de ces programmes dans le domaine administré, vous devez les inclure dans l'environnement de test et permettre leur utilisation lors de la vérification et de la configuration des règles relatives aux applications du tableau **Logiciels espions et riskwares signalés par les hôtes**.

1. Création d'un domaine de test et activation de la recherche de logiciels espions :
   a) Créez un environnement de test avec quelques ordinateurs où tournent les programmes normalement utilisés dans votre entreprise.
   b) Importez ces hôtes dans le domaine géré de manière centralisée.
   c) Accédez à l'onglet **Paramètres** et sélectionnez la page **Analyse en temps réel**.
   d) Vérifiez que l'option**Analyse en temps réel activée** est sélectionnée.
      Vous pouvez également lancer une recherche manuelle de logiciels espions sur les hôtes.
   e) Cliquez sur pour enregistrer et distribuer la stratégie.
2. Vérifier les logiciels espions et riskwares signalés :

Une liste des logiciels espions et riskwares qui ont été trouvés pendant la recherche s'affiche dans la table **Logiciels espions et riskwares signalés par les hôtes**. Cette table s'affiche sur la page **Contrôle des logiciels espions**.

a) Vérifiez la liste des logiciels espions et riskwares signalés.
b) Si des applications sont nécessaires dans votre entreprise, sélectionnez-les dans le tableau et cliquez sur **Exclure une application**.
Une boîte de dialogue vous invitant à confirmer l'action s'ouvre.
c) Vérifiez les informations affichées dans la boîte de dialogue, puis si vous souhaitez autoriser l'exécution du logiciel espion ou riskware sur l'hôte ou le domaine, cliquez sur **OK**.
L'application sélectionnée sera placée dans la table **Applications exclues de la recherche de logiciels espions**.

3. Si vous souhaitez être certain que les utilisateurs ne peuvent pas autoriser l'exécution de logiciels espions ou de riskwares sur leur ordinateur, assurez-vous que **Autoriser les utilisateurs à définir les éléments de logiciels espions autorisés** a la valeur **Non autorisé**.
4. Vérifiez que les paramètres de recherche manuelle de logiciels espions sont valides pour le domaine géré.
5. Cliquez sur pour enregistrer et distribuer la stratégie.

Lancement de la recherche de logiciels espions dans l'ensemble du domaine

Dans cet exemple, une analyse manuelle est lancée dans l'ensemble du domaine.

Cette intervention nettoie partiellement la table **Logiciels espions et riskware signalés par les hôtes**.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Comme la tâche d'analyse manuelle inclut également la recherche manuelle de virus, vérifiez les paramètres sur la page **Analyse manuelle** et modifiez-les si nécessaire.
3. Accédez à l'onglet **Opérations** et cliquez sur le bouton **Recherche de virus et de logiciels espions**.

   Remarque: Vous devez distribuer la stratégie pour lancer l'opération.

4. Cliquez sur pour enregistrer et distribuer la stratégie.

Autorisation de l'utilisation d'un composant de logiciel espion ou de riskware

Dans cet exemple, l'utilisation d'un composant de logiciel espion ou de riskware qui a été trouvé pendant la recherche de logiciels espions est autorisée pour un hôte.

1. Dans l'onglet **Domaines de stratégie**, sélectionnez l'hôte pour lequel vous souhaitez autoriser l'utilisation de logiciels espions.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Contrôle des logiciels espions**.
3. Sélectionnez le composant de logiciel espion que vous voulez autoriser dans la table **Logiciels espions et riskwares signalés par les hôtes**, puis cliquez sur **Exclure une application**.
Une boîte de dialogue vous invitant à confirmer l'action s'ouvre.
4. Vérifiez les informations affichées dans la boîte de dialogue, puis si vous souhaitez autoriser l'exécution de l'application sur l'hôte ou le domaine, cliquez sur **OK**.
L'application sélectionnée sera placée dans le tableau **Applications exclues de la recherche de logiciels espions**.
5. Cliquez sur pour enregistrer et distribuer la stratégie.

Gestion des objets en quarantaine

La gestion de la quarantaine vous permet de traiter des objets qui ont été mis en quarantaine sur des machines hôtes de façon centralisée.

Tous les fichiers infectés, logiciels espions ou riskwares qui ont été mis en quarantaine sur des machines hôtes sont affichés sur la page **Paramètres** ➤ **Gestion de la quarantaine**. A partir de la, vous pouvez libérer les objets de la quarantaine ou les supprimer.

Remarque: La gestion de la quarantaine doit être principalement utilisée à des fins de dépannage. Par exemple, si une application vitale est considérée comme un riskware et qu'elle n'a pas encore été incluse à la base de données de définition des virus, vous pouvez utiliser la gestion de la quarantaine pour autoriser son utilisation. Certains cas sont relativement rares, et dès que des nouvelles mises à jour de définition des virus qui considérent l'application comme étant normale seront disponibles, le problème sera automatiquement résolu.

Suppression des objets en quarantaine

Les fichiers infectés, logiciels espions ou riskwares, qui ont été mis en quarantaine sur des hôtes, peuvent être supprimés de la quarantaine et par conséquent de la machine hôte.

1. Sélectionnez le domaine cible.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Gestion de la quarantaine**.
3. Sélectionnez l'objet en quarantaine que vous voulez supprimer sur le tableau **Objets en quarantaine**, puis cliquez sur **Supprimer**.
   Cet objet est déplacé vers le tableau **Actions à réaliser sur les objets en quarantaine**, avec **Supprimer** comme **Action** pour l'objet.
4. Cliquez sur pour enregistrer et distribuer la stratégie.

Libération d'objets en quarantaine

Les fichiers infectés, les logiciels espions ou les riskwares qui ont été mis en quarantaine sur les hôtes peuvent être libérés de la quarantaine. Dans ce cas, ils sont autorisés sur les machines hôtes, y sont accessibles et exécutables normalement.

1. Sélectionnez le domaine cible.
2. Créez une règle d'exclusion pour l'objet.

   Les règles d'exlcusion sont requises pour vérifier que l'objet ne sera pas mis en quarantaine à nouveau. Si l'objet est répertorié comme virus ou fichier infecté :

   a) Accédez à la page **Paramètres** ➤ **Gestion de la quarantaine** et copiez le chemin d'accès au fichier de l'objet.
   b) Accédez à la page **Paramètres** ➤ **Analyse en temps réel**.
   c) Cliquez avec le bouton droit sur **Activer les objets exclus** et sélectionnez **Localiser en mode avancé** dans le menu contextuel.
   L'interface utilisateur s'affiche en **Mode Avancé**.
   d) Dans l'onglet **Stratégie**, sélectionnez **Objets exclus**.
   e) Cliquez sur **Ajouter** et saisissez le chemin d'accès au fichier de l'objet en quarantaine.
   f) Sélectionnez **Affichage** ➤ **Mode antivirus** dans le menu pour revenir sur l'interface utilisateur du **Mode antivirus** et vérifiez que l'option **Activer les objets exclus** est sélectionnée sur la page **Paramètres** ➤ **Analyse en temps réel**.

   Si l'objet est un logiciel espion ou un riskware :

   a) Accédez à la page **Paramètres** ➤ **Contrôle des logiciels espions**.

b) Sélectionnez l'objet que vous voulez autoriser sur la table **Logiciels espions et riskwares signalés par les hôtes** et cliquez sur **Exclure une application**.
Une boîte de dialogue vous invitant à confirmer l'action s'ouvre, après quoi l'application sélectionnée sera déplacée vers la table **Applications exclues de la recherche de logiciels espions**.

3. Accédez à l'onglet **Paramètres** et sélectionnez la page **Gestion de la quarantaine**.
4. Sélectionnez l'objet de la quarantaine que vous voulez autoriser dans la table **Objets en quarantaine** et cliquez sur **Libérer**.
L'objet est déplacé vers la table **Actions à exécuter sur les objets en quarantaine**, avec **Libérer** comme **Action** définir pour l'objet.
5. Cliquez sur  pour enregistrer et distribuer la stratégie.

Interdiction de modification des paramètres par les utilisateurs

Si vous souhaitez faire en sorte que les utilisateurs ne puissent pas modifier certains paramètres de protection antivirus, vous pouvez définir ces paramètres comme étant finaux.

Cela peut se faire de différentes manières :

- Si vous souhaitez empêcher les utilisateurs de changer un paramètre défini, cliquez sur le symbole de cadenas qui lui correspond.
- Lorsque vous êtes dans l'une des pages de l'onglet **Paramètres**, vous pouvez définir tous les paramètres comme étant finaux en une fois en cliquant sur **Interdire les modifications utilisateur**. Ce raccourci spécifique à la page concerne uniquement les paramètres auxquels est associé un verrou et actionne tous les verrous de la page en une fois.
- Si vous souhaitez définir comme étant finaux tous les paramètres de la protection antivirus et de la protection Internet, accédez à l'onglet **Paramètres** et à la page **Gestion centralisée**, puis cliquez sur **Ne pas autoriser les utilisateurs à modifier des paramètres**. Cette opération définit également comme étant finaux les paramètres du **Mode avancé**.

Marquage de tous les paramètres de protection antivirus comme finaux

Dans cet exemple, tous les paramètres de la protection antivirus sont définis comme finaux.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Mises à jour automatiques**.
3. Vérifiez que tous les paramètres de cette page sont corrects.
4. Cliquez sur **Interdire les modifications utilisateur**.
   Tous les paramètres de cette page sont maintenant marqués comme finaux.
5. Sélectionnez la page **Analyse en temps réel**.
6. Vérifiez que tous les paramètres de cette page sont corrects.
7. Cliquez sur **Interdire les modifications utilisateur**.
8. Sélectionnez la page **Analyse manuelle**.
9. Vérifiez que tous les paramètres de cette page sont corrects.
10. Cliquez sur **Interdire les modifications utilisateur**.
11. Sélectionnez la page **Analyse du courrier électronique**.
12. Vérifiez que tous les paramètres de cette page sont corrects.
13. Cliquez sur **Interdire les modifications utilisateur**.
14. Cliquez sur  pour enregistrer et distribuer la stratégie.

Configuration de l'envoi d'alertes

Cette section décrit comment configurer le produit de façon à envoyer les alertes de virus Client Security à une adresse électronique et comment désactiver les fenêtres contextuelles d'alerte.

Il est judicieux d'envoyer toutes les alertes de virus aux administrateurs par courrier électronique afin de s'assurer qu'ils sont informés de toute attaque possible aussi rapidement que possible.

Configuration de Client Security de façon à envoyer les alertes de virus à une adresse électronique

Dans cet exemple, toutes les alertes de sécurité générées par les clients gérés Client Security sont transmises au courrier électronique.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Envois d'alertes**.
3. Configuration de l'**envoi d'alertes par courrier électronique** :

   Si l'envoi d'alertes par courrier électronique n'a pas encore été configuré, vous pouvez le faire maintenant, de la manière suivante :

   a) Entrez l'adresse du serveur SMTP dans le champ **Adresse du serveur de messagerie (SMTP)**.

      Utilisez le format suivant :

      `<hôte>[:<port>]` où `hôte` est le nom DNS ou l'adresse IP du serveur SMTP et `port` est le numéro de port du serveur SMTP.

   b) Entrez l'adresse de l'expéditeur pour les messages d'alerte par courrier électronique dans le champ **Adresse de l'expéditeur [De]**.

   c) Entrez l'objet du message d'alerte dans le champ **Objet du courrier électronique :**.

      Pour obtenir une liste des paramètres utilisables dans l'objet du message, reportez-vous au texte d'aide MIB.

4. Configuration de la **transmission d'alertes** :

   Le tableau **Transmission des alertes** permet de configurer la destination des différents types d'alertes.

   a) Cochez la case **Adresse électronique** sur la ligne **Alerte de sécurité**.
   La boîte de dialogue **Adresses du destinataire [A]**.

   b) Sélectionnez **Utiliser la même adresse pour tous les produits** et entrez l'adresse électronique dans le champ activé.

      Si vous souhaitez envoyer les alertes à plusieurs adresses, séparez-les par des virgules.

   c) Une fois terminé, cliquez sur **OK**.

5. Cliquez sur pour enregistrer et distribuer la stratégie.

Désactivation des fenêtres indépendantes d'alerte de Client Security

Dans cet exemple, les alertes Client Security sont configurées de sorte qu'aucune fenêtre indépendante ne s'affiche sur l'écran des utilisateurs.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Envois d'alerte**.
3. Désactivez les cases à cocher pour tous les produits dans la colonne **Interface utilisateur locale**.
4. Cliquez sur pour enregistrer et distribuer la stratégie.

Surveillance des virus sur le réseau

Policy Manager offre plusieurs méthodes et niveaux de détails pour la surveillance des infections sur votre réseau.

La meilleure façon de vérifier s'il y a des virus sur le réseau est de vérifier la section **Protection antivirus** de l'onglet **Résumé**. Si cette section affiche de nouvelles infections, vous pouvez accéder à des informations plus détaillées en cliquant sur **Afficher l'état d'infection des hôtes....**. L'onglet **Etat** et la page **Protection antivirus** s'affichent, montrant les détails de l'état d'infection de chaque hôte.

Vous pouvez également examiner les onglets **Alertes** et **Rapports** pour afficher les rapports d'analyse des différents hôtes.

Test de la protection antivirus

Pour vérifier le bon fonctionnement de Client Security, vous pouvez utiliser un fichier de test spécial qui sera détecté par Client Security comme s'il s'agissait d'un virus.

Ce fichier (EICAR Standard Anti-Virus Test) est également détecté par d'autres programmes antivirus. Vous pouvez également utiliser ce fichier pour tester l'analyse de votre courrier électronique. EICAR signifie European Institute of Computer Anti-virus Research (Institut européen de recherche en matière d'antivirus informatiques). La page d'informations Eicar se trouve à l'adresse *http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml*.

Vous pouvez tester votre protection antivirus comme suit

1. Vous pouvez télécharger le fichier test `EICAR` à partir de l'adresse *http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml*.

   Vous pouvez également utiliser un éditeur de texte afin de créer le fichier. Il ne doit contenir que la ligne suivante :

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

2. Enregistrez ce fichier sous n'importe quel nom avec l'extension `.com` (par exemple `EICAR.COM`).

   Assurez-vous d'enregistrer le fichier au format ASCII MS-DOS standard. Notez également que le troisième caractère de l'extension est un O majuscule et non un 0 (zéro).

3. Vous pouvez maintenant utiliser ce fichier pour voir comment il se présente lorsque Client Security détecte un virus.

   Naturellement, ce fichier n'est pas un virus. Lorsqu'il est exécuté sans protection, `EICAR.COM` affiche le texte `EICAR-STANDARD-ANTIVIRUS-TEST-FILE!` et se ferme.

Chapitre

6

Configuration de la protection Internet

Sujets :

- *Niveaux de sécurité globale de pare-feu*
- *Elaboration des principes des niveaux de sécurité*
- *Configuration des niveaux et des règles de sécurité*
- *Configuration de la quarantaine réseau*
- *Configuration des alertes de règle*
- *Configuration du contrôle des applications*
- *Utilisation d'alertes pour vérifier le fonctionnement de la protection Internet*
- *Configuration de la prévention des intrusions*

La protection Internet protège les ordinateurs contre les accès non autorisés à partir d'Internet ainsi que contre les attaques provenant de l'intérieur du réseau.

La protection Internet offre une protection contre le vol d'informations, car elle permet d'empêcher et de détecter les tentatives d'accès non autorisées.Elle protège également les utilisateurs contre les applications malveillantes et offre une possibilité de contrôler l'utilisation du réseau et d'empêcher l'utilisation d'applications gourmandes en bande passante.

Le composant pare-feu intégré dans la protection Internet permet de restreindre le trafic en fonction des protocoles utilisés. La fonction Contrôle des applications est conçue pour empêcher les programmes malveillants d'envoyer des informations concernant l'ordinateur. Elle peut servir à restreindre davantage le trafic en fonction des applications, des adresses IP et des ports utilisés. Le système de détection des intrusions bloque les paquets malveillants visant ce type de port sur l'hôte.

La protection Internet contient sept niveaux de sécurité prédéfinis, avec chacun son jeu de règles de pare-feu préconfigurées. Différents niveaux de sécurité peuvent être affectés à différents utilisateurs selon, par exemple, la stratégie de sécurité de l'entreprise, la mobilité de l'utilisateur, l'emplacement et l'expérience de l'utilisateur.

Niveaux de sécurité globale de pare-feu

Si la personnalisation des paramètres du pare-feu n'est pas nécessaire pour votre réseau, vous pouvez choisir parmi plusieurs niveaux de sécurité pré-configurés.

Les niveaux de sécurité globale de pare-feu qui existent dans la protection Internet sont les suivants :

Quarantaine réseau	Si la quarantaine réseau est activée, ce niveau de sécurité est automatiquement sélectionné lorsque les critères de quarantaine réseau sur l'hôte sont remplis. Ce niveau de sécurité permet le téléchargement de mises à jour automatiques et des connexions à Policy Manager Server.
Bloquer tout	Ce niveau de sécurité bloque tout le trafic réseau.
Mobile	Ce niveau de sécurité permet une navigation normale sur le Web et le chargement de fichiers (HTTP, HTTPS, FTP), ainsi que le trafic de messagerie électronique et celui des groupes de discussion Usenet. Les programmes de cryptage, comme VPN et SSH, sont également admis. Tout autre trafic est interdit, et le trafic TCP entrant qui est bloqué entraîne la génération d'alertes. Des règles locales peuvent être ajoutées lorsqu'un antiprogramme provoque une détection.
Accueil	Ce niveau de sécurité accepte tout le trafic TCP entrant ainsi que le chargement de fichiers via FTP. Tout autre trafic est interdit, et le trafic TCP entrant qui est bloqué entraîne la génération d'alertes. Des règles locales peuvent être ajoutées pour autoriser d'autres fonctionnalités réseau.
Bureau	Ce niveau de sécurité accepte tout le trafic TCP entrant ainsi que le chargement de fichiers via FTP. Par défaut, tout autre trafic est bloqué, et seules les tentatives de connexion dangereuses entraînent la génération d'alertes.Des règles locales peuvent être ajoutées pour autoriser d'autres fonctionnalités réseau.
Strict	Ce niveau de sécurité permet la navigation sur le Web sortante, le trafic de messagerie électronique et celui des groupes de discussion, les transferts de fichiers FTP et les mises à jour distantes. Tout autre trafic est bloqué, et les accès entrants d'antiprogrammes et les tentatives de connexion TCP entraînent la génération d'alertes.
Normale	Ce niveau de sécurité permet tout le trafic sortant et refuse certains services entrants précis. Il est toujours possible d'ajouter des règles via la fonction de contrôle des applications, de manière à garantir le bon

	fonctionnement de la plupart des applications de réseau.
Désactivé	Ce niveau de sécurité autorise tout le trafic réseau, entrant et sortant, et n'entraîne la génération d'aucune alerte. La création de règles locales est impossible.

Elaboration des principes des niveaux de sécurité

Les principes de base de l'élaboration des niveaux de sécurité sont décrits ici.

Chaque niveau de sécurité possède un ensemble de règles de pare-feu préconfigurées. En outre, vous pouvez créer de nouvelles règles pour tous les niveaux de sécurité pour lesquels le **Mode de filtrage** ➤ **Normal** est affiché dans le tableau **Niveaux de sécurité du pare-feu**. Les règles de ce **tableau des niveaux de sécurité du pare-feu** se lisent de haut en bas.

Lorsque vous créez de nouveaux niveaux de sécurité, gardez à l'esprit le principe général suivant pour la définition des règles de pare-feu associées :

- N'autorisez que les services requis et refusez tous les autres. Par contre, vous devez reconfigurer le pare-feu lorsque de nouveaux services sont requis. Il s'agit malgré tout d'un inconvénient bien minime pour bénéficier d'une sécurité optimale.

Le concept opposé (refuser les services suspects et autoriser tous les autres) est inacceptable car personne ne peut dire avec certitude quels services sont malveillants ou peuvent le devenir ultérieurement lorsqu'un nouveau problème de sécurité est découvert.

Exemple de niveau de sécurité correct :

1. Règles de refus pour la plupart des services et hôtes malveillants avec alerte en option.
2. Règles d'autorisation pour les services et les hôtes standard les plus utilisés.
3. Règles de refus de services spécifiques pour lesquels vous souhaitez une alerte (par exemple tentatives d'accès d'un cheval de Troie) avec alerte.
4. Règles d'autorisation plus générales.
5. Refuser dans tous les autres cas.

Configuration des niveaux et des règles de sécurité

Cette section explique comment définir et sélectionner les niveaux de sécurité en fonction des besoins des utilisateurs.

Dans les exemples de configuration pratiques, on suppose que les hôtes gérés ont été importés dans une structure du domaine, où par exemple, les portables et ordinateurs de bureau se trouvent dans leur propre sous-domaine.

Lorsque vous activez un niveau de sécurité donné pour un domaine, vérifiez que le niveau de sécurité est approprié pour le domaine en question. Différents domaines peuvent avoir différents niveaux de sécurité.

Important: Lorsque vous changez un niveau de sécurité sur un hôte, cliquez sur le symbole cadenas en regard du paramètre pour vous assurer que le nouveau niveau de sécurité sera utilisé.

Sélection d'un niveau de sécurité actif pour un poste de travail

Dans cet exemple, le niveau de sécurité **Bureau** est défini comme niveau de sécurité actif pour les postes de travail dans le sous-domaine `Desktops/Eng.`.

Pour changer le niveau de sécurité de la protection Internet du sous-domaine `Desktops/Eng.`, procédez comme suit :

1. Sélectionnez le sous-domaine **Desktops/Eng.** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Niveaux de sécurité du pare-feu**.
   Le niveau de sécurité par défaut actuellement appliqué à la stratégie apparaît dans la liste déroulante **Niveau de sécurité de protection Internet sur l'hôte**.
3. Sélectionnez **Bureau** dans la liste déroulante **Niveau de sécurité de protection Internet sur l'hôte**.
4. Pour empêcher les utilisateurs de changer ces paramètres, cliquez sur le symbole cadenas correspondant.
5. Cliquez sur pour enregistrer et distribuer la stratégie.

Vous pouvez vérifier que le nouveau changement de niveau de sécurité est devenu effectif en accédant à l'onglet **Etat** et en sélectionnant la fenêtre **Protection globale**.

Remarque: Si le niveau de sécurité sélectionné ne peut pas être utilisé pour une raison quelconque, celui par défaut est utilisé à la place. Le niveau de sécurité par défaut actuel est indiqué dans la table **Niveaux de sécurité globale** de la page **Niveaux de sécurité du pare-feu**.

Configuration d'un niveau de sécurité par défaut pour les hôtes administrés

Le niveau de sécurité par défaut est un paramètre global et s'utilise uniquement si celui sélectionné par ailleurs est désactivé.

Dans cet exemple, le niveau de sécurité **Bureau** est configuré comme niveau par défaut pour tous les hôtes du domaine.

1. Sélectionnez le domaine **Laptops/Eng.** sur l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Niveaux de sécurité du pare-feu**.
3. Dans la table **Niveaux de sécurité du pare-feu**, activez la case d'option **Par défaut** sur la ligne **Bureau**.
   Policy Manager vous invite à confirmer le changement de niveau de sécurité pour tous les hôtes gérés.
4. Cliquez sur **OK**.
5. Cliquez sur pour enregistrer et distribuer la stratégie.

Ajout d'un nouveau niveau de sécurité pour un domaine particulier

Dans cet exemple, un nouveau niveau de sécurité est créé avec deux règles associées.

Le nouveau niveau de sécurité est ajouté pour un sous-domaine uniquement et les hôtes sont contraints à utiliser ce nouveau niveau. Le sous-domaine en question contient des ordinateurs utilisés uniquement pour la navigation sur Internet et qui ne sont pas connectés au réseau de l'entreprise.

Pour ajouter un nouveau niveau de sécurité à affecter à un domaine particulier, vous devez d'abord désactiver ce niveau de sécurité au niveau racine, puis le réactiver au niveau inférieur approprié.

Création d'un niveau de sécurité

La première étape pour ajouter un niveau de sécurité consiste à créer ce niveau de sécurité.

La procédure est la suivante :

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres**, puis sélectionnez la page **Niveaux de sécurité du pare-feu**.
3. Cliquez sur **Ajouter** pour ajouter un niveau de sécurité.
   La boîte de dialogue **Niveau de sécurité - Description** s'ouvre.
4. Entrez le nom à donner au nouveau niveau de sécurité, par exemple, `Navigation`.

   Vous pouvez également inclure une description dans la zone de texte **Description**.
5. Cliquez sur **Terminer**.
6. Cliquez sur pour enregistrer et distribuer la stratégie.

Création de règles pour le nouveau niveau de sécurité

La prochaine étape consiste à créer des règles pour le nouveau niveau de sécurité.

Les règles associées au nouveau niveau de sécurité sont créées comme suit :

1. Accédez à la page **Règles de pare-feu**.
2. Sélectionnez le niveau de sécurité de la protection Internet **Navigation**.

   La table **Règles de pare-feu** est vide lorsque ce niveau de sécurité est sélectionné, parce qu'il n'y a pas encore de règles associées.
3. Cliquez sur **Ajouter avant** pour ajouter en début de liste une règle autorisant le trafic HTTP sortant.
   La fenêtre de l'Assistant **Règles de pare-feu** s'ouvre.
4. Complétez l'assistant **Règles de pare-feu** :
   a) Sur la page **Type de règle**, sélectionnez **Autoriser**.
   b) Sur la page **Hôtes distants**, sélectionnez **Tout hôte distant** pour appliquer la règle à toutes les connexions Internet.
   c) Sur la page **Services**, sélectionnez **HTTP** dans la colonne **Service** pour appliquer la règle au trafic HTTP.
   d) Sur la page **Services**, sélectionnez **=>** dans la colonne **Direction** pour appliquer la règle aux connexions sortantes uniquement.
   e) Vous pouvez accepter les valeurs par défaut sur la page **Paramètres avancés**.
   f) Vérifiez la nouvelle règle sur la page **Résumé**.

      Vous pouvez également ajouter un commentaire décrivant la règle, par exemple, `Autorisation du trafic HTTP sortant pour la navigation.`.
   g) Cliquez sur **Terminer**.
5. Cliquez sur **Ajouter après** pour ajouter en fin de liste une règle interdisant tout autre trafic dans les deux sens.

6. Complétez l'Assistant **Règles de pare-feu** :
   a) Sur la page **Type de règle**, sélectionnez **Refuser**.
   b) Sur la page **Hôtes distants**, sélectionnez **Tout hôte distant** pour appliquer la règle à toutes les connexions.
   c) Sur la page **Services**, sélectionnez **Tout le trafic** dans la colonne **Service** pour appliquer la règle à tout le trafic.
   d) Sur la page **Services**, sélectionnez **Les deux** dans la colonne **Direction** pour appliquer la règle aux connexions entrantes et sortantes.
   e) Vous pouvez accepter les valeurs par défaut sur la page **Paramètres avancés**.
   f) Vérifiez la nouvelle règle sur la page **Résumé**.

      Vous pouvez également ajouter un commentaire décrivant la règle. Par exemple, `Refuser le reste`.

   g) Cliquez sur **Terminer**.

Mise en application du nouveau niveau de sécurité

La prochaine étape consiste à mettre en application le nouveau niveau de sécurité.

Pour mettre en application le nouveau niveau de sécurité dans le ou les sous-domaines sélectionnés uniquement, vous devez commencer par le désactiver au niveau de la racine avant de l'activer à un niveau inférieur de la hiérarchie des domaines de stratégie. La procédure est la suivante :

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à la page **Niveaux de sécurité du pare-feu**.
3. Désactivez le niveau de sécurité **Navigation** en désactivant la case **Activé** correspondante dans la table **Niveaux de sécurité du pare-feu**.
4. Sélectionnez le sous-domaine dans lequel utiliser ce niveau de sécurité dans l'onglet **Domaines de stratégie**.
5. Activez le niveau de sécurité **Navigation** en cochant la case **Activé** correspondante dans la case **Niveaux de sécurité du pare-feu**.
6. Sélectionnez le nouveau niveau de sécurité comme niveau de sécurité actif en le sélectionnant dans la liste déroulante **Niveau de sécurité de protection Internet sur l'hôte**.
7. Cliquez sur  pour enregistrer et distribuer la stratégie.

Configuration de la quarantaine réseau

La quarantaine réseau est une fonction de protection Internet permettant de restreindre l'accès au réseau des hôtes ayant d'anciennes définitions de virus et/ou pour lesquels l'analyse en temps réel est désactivée.

Les droits d'accès normaux de ces hôtes sont automatiquement rétablis après la mise à jour des définitions de virus et/ou dès que l'analyse en temps réel est réactivée.

Cette section décrit les paramètres de quarantaine réseau et contient un exemple indiquant comment activer la fonction quarantaine réseau dans le domaine géré. Une courte description précise également comment configurer le niveau de sécurité Quarantaine réseau en ajoutant de nouvelles règles de pare-feu.

Paramètres de quarantaine réseau

Les paramètres de quarantaine réseau se trouvent dans la page **Niveaux de sécurité du pare-feu**.

Dans la section **Quarantaine réseau**, vous pouvez :

- Activer ou désactiver la quarantaine réseau.
- Spécifier les définitions de virus qui activent la quarantaine réseau.
- Spécifier si la désactivation de l'analyse en temps réel sur un hôte active la quarantaine réseau.

Activation de la quarantaine réseau à l'échelle du domaine

Pour activer la quarantaine réseau dans l'ensemble du domaine, suivez les étapes ci-dessous.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Niveaux de sécurité du pare-feu**.
3. Sélectionnez **Activer la quarantaine réseau**.
4. Spécifiez les **définitions de virus qui activent la quarantaine réseau**.
5. Si vous souhaitez empêcher l'hôte d'accéder au réseau lorsque l'analyse en temps réel est désactivée, sélectionnez **Activer la quarantaine réseau sur l'hôte si l'analyse en temps réel est désactivée**.
6. Cliquez sur  pour enregistrer et distribuer la stratégie.

Réglage de la quarantaine réseau

La quarantaine réseau est mise en œuvre en forçant les hôtes au niveau de sécurité **Quarantaine réseau**, qui a un ensemble restreint de règles de pare-feu.

Vous pouvez ajouter de nouvelles règles **Autoriser** aux règles de pare-feu dans le niveau de sécurité **Quarantaine réseau** pour autoriser un accès réseau supplémentaire aux hôtes en quarantaine réseau. Vous ne devriez pas imposer des restrictions d'accès supplémentaires car des hôtes risqueraient ainsi de perdre la connectivité réseau.

Configuration des alertes de règle

Les alertes de règle de la protection Internet peuvent être utilisées pour obtenir des notifications si certains types d'antiprogrammes tentent d'accéder aux ordinateurs.

Il est possible d'émettre une alerte chaque fois qu'une règle est mise en action ou que des datagrammes interdits sont reçus, ce qui permet de visualiser plus facilement le type de trafic circulant sur le système.

Pour obtenir des alertes adéquates, le niveau de sécurité doit avoir la « granularité » appropriée, c'est-à-dire disposer d'une règle pour chaque type d'alerte souhaité. Concevoir des alertes à partir de règles élargies génère de nombreuses alertes, d'où le risque de perdre des informations stratégiques au milieu des nombreuses données sans importance.

Ajout d'une nouvelle règle avec alerte

Dans cet exemple, une règle **Refuser** avec alerte est créée pour le trafic ICMP sortant pour un sous-domaine particulier, de sorte qu'une alerte soit émise lorsqu'un utilisateur tente d'envoyer une commande ping à l'ordinateur.

A la fin de cet exemple, la règle est testée en envoyant une commande ping à l'un des ordinateurs du sous-domaine. Cet exemple décrit également les différentes sélections que vous pouvez effectuer lors de la création de nouvelles règles avec l'Assistant **Règles de pare-feu**.

Sélection du type de règle et du service refusé

La première étape consiste à sélectionner le type de règle et à définir le service refusé.

Pour cela :

1. Sélectionnez le sous-domaine pour lequel créer la règle dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Règles de pare-feu**.
3. Sélectionnez le niveau de sécurité de la protection Internet pour lequel ajouter la nouvelle règle dans le menu déroulant **Niveau de sécurité de protection Internet en cours de modification**.
   Toutes les règles définies pour ce niveau de sécurité de la protection Internet sont maintenant affichées dans la table.
4. Cliquez sur **Ajouter avant** pour ajouter la nouvelle règle en début de liste.
   L'Assistant **Règle de pare-feu** s'ouvre.
5. Sélectionnez **Refuser** pour refuser les connexions ICMP entrantes.
6. Spécifiez les hôtes affectés.

   Choisissez si cette règle s'applique à toutes les connexions ou uniquement aux connexions sélectionnées. Vous pouvez au choix :

   - Cocher la case **Tout hôte distant** pour appliquer la règle à toutes les connexions Internet.
   - Cocher la case **Tous les hôtes sur les réseaux connectés localement** pour appliquer la règle à toutes les connexions provenant du réseau local.
   - Cocher la case **Hôtes distants spécifiés** pour appliquer la règle à une adresse IP, une plage d'adresses IP ou des adresses DNS. Lorsque cette option est sélectionnée, vous pouvez spécifier les adresses dans la zone de texte située en dessous. Si vous souhaitez spécifier plusieurs adresses ou des plages d'adresses, séparez-les par des espaces.

   Pour cette règle, sélectionnez **Tout hôte distant**.
7. Sélectionnez le service refusé et la direction de la règle.

   Dans la liste des services disponibles, sélectionnez le service auquel cette règle s'appliquera. Si vous voulez que la règle s'applique à tous les services, sélectionnez **Tous** en haut de la liste. Vous pouvez sélectionner autant de services individuels que vous le souhaitez dans cette fenêtre.

Pour les services choisis, sélectionnez la direction dans laquelle s'applique la règle en cliquant sur la flèche dans la colonne **Direction**. Continuez à cliquer pour faire défiler les options disponibles. Pour obtenir des exemples, consultez le tableau ci-dessous.

Direction	Explication
<=>	Le service sera autorisé/refusé dans les deux directions, qu'il provienne de votre ordinateur ou qu'il s'y dirige.
<=	Le service sera autorisé/refusé s'il provient des hôtes distants ou réseaux définis en direction de votre ordinateur.
=>	Le service sera autorisé/refusé s'il provient de votre ordinateur en direction des hôtes distants ou réseaux définis.

Pour cette règle, sélectionnez :

- **ICMP** dans la liste déroulante **Service**
- **<=** dans la colonne **Direction**.

Définition des options avancées

La prochaine étape consiste à définir les options avancées de la règle.

Pour cela :

1. Précisez si la règle s'applique uniquement lorsqu'une liaison à distance est ouverte en activant ou en désactivant la case à cocher.
   a) Précisez si la règle s'applique uniquement lorsqu'une liaison à distance est ouverte en activant ou en désactivant la case à cocher.
   b) Sélectionnez le type d'alerte dans la liste déroulante **Envoyer une alerte**.
      Pour cette règle, sélectionnez **Alerte de sécurité**.
   c) Sélectionnez l'interruption d'alerte à envoyer dans la liste déroulante **Interruption d'alerte**.
   d) Entrez un commentaire décrivant l'alerte dans le champ **Commentaire d'alerte**.
   e) Vous pouvez accepter les valeurs par défaut pour le reste des champs de cette fenêtre.
2. Sélectionnez le type d'alerte dans la liste déroulante **Envoyer une alerte**.
3. Sélectionnez l'interruption d'alerte à envoyer dans la liste déroulante **Interruption d'alerte**.
   Pour cette règle, sélectionnez **Evénement réseau : service entrant refusé**.
4. Entrez un commentaire décrivant l'alerte dans le champ **Commentaire d'alerte**.
   Ce commentaire s'affiche dans l'interface utilisateur locale de Client Security.
5. Vous pouvez accepter les valeurs par défaut pour le reste des champs de cette fenêtre.
6. Vérifiez et acceptez la règle.

   Vous pouvez maintenant vérifier la règle. Vous pouvez également ajouter un commentaire décrivant la règle pour vous aider à comprendre la fonction de la règle lorsqu'elle est affichée dans la table **Règles de pare-feu**. Si vous devez apporter un changement quelconque à la règle, cliquez sur **Précédent** dans la règle.
7. Si vous êtes satisfait de la nouvelle règle, cliquez sur **Terminer**.
   La nouvelle règle est ajoutée en haut de la liste des règles actives sur la page **Règles de pare-feu**.

Configurer la transmission des alertes

La prochaine étape consiste à configurer la transmission des alertes pour la règle.

Pour cela :

1. Accédez à l'onglet **Paramètres** et sélectionnez la fenêtre **Envoi d'alertes**.
2. Dans la section **Transmission des alertes**, assurez-vous que les alertes de sécurité sont transmises à Policy Manager Console.
3. Au besoin, cochez la case **Alerte de sécurité** dans la colonne **Policy Manager Console**.

Appliquer et tester la nouvelle règle

La dernière étape consiste à appliquer et à tester la nouvelle règle.

Pour cela :

1. Assurez-vous que le sous-domaine correct est sélectionné dans l'onglet **Domaines de stratégie**.
2. Sélectionnez la page **Niveaux de sécurité du pare-feu** sur l'onglet **Paramètres**.
3. Définissez le niveau de sécurité pour lequel vous avez créé la règle comme niveau de sécurité actif en le sélectionnant dans la liste déroulante **Niveau de sécurité de protection Internet sur l'hôte**.
4. Cliquez sur  pour enregistrer et distribuer la stratégie.
5. Testez la règle que vous avez créé.

   Vous pouvez tester la règle que vous venez de créer en envoyant une commande ping à l'un des hôtes administrés dans le sous-domaine à partir d'un ordinateur situé en dehors de ce domaine. Cela fait, vous pouvez vérifier que la règle fonctionne comme suit :

   a) Sélectionnez le sous-domaine pour lequel vous avez créé la règle dans l'onglet **Domaines de stratégie**.
   b) Activez l'onglet **Résumé**, et vérifiez si de nouvelles alertes de sécurité sont affichées pour le domaine.
   c) Pour afficher les détails des alertes, cliquez sur **Afficher les alertes par gravité**.
   L'onglet **Alertes** s'affiche, présentant une liste détaillée des alertes de sécurité.

Configuration du contrôle des applications

Le contrôle des applications permet une navigation en toute sécurité et constitue une excellente défense contre les programmes malveillants.

Le contrôle d'application est également un excellent outil pour éradiquer les chevaux de Troie et autres antiprogrammes réseau étant donné qu'il ne leur permet pas de transmettre des informations sur le réseau.

Des règles de contrôle des applications peuvent être utilisées afin de définir des restrictions plus spécifiques quant au trafic sur le réseau, en plus des restrictions définies dans les règles de pare-feu. Les autorisations au niveau des applications ne peuvent pas servir à autoriser un trafic refusé par des règles de pare-feu statiques. Cependant, si vous avez autorisé certains trafics réseau dans les règles statiques, vous pouvez utiliser le contrôle des applications pour déterminer si une application peut être autorisée à tirer profit de ces règles ou non. En d'autres termes, vous pouvez créer une règle qui autorise le trafic et limiter l'utilisation de cette règle à l'aide du contrôle des applications.

Lorsque le contrôle des applications est centralisé, l'administrateur peut décider quels programmes accédant au réseau peuvent être utilisés sur les postes de travail. Il est ainsi possible d'empêcher l'utilisation de programmes qui vont à l'encontre de la stratégie de sécurité de l'entreprise et de surveiller les programmes que les utilisateurs finaux utilisent réellement.

Le principe fondamental lors de la configuration du contrôle des applications est d'autoriser les applications nécessaires et de refuser les autres.

Comment le contrôle des applications et DeepGuard fonctionnent ensemble ?

Lorsque le contrôle des applications détecte une tentative de connexion sortante et qu'il est configuré pour inviter l'utilisateur à choisir si la connexion est autorisée ou refusée, vous pouvez configurer le contrôle des applications pour qu'il vérifie à partir de DeepGuard si la connexion doit être autorisée. Ceci réduit le nombre de fenêtres indépendantes du contrôle des applications.

Exemple :

1. S'il y a une règle pour l'application qui tente d'ouvrir une connexion sortante dans le tableau **Règles d'application pour les applications connues**, le contrôle des applications autorise ou refuse la tentative de connexion en fonction de cette règle.
2. S'il n'y a pas de règle pour l'application dans le tableau **Règles d'application pour les applications connues**, le contrôle des applications autorise ou refuse la tentative de connexion en fonction de la liste **Action par défaut pour les applications clientes**.
3. Si l'action définie par défaut est **Inviter l'utilisateur à choisir** et que le paramètre **Ne pas inviter pour les applications identifiées par DeepGuard** est activé, le contrôle des applications vérifie à partir de DeepGuard que la connexion sortante est autorisée. Si DeepGuard identifie maintenant l'application, l'utilisateur final n'est pas invité à choisir et la connexion sortante est autorisée.
4. Si DeepGuard n'a pas identifié l'application, l'utilisateur est invité à choisir si la connexion est autorisée ou refusée.

Paramètres de contrôle des applications

Les paramètres disponibles sur la page **Paramètres** ➤ **Contrôle des applications** sont décrits dans cette section.

La page Contrôle des applications contient les informations suivantes :

Règles d'application pour les applications connues	
Application	Affiche le nom du fichier exécutable.

Règles d'application pour les applications connues	
Faire office de client (sortant)	Les actions possibles sont les suivantes : **Refuser**, **Autoriser**, **Décision utilisateur**.
Faire office de serveur (entrant)	Les actions possibles sont les suivantes : **Refuser**, **Autoriser**, **Décision utilisateur**.
Description	Affiche la description interne du programme exécutable, généralement le nom de l'application. Vous pouvez également modifier cette description.
Message	Affiche le message éventuellement associé à la règle lors de sa création.
Editeur	Affiche l'éditeur de l'application.
Version	Affiche la description interne relative à la version du programme exécutable.

Applications inconnues rapportées par les hôtes

Pour les applications inconnues, les informations affichées sont les mêmes que pour les applications connues, si ce n'est que les applications inconnues n'ont pas encore de règles définies ni de messages associés

Vous pouvez déterminer ce qui se passe lorsque l'application essaie de se connecter au réseau à l'aide des sélections **Action par défaut pour les applications clientes** et **Action par défaut pour les applications serveur**. Les actions possibles sont les suivantes :

Action	Description
Refuser	Refuse toutes les connexions de l'application au réseau.
Autoriser	Autorise toutes les connexions de l'application au réseau.
Décision utilisateur	L'utilisateur est invité à décider de ce qu'il doit faire chaque fois que l'application se connecte au réseau.

Si vous souhaitez laisser les utilisateurs finaux décider du choix à faire lors des invites de connexion sortante, vous pouvez réduire le nombre de fenêtres indépendantes qu'ils voient en sélectionnant **Ne pas inviter pour les applications que DeepGuard a identifiées**.

Le contrôle des applications ne restreint pas les plug-ins dans des navigateurs tels que Netscape ou Microsoft Internet Explorer. Tous les plug-ins ont les mêmes capacités que le navigateur lui-même. Cependant, conseillez aux utilisateurs finaux de n'installer que les plug-ins approuvés.

Première configuration du contrôle des applications

Lorsque vous configurez le contrôle des applications pour la première fois, utilisez un petit environnement de test pour créer la liste des applications autorisées, dans laquelle vous placez les applications standard utilisées dans l'entreprise.

La liste des applications autorisées est distribuée à l'ensemble du domaine géré dans le cadre d'une stratégie. La procédure est la suivante :

1. Créez une liste d'applications connues :
   a) Créez un environnement de test avec, par exemple, deux ordinateurs où tournent les programmes normalement utilisés dans votre entreprise.
   b) Importez ces hôtes dans le domaine géré de manière centralisée.
   c) Sélectionnez **Rapport** dans la liste déroulante **Envoyer des notifications pour les nouvelles applications**, de sorte que les nouvelles applications apparaissent dans la liste **Applications inconnues signalées par les hôtes**.
   d) Définissez les règles d'autorisation pour ces applications.
   e) Une fois que vous avez des règles pour toutes les applications nécessaires, ce jeu de règles peut être distribué comme stratégie à l'ensemble du domaine géré.
2. Configurez les paramètres de base qui seront utilisés lors de l'exécution du contrôle des applications :
   a) Dans la liste déroulante **Action par défaut pour les applications clientes**, sélectionnez l'action par défaut à exécuter lorsqu'une application inconnue tente d'établir une connexion sortante.
   b) Dans la liste déroulante **Action par défaut pour les applications serveur**, sélectionnez l'action par défaut à exécuter lorsqu'une application inconnue tente d'établir une connexion entrante.
   c) Spécifiez que les nouvelles applications doivent être signalées à l'administrateur en sélectionnant **Répertorier les nouvelles applications inconnues**.
   De cette manière, vous pouvez voir quels types d'applications les utilisateurs tentent de lancer et, au besoin, définir de nouvelles règles les concernant.
   d) Spécifiez si les messages par défaut sont affichés sur l'écran des utilisateurs lorsqu'une application inconnue tente d'établir une connexion entrante ou sortante en sélectionnant ou en désélectionnant la case **Afficher les messages par défaut pour les applications inconnues**.
3. Vérifiez et mettez en application les paramètres.
   Le contrôle des applications peut être activé pour l'ensemble du domaine comme suit :
   a) Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
   b) Sélectionnez la page **Niveaux de sécurité du pare-feu** dans l'onglet **Paramètres** et assurez-vous que l'option **Activer le contrôle des applications** est sélectionné.
   c) Cliquez sur pour enregistrer et distribuer la stratégie.

Création d'une règle pour une application inconnue au niveau racine

Dans cet exemple, vous allez créer une règle pour refuser l'utilisation d'Internet Explorer 4.

On suppose ici que cette application apparaît déjà dans la liste **Applications inconnues rapportées par les hôtes**.

1. Sélectionnez les applications sur lesquelles porte la règle :
   a) Accédez à l'onglet **Paramètres** et sélectionnez la page **Contrôle des applications**.
   b) Sélectionnez **Internet Explorer 4.01** dans la table **Applications inconnues rapportées par les hôtes**.
   c) Cliquez sur **Créer une ou plusieurs règles** pour lancer l'Assistant de règle de contrôle des applications.
2. Sélectionnez le type de règle d'application :
   a) Sélectionnez **Refuser** comme action à exécuter lorsque l'application fait office de client et tente d'établir une connexion sortante.
   b) Sélectionnez **Refuser** comme action à exécuter lorsque l'application fait office de serveur et tente d'établir une connexion entrante.
3. Sélectionnez le message affiché aux utilisateurs :
   a) Indiquez si un message est affiché aux utilisateurs en cas de tentative de connexion.
   Les options sont les suivantes : **Aucun message**, **Message par défaut** ou **Message personnalisé**.
   Si vous avez choisi d'afficher le **message par défaut**, vous pouvez vérifier les messages par défaut actuellement définis en cliquant sur **Définir des messages par défaut...**.

b) Si vous avez choisi **Message personnalisé**, la zone de texte du message personnalisé s'active et vous pouvez taper le message de votre choix.

Vous pouvez dans ce cas utiliser un message personnalisé tel que : `L'utilisation d'Internet Explorer 4 est interdite par la stratégie de sécurité de l'entreprise. Utilisez un autre navigateur à la place.`

4. Sélectionnez la cible de la règle :
   a) Sélectionnez le domaine ou l'hôte concerné par la règle parmi les domaines et hôtes affichés dans la fenêtre.

   Si l'hôte ou le domaine de destination a déjà une règle pour une des applications affectées par la nouvelle règle, vous êtes invité à confirmer si vous voulez continuer et écraser la règle existante pour cet hôte.

   Dans cet exemple, sélectionnez **Racine**.

   b) Lorsque la règle est prête, cliquez sur **Terminer**.
   La nouvelle règle s'affiche maintenant dans la table **Règles d'application pour les applications connues**. La table **Applications inconnues rapportées par les hôtes** a été actualisée.
5. Cliquez sur pour enregistrer et distribuer la stratégie.

Modification d'une règle de contrôle des applications existante

Dans cet exemple, la règle créée plus haut est modifiée pour permettre l'utilisation temporaire d'Internet Explorer 4 à des fins de test dans un sous-domaine appelé `Ingénierie/Test`.

1. Sélectionnez la règle à modifier :
   a) Accédez à l'onglet **Paramètres** et sélectionnez la page **Contrôle des applications**.
   b) Sélectionnez la règle à modifier dans la table **Règles d'application pour les applications connues**.
   c) Cliquez sur **Modifier** pour lancer l'Assistant Règles de contrôle des applications.
2. Modifiez le type de règle d'application :
   a) Sélectionnez l'action à exécuter lorsque l'application fait office de client et tente d'établir une connexion sortante.

   En l'occurrence, sélectionnez **Autoriser** pour **Faire office de client (sortant)**.

   b) Sélectionnez l'action à exécuter lorsque l'application fait office de serveur et tente d'établir une connexion entrante.
3. Sélectionnez le message affiché pour les utilisateurs.

   Indiquez si un message est affiché aux utilisateurs en cas de tentative de connexion.
4. Sélectionnez la nouvelle cible de la règle :
   a) Sélectionnez le domaine ou l'hôte sur lequel porte la règle.

   En l'occurrence, sélectionnez **Ingénierie/Test**.

   Si l'hôte ou le domaine de destination dispose déjà d'une règle pour une des applications affectées par la nouvelle règle, vous êtes invité à confirmer si vous voulez continuer et écraser la règle existante pour cet hôte.

   b) Lorsque la règle est prête, cliquez sur **Terminer**.
   La règle modifiée s'affiche maintenant dans la table **Règles d'application pour les applications connues**. Il s'agit d'une copie de la règle d'origine, avec les modifications que vous venez d'effectuer.
5. Cliquez sur pour enregistrer et distribuer la stratégie.

Désactivation des fenêtres contextuelles de contrôle des applications

Si vous souhaitez que le contrôle des applications soit entièrement transparent vis-à-vis des des utilisateurs finaux, vous devez désactiver toutes les fenêtres contextuelles.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez la page **Contrôle des applications**.

   Sur cette page, sélectionnez :

   - **Autoriser** dans la liste déroulante **Action par défaut pour les applications serveur**.
   - **Autoriser** dans la liste déroulante **Action par défaut pour les applications clientes**.
3. Lorsque vous créez des règles de contrôle des applications avec l'Assistant **Règles de contrôle des applications**, sélectionnez :

   - **Autoriser** ou **Refuser** comme action en cas de tentative de connexion entrante et sortante dans la boîte de dialogue **Type de règle d'application**.
   - **Aucun message** dans la boîte de dialogue **Message affiché pour les utilisateurs**.
4. Cliquez sur  pour enregistrer et distribuer la stratégie.

Utilisation d'alertes pour vérifier le fonctionnement de la protection Internet

Dans des conditions normales, vous ne devriez recevoir aucune alerte de la protection Internet ; si, brusquement, vous commencez à recevoir de nombreuses alertes, cela signifie qu'il y a soit une erreur de configuration, soit un problème.

Lorsque vous configurez les alertes, rappelez-vous que vous devriez avoir une règle par type d'alerte voulu. Concevoir des alertes à partir de règles élargies génère de nombreuses alertes, d'où le risque de perdre des informations stratégiques au milieu des nombreuses alertes sans importance.

Vous pouvez également créer des règles spéciales que vous pouvez utiliser pour tester le fonctionnement de la protection Internet. Cet exemple crée une règle autorisant l'utilisation de commandes ping. Si cette règle comprend une option d'alerte, elle peut être utilisée afin de tester le fonctionnement du système d'alerte.

1. Accédez à l'onglet **Paramètres** et sélectionnez la page **Règles de pare-feu**.
2. Sélectionnez le niveau de sécurité à utiliser à des fins de test.
3. Pour démarrer la création de la nouvelle règle, cliquez sur **Ajouter avant**.
   L'Assistant **Règles de pare-feu** démarre.
4. Sélectionnez **Autoriser** sur la page **Type de règle**.
5. Sélectionnez **Tout hôte distant** sur la page **Hôtes distants**.
6. Sur la page **Services**, sélectionnez **Ping** dans la liste déroulante **Service**, puis **Les deux** dans la liste déroulante **Directions**.
7. Sur la page **Options avancées**, sélectionnez les options suivantes :
   - **Alerte de sécurité** dans la liste déroulante **Envoyer une alerte**
   - **Evénement réseau : service potentiellement dangereux autorisé** dans la liste déroulante **Interruption d'alerte**
   - Vous pouvez aussi entrer un commentaire décrivant l'alerte dans le champ **Commentaire sur l'alerte**.
8. Sur la page **Résumé**, vous pouvez vérifier que la règle est correcte et entrer un commentaire décrivant la règle.
9. Cliquez sur pour enregistrer et distribuer la stratégie.
10. Vous pouvez maintenant tester la règle en envoyant une commande ping à l'un des hôtes gérés et en vérifiant qu'une alerte est créée et affichée dans l'onglet **Alertes**.

Configuration de la prévention des intrusions

La prévention des intrusions surveille le trafic entrant et tente de détecter d'éventuelles tentatives d'intrusion.

Le système de prévention des intrusions (IPS) peut aussi être utilisé pour surveiller les virus qui tentent de s'attaquer aux ordinateurs du réseau local. La prévention des intrusions analyse la charge (le contenu) et les données d'en-tête des paquets IP et les compare aux schémas d'attaque connus. Si les informations sont identiques ou similaires à l'un des schémas d'attaque connus, la prévention des intrusions crée une alerte et exécute l'action prévue lors de sa configuration.

Paramètres de la prévention des intrusions

Les paramètres de la prévention des intrusions se trouvent dans la section **Prévention des intrusions** de la page **Niveaux de sécurité du pare-feu**.

- **Activer la prévention des intrusions**

  Si cette option est activée, la prévention des intrusions est utilisée pour surveiller le trafic entrant et détecter d'éventuelles tentatives d'intrusion. Dans le cas contraire, la prévention des intrusions ne surveille pas le trafic.

- **Action en cas de paquet dangereux**

  Les options sont :

  - **Consigner et éliminer le paquet** : le paquet est consigné dans le journal d'alertes avec ses données d'en-tête (IP, ports et protocole) et n'est pas autorisé à passer par le composant de détection des intrusions.
  - **Consigner sans éliminer le paquet** : le paquet est consigné dans le journal d'alertes avec ses données d'en-tête (IP, ports et protocole), mais est autorisé à passer par le composant de prévention des intrusions.

- **Gravité de l'alerte**

  Les options sont : **Pas d'alerte**, **Informations**, **Avertissement**, **Alerte de sécurité**. Différentes gravités peuvent être associées aux tentatives d'intrusion selon la façon dont l'administrateur ou l'utilisateur local souhaite voir les messages.

- Sensibilité de la détection

  Ce paramètre a deux fonctions : il réduit le nombre d'alertes et a une incidence sur les performances de l'ordinateur local. En utilisant une petite valeur, vous réduisez le nombre de fausses alertes.

  - 10 = performances maximales du réseau, alertes minimales
  - 50 = seuls 50 % (les plus importants et les plus malveillants) des schémas IPS sont vérifiés et signalés en cas de correspondance.
  - 100 = tous les schémas préprogrammés sont vérifiés et signalés en cas de correspondance.
  - Plus le nombre est petit, moins il y a de schémas vérifiés.
  - La valeur recommandée pour les utilisateurs privés est 100
  - La valeur recommandée pour les ordinateurs de bureau est 25

Qu'est-ce qu'une fausse alerte ?

Une fausse alerte est une alerte qui indique à tort que l'événement correspondant s'est produit. Dans la protection Internet, le texte de l'alerte l'indique généralement avec des mots tels que « probable » ou « possible ». Les alertes de ce type devraient être éliminées ou minimisées.

Configuration d'IPS pour les ordinateurs de bureau et les portables

Dans cet exemple, l'IPS est activé pour tous les ordinateurs de bureau et portables dans deux sous-domaines.

On suppose que les ordinateurs de bureau et les portables sont placés dans leurs propres sous-domaines, `Desktops/Eng` et `Laptops/Eng`. On suppose que les ordinateurs de bureau sont également protégés par le pare-feu de l'entreprise, si bien que le niveau de performances d'alerte correspondant est moins élevé. Les portables sont régulièrement connectés à des réseaux qui ne peuvent pas être considérés comme sûrs, de sorte que le niveau de performances d'alerte sélectionné est plus élevé.

1. Configuration d'IPS pour les ordinateurs de bureau :
   a) Sélectionnez le sous-domaine **Desktops/Eng** dans l'onglet **Domaines de stratégie**.
   b) Accédez à l'onglet **Paramètres** et sélectionnez la page **Niveaux de sécurité du pare-feu**.
   c) Cochez la case **Activer la prévention des intrusions**.
   d) Sélectionnez **Consigner sans supprimer le paquet** dans la liste déroulante **Action en cas de paquet dangereux**.
   e) Sélectionnez **Avertissement** dans la liste déroulante **Gravité de l'alerte**.
   f) Sélectionnez **25%** dans la liste déroulante **Sensibilité de détection**.
2. Configuration d'IPS pour les portables :
   a) Sélectionnez le sous-domaine **Laptops/Eng** dans l'onglet **Domaines de stratégie**.
   b) Accédez à l'onglet **Paramètres** et sélectionnez la page **Niveaux de sécurité du pare-feu**.
   c) Cochez la case **Activer la prévention des intrusions**.
   d) Sélectionnez **Consigner sans supprimer le paquet** dans la liste déroulante **Action en cas de paquet dangereux**.
   e) Sélectionnez **Avertissement** dans la liste déroulante **Gravité de l'alerte**.
   f) Sélectionnez **100%** dans la liste déroulante **Niveau d'alerte et de performances**.
3. Cliquez sur  pour enregistrer et distribuer la stratégie.

Chapitre

7

Comment vérifier la protection de l'environnement réseau

Sujets :

- *Vérifier que tous les hôtes utilisent la dernière stratégie*
- *Vérifier que le serveur utilise les définitions de virus les plus récentes*
- *Vérifier que les hôtes ont les définitions de virus les plus récentes*
- *Vérifier qu'aucun hôte n'est déconnecté*
- *Affichage des rapports d'analyse*
- *Affichage des alertes*
- *Création d'un rapport d'infection hebdomadaire*
- *Surveillance d'une attaque réseau potentielle*

Dans le cadre des processus de surveillance et d'administration système, vous pouvez régulièrement effectuer les tâches répertoriées dans cette section pour vérifier la protection de votre environnement réseau.

Vérifier que tous les hôtes utilisent la dernière stratégie

Vous pouvez vous assurer que tous les hôtes possèdent les paramètres appropriés en vérifiant qu'ils utilisent bien la dernière stratégie.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Résumé** et vérifiez combien d'hôtes, sur l'ensemble du domaine, ont la stratégie la plus récente.
3. Si aucun hôte ne dispose de la stratégie la plus récente, cliquez sur **Afficher la dernière mise à jour de stratégie des hôtes**.
   L'onglet **Etat** et la page **Gestion centralisée** s'ouvrent.
4. Vérifiez les hôtes qui n'ont pas la stratégie la plus récente sur la page **Gestion centralisée**.

   Vous pouvez également prendre connaissance des raisons pouvant expliquer cette situation ; par exemple, l'hôte est déconnecté ou a subi une erreur fatale.

Vérifier que le serveur utilise les définitions de virus les plus récentes

Vous devez vérifier que les définitions de virus du serveur sont mises à jour.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Cliquez sur l'onglet **Résumé** et vérifiez que les définitions de virus du serveur sont les plus récentes.

Vérifier que les hôtes ont les définitions de virus les plus récentes

Vous devez régulièrement vérifier que les définitions de virus sont à jour sur tous les hôtes du domaine.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Cliquez sur l'onglet **Résumé** et vérifiez le contenu de la section **Protection antivirus pour postes de travail** en regard de **Définitions de virus**.
3. Si les définitions de virus de certains hôtes ne sont plus à jour, vous avez deux possibilités

   - Vous pouvez sélectionner l'onglet **Etat** et la page **Protection globale** pour voir les hôtes ne disposant pas des définitions de virus les plus récentes. Sélectionnez ensuite ces hôtes sous l'onglet **Domaines de stratégie**, cliquez sur l'onglet **Opérations**, puis sur **Mettre à jour les définitions de virus**. Cette commande enjoint aux hôtes sélectionnés d'aller chercher immédiatement de nouvelles définitions de virus.
   - Vous pouvez également cliquer sur le lien **Mettre à jour les définitions de virus**. L'onglet **Opérations** s'affiche. Une fois dans l'onglet **Opérations**, cliquez sur **Mettre à jour les définitions de virus**. Cette commande enjoint à tous les hôtes d'aller chercher immédiatement de nouvelles définitions de virus.

Vérifier qu’aucun hôte n'est déconnecté

Vous pouvez vous assurer que tous les hôtes disposent des mises à jour les plus récentes en vérifiant qu'aucun hôte n'est déconnecté.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Cliquez sur l'onglet **Résumé** et vérifiez le contenu de la section **Domaine** en regard de **Hôtes déconnectés**.
3. Si certains hôtes sont déconnectés, cliquez sur **Afficher les hôtes déconnectés...**.
   L'onglet **Etat** et la page **Gestion centralisée** s'ouvrent.
4. Vérifiez les hôtes qui sont déconnectés et les raisons pouvant expliquer cette situation.

Remarque: Vous pouvez définir la période au terme de laquelle un hôte est considéré comme déconnecté. Sélectionnez **Outils** ➤ **Préférences** dans le menu, puis cliquez sur l'onglet **Communications** dans la fenêtre **Préférences**. Vous verrez la durée définie dans la section **Connexion de l'hôte**.

Affichage des rapports d'analyse

Vous pouvez afficher les rapports d'analyse à partir des hôtes pour vérifier si des problèmes se sont produits.

Si vous souhaitez voir le rapport d'analyse de certains hôtes, procédez comme suit

1. Sélectionnez les hôtes dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Rapports**.
   Les données d'analyse des hôtes sélectionnés s'affichent dans le tableau **Rapports**.
3. Sélectionnez un hôte en cliquant sur une ligne de la table.
   Le rapport d'analyse correspondant de cet hôte s'affiche maintenant dans la vue du rapport, dans la partie inférieure de la fenêtre.

Affichage des alertes

Les hôtes peuvent émettre des alertes et des rapports en cas de problème avec un programme ou une opération.

Il est bon de vérifier régulièrement qu'il n'y a pas de nouvelles alertes et d'accuser réception (et supprimer) les alertes que vous avez déjà gérée.

Lorsqu'une alerte est reçue, le bouton s'allumera. Pour afficher les alertes :

1. Cliquez sur .
   Vous pouvez également cliquer sur **Afficher le résumé des alertes....** sous l'onglet **Résumé**.
   L'onglet **Alertes** s'ouvrira. Toutes les alertes reçues s'affichent au format suivant :

Accep.	Cliquez sur le bouton **Accep.** pour accuser réception d'une alerte. Si vous avez accusé réception de toutes les alertes, le bouton **Accep.** sera grisé.		
Gravité	Gravité du problème. Une icône est associée à chaque niveau de gravité :		
		Info	Informations de fonctionnement normal émises par un hôte.
		Avertissement	Avertissement émanant de l'hôte.
		Erreur	Erreur non fatale survenue sur l'hôte.
		Erreur fatale	Erreur fatale survenue sur l'hôte.
		Alerte de sécurité	Incident lié à la sécurité survenu sur l'hôte.
Date/Heure	Date et heure de l'alerte.		
Description	Description du problème.		
Hôte/Utilisateur	Nom de l'hôte/utilisateur.		
Produit	Le produit F-Secure qui a envoyé l'alerte.		

   Lorsque vous sélectionnez une alerte dans la liste, le volet **Affichage de l'alerte**, sous la table des alertes, affiche des informations détaillées sur celle-ci.
2. Vous pouvez utiliser le bouton **Accep.** pour marquer les alertes que vous avez vues et que vous prévoyez de résoudre.
3. Le résumé des alertes affiché sous l'onglet **Résumé** n'est pas automatiquement actualisé ; vous pouvez cliquer sur **Actualiser le résumé des alertes** pour actualiser l'affichage des alertes.

Création d’un rapport d’infection hebdomadaire

Lorsque vous souhaitez créer un rapport d'infection hebdomadaire (ou tout autre rapport généré à intervalles réguliers), deux outils s'offrent à vous.

- Web Reporting, un outil Web avec lequel vous pouvez générer un large éventail de rapports graphiques à partir des alertes et des informations d'état associées à Client Security.

Surveillance d’une attaque réseau potentielle

Si vous soupçonnez qu'une attaque réseau est en cours sur le réseau local, vous pouvez surveiller la situation en suivant les étapes ci-dessous.

1. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
2. Cliquez sur l'onglet **Résumé**.
3. Vérifiez ce qui est affiché en regard de **Dernière attaque la plus courante**.
4. En cas d'attaque, vous pouvez accéder à des informations plus détaillées en cliquant sur **Afficher l'état de protection Internet...**.
   L'onglet **Etat** et la page **Protection Internet** s'affichent, montrant des informations détaillées sur les attaques récentes sur les différents hôtes.

Chapitre

8

Mise à jour du logiciel

Sujets :

- *Utilisation de l'éditeur d'installation*

Vous pouvez effectuer une mise à jour à distance du logiciel F-Secure déjà installé sur les hôtes à l'aide de l'**éditeur d'installation**. Cet éditeur crée des tâches d'installation basées sur la stratégie que chaque hôte du domaine exécutera après la prochaine mise à jour de la stratégie.

Remarque: Il est également possible de mettre à niveau Client Security en utilisant toute autre procédure d'installation .

Utilisation de l'éditeur d'installation

L'éditeur d'installation doit être utilisé sur les hôtes équipés de Management Agent.

Pour utiliser l'éditeur d'installation :

1. Ouvrez l'onglet **Stratégie** et sélectionnez le nœud racine (l'arborescence secondaire **F-Secure**).
   Vous pouvez également ouvrir l'onglet **Installer**.
   L'**Editeur d'installation** s'affiche.
2. Dans l'**Editeur d'installation**, sélectionnez les produits à installer sur l'hôte ou le domaine de stratégie actuellement sélectionné.
   L'**Editeur d'installation** contient les informations suivantes relatives aux produits installés sur l'hôte ou un domaine de stratégie de destination :

Nom de produit	Nom du produit déjà installé sur un hôte ou un domaine ou qui peut être installé à l'aide d'un package d'installation disponible.
Version installée	Numéro de version du produit. Si plusieurs versions du produit sont installées, tous les numéros de version correspondants s'affichent. Pour les hôtes, il s'agit toujours d'un numéro de version unique.
Version à installer	Numéros de version des packages d'installation disponibles pour le produit.
Version actuelle	Version actuelle, en cours d'installation sur un hôte ou un domaine.
En cours	Progression de l'installation. Le champ **En cours** affiche des informations différentes pour les hôtes et pour les domaines.

- Lorsqu'un hôte est sélectionné, le champ **En cours** affiche l'un des messages suivants :

En cours	L'installation a démarré (et a été ajoutée aux données de stratégie), mais l'hôte n'a pas encore signalé le succès ou l'échec de l'opération.
Échec	L'installation ou la désinstallation a échoué. Cliquez sur le bouton du champ **En cours** pour afficher des informations d'état détaillées.
Terminé	L'installation ou la désinstallation est achevée. Ce message disparaît lorsque vous fermez l'**Editeur d'installation**.
(Zone vide)	Aucune opération n'est en cours. Le champ **Version installée** affiche le numéro de version des produits actuellement installés.

- Lorsqu'un domaine est sélectionné, la zone **En cours** contient l'une des informations suivantes :

<nombre> hôtes restants - <nombre> installations ayant échoué	Nombre d'hôtes restants et nombre d'installations qui ont échoué. Cliquez sur le bouton de la zone **En cours** pour afficher des informations d'état détaillées.
Terminé	L'installation ou la désinstallation est achevée sur tous les hôtes.

(Zone vide)	Aucune opération n'est en cours. La **version installée** affiche le numéro de version des produits actuellement installés.

3. Lorsque tous les numéros de version requis sont sélectionnés, cliquez sur **Démarrer**. L'**Editeur d'installation** lance l'**Assistant d'installation**, qui invite l'utilisateur à configurer les paramètres de l'installation. L'**Editeur d'installation** prépare ensuite un package personnalisé de distribution de l'installation pour chaque opération d'installation. Ce package est sauvegardé sur Policy Manager Server.

   👉 **Remarque:** Le bouton **Démarrer** permet à l'administrateur de démarrer les opérations d'installation sélectionnées dans la zone **Version à installer**. Si vous fermez l'**Editeur d'installation** sans cliquer sur le bouton **Démarrer**, toutes les modifications sont annulées.

4. L'installation étant déclenchée par une stratégie, vous devez distribuer les nouveaux fichiers de stratégie.

   Le fichier de stratégie contient une entrée qui invite l'hôte à rechercher le package d'installation et à démarrer l'installation.

   Notez qu'une installation peut prendre énormément de temps, notamment lorsqu'un hôte concerné n'est pas connecté au réseau lors de l'installation ou si l'opération activée requiert que l'utilisateur redémarre son poste de travail avant que l'installation soit terminée. Si les hôtes sont connectés au réseau et qu'ils n'envoient ou ne reçoivent pas correctement les fichiers de stratégie, cela signifie qu'il peut y avoir un problème important. Il est possible que l'hôte ne confirme pas correctement la réception de l'installation. Dans tous les cas, vous pouvez supprimer l'opération d'installation de la stratégie en cliquant sur le bouton **Tout arrêter**. Toutes les opérations d'installation définies pour le domaine de stratégie ou l'hôte sélectionné seront alors annulées. Vous pouvez arrêter toutes les tâches d'installation dans le domaine sélectionné et tous ses sous-domaines en choisissant l'option **Annuler de façon récurrente les installations pour les sous-domaines et les hôte** dans la boîte de dialogue de confirmation.

   Le bouton **Tout arrêter** est activé uniquement si une opération d'installation est définie pour l'hôte ou le domaine actuel. Les opérations définies pour les sous-domaines ne modifient pas son état. **Tout arrêter** supprime uniquement l'opération de la stratégie. Si un hôte a déjà récupéré le fichier de stratégie précédent, il est possible qu'il tente d'exécuter l'installation même si elle n'est plus visible dans l'**Editeur d'installation**.

Désinstallation à distance :

La désinstallation d'un produit peut s'exécuter aussi facilement qu'une mise à jour. Le système crée un fichier de diffusion contenant uniquement le logiciel nécessaire à la désinstallation du produit. Si ce dernier ne prend pas en charge la désinstallation à distance, l'**Editeur d'installation** n'affiche aucune option de désinstallation.

Si vous sélectionnez **Réinstaller**, la version actuelle sera à nouveau installée. Utilisez cette option uniquement pour résoudre certains problèmes. En règle générale, il n'est pas nécessaire de réinstaller un produit.

Lors de la désinstallation de Management Agent, aucune information statistique indiquant que la désinstallation a réussi n'est envoyée car Management Agent a été supprimé et ne peut pas envoyer d'informations. Si vous désinstallez par exemple F-Secure Anti-Virus et Management Agent :

1. Désinstaller F-Secure Anti-Virus
2. Attendez que Policy Manager Console signale le succès ou l'échec de la désinstallation.
3. Si F-Secure Anti-Virus a été désinstallé correctement, désinstallez Management Agent.
4. Si la désinstallation de Management Agent a échoué, Policy Manager Console affiche un rapport statistique de l'échec. La réussite ne peut pas être signalée, mais elle se remarque à la coupure des communications, le rapport final de Management Agent contenant la mention « `en cours` »..

Chapitre
9

Opérations sur les hôtes locaux

Sujets :

- *Analyse manuelle*
- *Analyse à heures fixes*
- *Où trouver des alertes de pare-feu et des fichiers journal ?*
- *Connexion à Policy Manager et importation manuelle d'un fichier de stratégie*
- *Suspension des téléchargements et mises à jour*
- *Autoriser les utilisateurs à décharger les produits F-Secure*

Ces opérations sont utiles lorsque vous soupçonnez la présence d'un virus sur un hôte local ou devez effectuer localement certaines tâches administratives.

Analyse manuelle

Vous pouvez analyser votre ordinateur manuellement si vous suspectez la présence d'un *programme malveillant* sur votre ordinateur.

Comment sélectionner le type d'analyse manuelle

Vous pouvez analyser l'ordinateur entier ou un type spécifique de *programme malveillant* ou un emplacement spécifique.

Si vous suspectez un certain type de *programme malveillant* , vous pouvez n'analyser que ce type. Si vous suspectez un emplacement donné de l'ordinateur, vous pouvez n'analyser que cet emplacement. Ces analyses seront plus rapides qu'une analyse complète de l'ordinateur.

Pour lancer manuellement l'analyse de votre ordinateur :

1. Sur la page principale, cliquez sur la flèche située sous **Analyse**.
   Les options d'analyse s'affichent.
2. Accédez à **Protection du serveur** ➤ **Analyse manuelle**.
3. Sélectionnez le type d'analyse.
   Pour changer les paramètres d'analyse, sélectionnez **Modifier les paramètres de l'analyse...**.
4. Sous **Nouvelle analyse**, sélectionnez le type d'analyse.
   Pour modifier les paramètres de l'analyse, cliquez sur l'onglet **Paramètres**.
5. Si vous avez choisi **Sélectionner les éléments à analyser**, vous pouvez indiquer l'emplacement à analyser dans la fenêtre qui s'ouvre.
   L' **Assistant d'analyse** s'ouvre.
6. Si vous avez choisi **Sélectionner les éléments à analyser**, cliquez sur **Sélectionner...**.
   Une fenêtre s'ouvre. Vous pouvez alors sélectionner l'emplacement à analyser.
7. Pour lancer l'analyser, cliquez sur **Démarrer**.
   Lorsqu'aucun programme malveillant n'est détecté, la ligne État de la partie supérieure de la page affichera "Terminé". Autrement, l'assistant d'analyse s'ouvre.

👉 **Remarque:** Vous pouvez également lancer l'analyse du serveur manuellement, en cliquant avec le bouton droit de votre souris sur l'icône du produit dans la barre système.

Types d'analyses

Vous pouvez analyser l'ordinateur entier ou un type spécifique de programme malveillant ou un emplacement spécifique.

Voici les différents types d'analyses :

Type d'analyse	Sur quoi porte l'analyse ?	Quand utiliser ce type ?
Analyse complète de l'ordinateur	Recherche de virus, de logiciels espions et de riskware dans l'intégralité de votre ordinateur (disques durs internes et externes)	Lorsque vous voulez être sûr qu'il n'y a aucun programme malveillant ou programme à risque sur votre ordinateur.Ce type d'analyse est celui qui prend le plus de temps. Il associe la détection rapide des programmes malveillants et l'analyse du disque dur. Il recherche également les éléments susceptibles d'être dissimulés derrière un rootkit.

Type d'analyse	Sur quoi porte l'analyse ?	Quand utiliser ce type ?
Sélectionner les éléments à analyser	Analyser un fichier, dossier ou lecteur particulier pour détecter la présence éventuelle de virus, logiciels espions et riskware	Vous suspectez la présence d'un programme malveillant à un emplacement précis de votre ordinateur, tel que le dossier contenant des téléchargements provenant de sources potentiellement dangereuses (par exemple les réseaux peer-to-peer de partage de fichiers). La durée de l'analyse dépend de la taille de la cible à analyser. L'analyse se fait rapidement si vous analysez un dossier contenant uniquement quelques petits fichiers.
Analyser les disques durs	Tous les disques durs internes de votre ordinateur sont analysés pour détecter les virus, logiciels espions et riskware.	Ce type d'analyse s'étend à tous les disques durs de l'ordinateur. A la différence de la détection des programmes malveillants, ce type d'analyse ne s'arrête pas uniquement sur les parties du système hébergeant des fichiers programmes, mais vérifie aussi tous les fichiers de données, tels que les documents, la musique, les images et les clips vidéo. Ce type d'analyse est lent et uniquement recommandé si l'analyse rapide des programmes malveillants n'a détecté aucun programme malveillant et si vous voulez vous assurer que les autres parties de votre ordinateur ne contiennent pas de fichiers malveillants.
Analyser les disques durs	Tous les disques durs internes de votre ordinateur sont analysés pour détecter les virus, logiciels espions et riskware.	Ce type d'analyse s'étend à tous les disques durs de l'ordinateur. A la différence de la détection des programmes malveillants, ce type d'analyse ne s'arrête pas uniquement sur les parties du système hébergeant des fichiers programmes, mais vérifie aussi tous les fichiers de données, tels que les documents, la musique, les images et les clips vidéo. Ce type d'analyse est lent et uniquement recommandé si l'analyse rapide des programmes malveillants n'a détecté aucun programme malveillant et si vous voulez vous assurer que les autres parties de votre ordinateur ne contiennent pas de fichiers malveillants.
Recherche de virus et logiciels espions	Certaines parties de votre ordinateur sont analysées pour détecter la présence éventuelle de virus, logiciels espion et riskware.	Ce type d'analyse est beaucoup plus rapide qu'une analyse complète. Il ne recherche que les parties de votre système contenant des fichiers programmes installés. Ce type d'analyse est recommandé si vous souhaitez vérifier rapidement que votre ordinateur est propre, car il permet de rechercher et de supprimer efficacement tout programme malveillant installé sur votre ordinateur.
Analyse du rootkit	Emplacements système importants où un élément suspect peut entraîner un problème de sécurité. Analyse les fichiers, dossiers, lecteurs et processus cachés.	Lorsque vous soupçonnez la présence d'un rootkit sur votre ordinateur. Par exemple, si un programme a été récemment détecté sur votre ordinateur et vous souhaitez vous assurer qu'il n'a pas installé de rootkit.

Nettoyer automatiquement les programmes malveillants

Lorsqu'un *programme malveillant* est détecté lors de l'analyse, vous pouvez laisser le programme décider automatiquement de la méthode de nettoyage de votre ordinateur, ou vous pouvez décider vous-même pour chaque élément.

1. Sélectionnez l'une des options :

Option	Action effectuée
Gérer automatiquement (recommandé)	Le programme choisit l'action pour chaque *programme malveillant* afin de nettoyer automatiquement votre ordinateur.
Je veux décider élément par élément	Le programme vous demande ce qu'il faut faire pour chaque élément de *programme malveillant*.

2. Cliquez sur **Suivant**.
   - Si vous avez sélectionné **Agir automatiquement (recommandé)**, une fenêtre s'ouvre avec les résultats des traitements automatiques des programmes malveillants.

     Remarque: Certains éléments d'un programme malveillant peuvent se voir attribuer l'état "Non traité", ce qui signifie que le fichier se trouve dans une archive (un fichier zip, par exemple) et ne peut donc pas être traité automatiquement. Vous pouvez supprimer le fichier infecté en ouvrant l'archive et supprimant le fichier manuellement. Si le contenu du fichier n'est pas important, vous pouvez supprimer l'archive entière.
   - Si vous avez sélectionné **Je veux décider élément par élément**, vous devez spécifier l'action pour chaque programme malveillant détecté.
3. Cliquez sur **Terminer** pour fermer l'Assistant d'analyse.

Afficher les résultats de l'analyse manuelle

Une fois l'analyse terminée, vous pouvez afficher un rapport présentant les résultats de l'analyse.

Remarque: Vous pouvez décider d'afficher ce rapport, car l'action sélectionnée n'est pas toujours celle exécutée. Par exemple, si vous avez choisi de nettoyer un fichier infecté mais que le *virus* n'a pas pu être supprimé du fichier, le produit peut avoir effectué une autre action sur le fichier.

Pour afficher le rapport :

1. Cliquez sur **Afficher le rapport**.

   Le rapport inclut :
   - Le nombre de *programmes malveillants* trouvés.
   - Le type de *programme malveillant* trouvé et des liens vers des descriptions du *programme malveillant* sur Internet.
   - Les actions appliquées à chaque *programme malveillant*.
   - Tous les éléments qui ont été exclus de l'analyse.
   - Les moteurs d'analyse qui ont été utilisés pour le *programme malveillant*.

   Remarque: Le nombre de fichiers analysés peut différer si les fichiers ont été analysés à l'intérieur des archives lors de l'analyse. Si des fichiers archivés ont été analysés auparavant, les résultats de l'analyse peuvent être sauvegardés dans la mémoire cache.
2. Cliquez sur **Terminer** pour fermer l'**Assistant d'analyse**.
3. Accédez à **Protection du serveur** ➤ **Analyse manuelle**, puis ouvrez l'onglet État.
4. Sous **Tâches**, cliquez sur **Afficher le rapport d'analyse...**.

   Remarque: En mode Administration centralisée, le rapport d'analyse est envoyé à F-Secure Policy Manager. Vous pouvez également le consulter dans F-Secure Policy Manager Console.

Astuce: Vous pouvez afficher les résultats de votre dernière analyse en cliquant sur **Paramètres** ➤ **Ordinateur** ➤ **Analyse manuelle**. Cliquez sur **Afficher le dernier rapport d'analyse**.

Analyse à heures fixes

Vous pouvez analyser votre ordinateur pour y détecter les *programmes malveillants* à intervalles réguliers, par exemple tous les jours, toutes les semaines ou tous les mois.

La recherche de *programme malveillant* est un processus intensif. Il requiert toute la puissance de votre ordinateur et demande beaucoup de temps. C'est pourquoi il est conseillé de configurer le programme pour qu'il analyse l'ordinateur lorsque vous ne l'utilisez pas.

Planifier une analyse

Configurez le programme afin d'analyser votre ordinateur à intervalles réguliers.

Pour planifier une analyse :

1. Sur la page principale, cliquez sur **Paramètres**.
2. Sélectionnez **Système** ➤ **Analyse planifiée**.
3. Accédez à **Protection du serveur** ➤ **Analyse planifiée**.
4. Sélectionnez **Activer l'analyse planifiée**.
5. Sélectionnez les jours souhaités pour rechercher régulièrement des *virus* et *logiciels espions* .

Option	Description
Tous les jours	Pour analyser tous les jours.
Toutes les semaines	Pour analyser les jours sélectionnés de la semaine. Sélectionnez les jours de l'analyse dans la liste à droite.
Tous les mois	Pour analyser jusqu'à trois jours par mois. Pour sélectionner les jours : 1. Sélectionnez parmi les options **Jour**. 2. Sélectionnez le jour du mois dans la liste en regard du jour sélectionné. 3. Répétez pour analyser un autre jour.

6. Sélectionnez le moment souhaité pour démarrer l'analyse les jours sélectionnés.

Option	Description
Heure début	Heure de début de l'analyse. Vous devez sélectionnez une heure pendant laquelle vous n'utiliserez pas l'ordinateur.
Si l'ordinateur est inutilisé pendant	Sélectionnez une période d'inactivité au bout de laquelle l'analyse démarre lorsque vous n'utilisez pas votre ordinateur.

7. Cliquez sur **Appliquer**.

Annuler une analyse planifiée

Lorsqu'une analyse planifiée démarre à un moment qui ne vous convient pas, vous pouvez l'annuler en local. L'analyse planifiée sera de nouveau exécutée à l'heure définie.

Remarque: Vous ne pouvez pas annuler une analyse planifiée depuis la console Web.

Une analyse planifiée peut avoir un effet sur la performance de votre ordinateur. Pour annuler l'analyse planifiée :

Remarque: En mode Administration centralisée, vous ne pourrez probablement pas annuler les analyses planifiées.

1. Cliquez sur le lien**L'analyse planifiée a commencé**dans le panneau**Recherche de virus et de logiciels espions**.

   Le panneau reste affiché pendant environ 15 secondes, puis disparaît.Si vous ne cliquez pas sur le lien du panneau, vous ne pourrez plus annuler l'analyse planifiée.
2. Cliquez sur **Annuler** dans la fenêtre **Recherche de virus et de logiciels espions.**.
3. Cliquez sur **Fermer**.

L'analyse planifiée est annulée. La prochaine analyse planifiée démarrera normalement.

Afficher les résultats de l'analyse planifiée

A la fin d'une analyse planifiée, vous pouvez vérifier si un *programme malveillant* a été détecté.

Pour vérifier les résultats d'une analyse planifiée :

1. Cliquez sur **L'analyse planifiée est terminée** dans le panneau **Recherche de virus et de logiciels espions**.
2. Cliquez sur **Afficher le rapport** pour connaître les résultats de l'analyse.

   👉 **Remarque:** Si vous avez ouvert la boîte de dialogue depuis la boîte de dialogue **Historique du panneau**, le bouton **Afficher le rapport** est désactivé. Vous ne pouvez pas afficher les résultats d'anciennes analyses planifiées.
3. Cliquez sur **Fermer** pour fermer la boîte de dialogue.

👉 **Astuce:** Vous pouvez également afficher les résultats de la dernière analyse en cliquant sur **Paramètres** ➤ **Ordinateur** ➤ **Analyse planifiée**. Cliquez sur **Afficher le dernier rapport d'analyse**.

👉 **Astuce:** ➤ Vous pouvez également afficher les résultats de la dernière analyse en cliquant sur ParamètresOrdinateurAnalyse planifiée. Cliquez sur Afficher le dernier rapport d'analyse.

👉 **Remarque:** En mode Administration centralisée, le rapport d'analyse est envoyé à F-Secure Policy Manager. Vous pouvez également le consulter dans F-Secure Policy Manager Console.

Où trouver des alertes de pare-feu et des fichiers journal ?

La consultation des alertes de pare-feu et des fichiers journal permet de vérifier le niveau de protection des connexions réseau sur votre ordinateur.

Afficher les alertes du pare-feu

Vous pouvez afficher une liste de toutes les alertes de pare-feu générées .

La liste contient des alertes générées par le pare-feu et la prévention contre les intrusions.

Pour afficher la liste :

1. Sur la page principale, cliquez sur **Paramètres**.
2. Sélectionnez **Connexions réseau** ➤ **Pare-feu**.
3. Cliquez sur l'onglet **Règles**.
4. Cliquez sur **Afficher le journal des alertes**.
   La boîte de dialogue **Alertes du pare-feu** s'ouvre et affiche les informations suivantes :

Champ	Description
Heure	Heure de l'alerte.
Adresse distante	*Adresse IP* de l'ordinateu duquel vous recevez du trafic ou auquel vous envoyez du trafic.
Occurrences	Indique le nombre de génération d'une alerte similaire.
Description	Texte d'alerte qui a été ajouté à la *règle de pare-feu*. Si une tentative d'intrusion a généré l'alerte, le champ indique des informations sur le *modèle* de tentative d'intrusion.

5. Pour afficher les détails d'une alerte, sélectionnez l'alerte et cliquez sur **Détails**.
6. Pour passer à l'alerte précédente ou suivante, cliquez sur **Préc** ou sur **Suivant**.
7. Une fois les détails consultés, cliquez sur **Fermer** pour fermer la boîte de dialogue de détails des **Alertes du pare-feu**.
8. Cliquez sur **Fermer** pour fermer la boîte de dialogue de la liste d'**Alertes du pare-feu**.

Informations d'alertes de pare-feu

Une alerte de pare-feu contient des informations sur le trafic ayant provoqué l'alerte.

Une alerte de pare-feu contient les informations suivantes :

Champ	Description
Description	Le texte d'alerte ajouté pour la *règle de pare-feu*. Si l'alerte est due à une tentative d'intrusion, l'alerte donne des informations sur le *modèle* de tentative d'intrusion.
Action	Indique ce qu'il s'est produit, que le *pare-feu* a bloqué ou autorisé le trafic par exemple.
Heure	Date et heure de génération de l'alerte.
Direction	Indique si le trafic est entrant ou sortant (d'un ordinateur distant sur votre ordinateur ou vice-versa).

Champ	Description
Protocole	Le *protocole IP* utilisé.
Services	Indique les *services de pare-feu* correspondant à ce trafic.
Adresse distante	L'*adresse IP* de l'ordinateur distant.
Port distant	Le *port* sur l'ordinateur distant.
Adresse locale	L'*adresse IP* de votre ordinateur.
Port local	Le *port* sur votre ordinateur.

Afficher le *journal des actions*

Si un programme, comme un jeu en réseau, ne fonctionne pas, vous pouvez vérifier dans le journal des actions si le contrôle d'application a refusé la connexion de ce programme à Internet.

Le *journal des actions* est un fichier texte (`action.log`) qui collecte automatiquement les informations relatives aux connexions réseau. Les entrées de journal les plus anciennes sont supprimées lorsque le fichier arrive à saturation.

Pour afficher le *journal des actions* :

1. Sur la page principale, cliquez sur **Paramètres**.
2. Sélectionnez **Connexion réseau** ➤ **Consignation**.
3. Cliquez sur **Afficher le journal des actions**.

Le *journal des actions* s'ouvre dans un éditeur de texte ou un visualiseur par défaut, Notepad par exemple.

Gestion du trafic réseau à l'aide de la consignation de paquets

Vous pouvez activer la journalisation de paquet pour collecter des informations sur le trafic réseau *IP*.

Comment fonctionne le journal des paquets ?

La *consignation de paquets* recueille des informations sur le trafic réseau *IP*.

Par défaut, la consignation de paquets est désactivée. Elle est destinée avant tout aux utilisateurs expérimentés familiarisés avec les réseaux informatiques.

Vous pouvez activer la consignation de paquets si vous avez créé votre propre jeu de *règles de pare-feu* et souhaitez vérifier comment elles bloquent le trafic. Vous pouvez aussi l'activer lorsque vous soupçonnez une activité malveillante sur le réseau.

Les informations sont collectées dans 10 fichiers (`packetlog.0-packetlog.9`). À chaque fois que vous activez la *consignation de paquets*, ces données sont collectées dans un nouveau fichier. Lorsque le dixième fichier arrive à saturation, la consignation suivante est de nouveau collectée dans le premier fichier. Vous pouvez ainsi afficher les consignations précédentes tandis que la génération d'une nouvelle consignation est en cours.

Outre le trafic *IP*, la *consignation de paquets* collecte également des informations sur d'autres types de trafic réseau, tels que les *protocoles* nécessaires à votre *réseau local* (LAN). Ces données incluent des informations sur le *routage* par exemple.

Le *journal des paquets* se présente au format *hexadécimal* et prend en charge le format *tcpdump*. Ceci vous permet d'ouvrir les fichiers journaux dans un programme de journalisation des paquets autre que le visualiseur de *journal des paquets* par défaut. Vous pouvez également utiliser un programme d'analyse de *protocole* réseau pour analyser le contenu de manière plus approfondie.

Démarrer la journalisation du paquet

Vous pouvez démarrer la journalisation de paquet si vous suspectez une activité réseau malveillante ou, par exemple, lorsqu'un jeu en réseau ne fonctionne plus.

Pour démarrer la journalisation :

1. Sur la page principale, cliquez sur **Paramètres**.
2. Sélectionnez **Connexion réseau** ➤ **Consignation**.
3. Utilisez la durée de journalisation et la taille de fichier recommandées indiquées dans les champs **Temps de consignation** et **Taille max du fichier journal**.Vous pouvez également les modifier si vous désirez.
4. Cliquez sur **Démarrer la journalisation**. Un nouveau fichier est ajouté à la liste de fichiers journaux. La taille du fichier augmente à mesure que des informations sont collectées dans le fichier. Si la liste contient déjà 10 fichiers journaux, le journal suivant est inscrit dans un fichier existant.
5. Pour arrêter manuellement la journalisation, cliquez sur **Arrêter la journalisation**. La journalisation s'arrête automatiquement une fois la période de journalisation définie écoulée ou lorsque la taille maximale du fichier journal est atteinte.

Un nouveau fichier journal est généré et ajouté à la liste de fichiers journaux.

Afficher le *journal des paquets*

Après avoir créé un *journal des paquets*, vous pouvez l'ouvrir pour le consulter.

Pour afficher la *consignation de paquets* :

1. Sur la page principale, cliquez sur **Paramètres**.
2. Sélectionnez **Connexion réseau** ➤ **Consignation**.
3. Sélectionnez le *journal des paquets* que vous souhaitez consulter et cliquez sur **Détails**.
   Le visualiseur de *journal des paquets* par défaut s'ouvre. Le volet supérieur de la fenêtre regroupe toutes les connexions journalisées.

Vous pouvez consulter les informations suivantes :

Champ	Description
Durée	Durée, en secondes, à partir du début de la journalisation. Si la durée de journalisation est définie sur 60 secondes, le démarrage du premier *paquet* s'effectue vers 0 seconde et le démarrage du dernier *paquet* s'effectue vers 60 secondes.
Tirer (rép)	Indique si le *pare-feu* a laissé passer ou a ignoré le *paquet*, ainsi que le sens du *paquet* : • **Non** : le*paquet* a été autorisé. • **Oui** : le*paquet* a été ignoré. • **Entrant** : *paquet* entrant. • **Sortant** : *paquet* sortant. Ces informations ne sont pas disponibles si vous consultez le fichier dans un programme de journalisation de paquet autre que le visualiseur de *journal des paquets* par défaut.
Protocole	Le *protocole IP* utilisé.
Source	L'*adresse IP* source du *paquet*.

Champ	Description
Destination	L'*adresse IP* de destination du *paquet*.
ID	En-tête de message du *paquetIP* : Identifiant du paquet
TTL	En-tête de message du *paquetIP* : La valeur *TTL (durée de vie)* du *paquet* définit le nombre de périphériques réseau par lesquels le *paquet* peut voyager avant d'être détruit.
Len	En-tête de message du *paquet IP* : Longueur totale du *paquet*.
Description	Description du *paquet*.

Le volet de droite montre les types de trafic et les informations correspondantes.

Le volet inférieur de la fenêtre vous donne les informations aux formats *hexadécimal* et *ASCII*.

Si vous souhaitez voir tous les types de trafic réseau, pas seulement le trafic *IP*), déselectionnez la case à cocher **Filtrer non IP**.

Connexion à Policy Manager et importation manuelle d'un fichier de stratégie

Si vous devez initialiser une connexion avec le serveur Policy Manager Server à partir de l'hôte local, vous pouvez procéder comme suit :

1. Sur l'hôte local, accédez à la page **Gestion centrale**, où vous pouvez voir la date et l'heure de la dernière connexion à Policy Manager Server.
2. Cliquez sur **Vérifier maintenant** pour initier une nouvelle connexion.
   Si vous devez importer manuellement un nouveau fichier de stratégie sur un hôte, vous devez d'abord exporter une stratégie spécifique de l'hôte depuis Policy Manager Console avant de l'importer. Pour ce faire, procédez ainsi :
3. Dans Policy Manager Console :
   a) Sélectionnez l'hôte dans l'onglet **Domaines de stratégie**.
   b) Cliquez avec le bouton droit sur l'hôte de votre choix et sélectionné **Exporter le fichier de stratégie de l'hôte** dans le menu contextuel qui apparaît.
   c) Enregistrez le fichier de stratégie de l'hôte sur un support de transfert de votre choix, par exemple une disquette.
4. Dans l'interface utilisateur locale Client Security :
   a) Cliquez sur **Importer manuellement la stratégie...**.
   b) Dans la fenêtre qui s'ouvre, localisez le fichier `Policy.bpf` à importer dans l'hôte.

   L'importation d'un fichier de stratégie sert essentiellement à des fins de dépannage. Dans des conditions normales de fonctionnement, les fichiers de stratégies sont toujours transférés automatiquement. L'exportation et l'importation de stratégies peuvent servir à restaurer la connexion à Policy Manager, si l'hôte géré a été déconnecté en raison d'une stratégie mal configurée.

Suspension des téléchargements et mises à jour

Vous pouvez autoriser les utilisateurs à suspendre les communications réseau, par exemple s'ils utilisent une connexion commutée.

Cette option est configurée depuis Policy Manager Console. Elle est utile pour les hôtes qui utilisent parfois une connexion commutée lente. Lorsque cette option est activée, l'utilisateur peut suspendre temporairement les communications réseau, telles que l'interrogation automatique de stratégies et l'envoi de statistiques et de mises à jour automatiques.

1. Sélectionnez l'hôte dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez **Gestion centralisée**.
3. Sélectionnez **Autoriser les utilisateurs à suspendre tous les téléchargements et mises à jour**.
4. Cliquez sur  pour enregistrer et distribuer la stratégie.

Autoriser les utilisateurs à décharger les produits F-Secure

Vous pouvez autoriser les utilisateurs à décharger les produits, par exemple pour libérer de la mémoire.

Cette option indique si l'utilisateur est autorisé à décharger temporairement tous les produits Policy Manager Console. Elle indique si l'utilisateur est autorisé à décharger temporairement tous les produits F-Secure, par exemple pour libérer de la mémoire pour un jeu ou une application similaire.

👉 **Remarque:** Notez que les fonctions principales des produits sont désactivées aussi longtemps que le produit est déchargé et que l'ordinateur devient donc vulnérable aux virus et aux attaques.

1. Sélectionnez l'hôte dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et sélectionnez **Gestion centralisée**.
3. Sélectionnez l'une des options dans le menu déroulant **Autoriser l'utilisateur à décharger des produits**.
4. Cliquez sur pour enregistrer et distribuer la stratégie.

Chapitre
10

Informations sur les virus

Sujets :

- *Informations sur les antiprogrammes et les outils sur les pages Web F-Secure*
- *Comment envoyer un échantillon de virus à F-Secure*
- *Que faire en cas d'apparition d'un virus ?*

Elle fournit des informations sur des sites traitant des virus et sur la façon de gérer les virus que vous rencontrez.

Informations sur les antiprogrammes et les outils sur les pages Web F-Secure

Vous pouvez trouver une liste de sources d'informations relatives aux programmes malveillants et aux outils utiles à l'adresse suivante : http://www.f-secure.com/security_center/.

Pour obtenir des informations relatives aux dernières menaces à la sécurité, consultez les sources suivantes :

- Le F-Secure blog : *http://www.f-secure.com/weblog/*
- Vous trouverez une liste répertoriant les points vulnérables à l'adresse suivante : *http://www.f-secure.com/vulnerabilities/*
- Les menaces les plus récentes sont également annoncées sur votre bureau par le biais de Client Security sous la forme d'informations F-Secure.

Avant de nous envoyer un échantillon, pensez à utiliser notre **RescueCD**. Il s'agit d'un outil qui lance son propre système d'exploitation et qui est capable de trouver des programmes malveillants qui ne peuvent pas être détectés sous Windows. Il est disponible dans le Security Center : *http://www.f-secure.com/security_center/*.

Vous trouverez des instructions relatives à l'utilisation de **RescueCD** dans le fichier téléchargé.

Comment envoyer un échantillon de virus à F-Secure

Cette section comporte les rubriques suivantes relatives à l'envoi d'un échantillon de virus à F-Secure Security Lab.

👉 **Remarque:** Cette section est destinée aux utilisateurs expérimentés.

Veuillez nous envoyer les descriptions détaillées du problème, les symptômes ou vos questions, en anglais dans la mesure du possible.

Votre temps de réponse habituel est inférieure à 24 heures. Les cas complexes peuvent être plus longs à étudier. Si vous n'obtenez pas de réponse de notre part dans les jours ouvrables qui suivent, veuillez nous renvoyer votre échantillon.

Comment préparer un échantillon de virus ?

Tous les fichiers doivent être envoyés dans un fichier d'archivage ZIP.

Pour ce faire, vous pouvez télécharger une version d'essai de WinZip à l'adresse : *http://www.winzip.com/*. L'utilitaire gratuit InfoZIP est également disponble à l'adresse *http://www.info-zip.org/pub/infozip/*.

Toutes les archives ZIP doivent avoir un nom composé uniquement de lettres ou de chiffres utilisés en anglais. Vous pouvez utiliser des noms de fichiers longs.

Pour vous assurer que nous recevrons bien le fichier .zip, protégez ce fichier avec le mot de passe `infected` (infecté). Sinon, tout autre échantillon de programme malveillant, que vous tentez de nous envoyer, risque d'être supprimé par un serveur intermédiaire par mesure de sécurité. Cependant, un fichier protégé par un mot de passe (crypté) ne peut pas être analysé et est considéré comme étant sûr. Vous trouverez des instructions relatives à la méthode d'envoi d'un échantillon de virus à l'adresse suivante : *http://support.f-secure.com/enu/home/virusproblem/samples/index.shtml*.

Quels fichiers envoyer ?

Cette section vous indique les fichiers et les détails à envoyer, car les virus ne sont pas tous du même type et ne peuvent donc pas tous être envoyés de la même façon.

Les paragraphes qui suivent indiquent ce qu'il faut envoyer en fonction du type de virus :

1. Cheval de Troie ou autre antiprogramme (programme malveillant) autonome :

   Si vous envoyez un échantillon d'antiprogramme suspect (ver, porte dérobée, cheval de Troie, injecteur), spécifiez l'emplacement du fichier sur le système infecté et la façon dont il a été lancé (registre, fichiers `.ini`, `Autoexec.bat`, etc.). Une description de la source du fichier est également utile.

2. Une fausse alarme d'un de nos produits antivirus :

   Si vous recevez un avis de détection raté ou incorrect, ou une fausse alarme Client Security, essayez de nous envoyer :

   - le fichier en question,
   - le numéro de version Client Security,
   - la date de la dernière mise à jour des définitions de virus,
   - une description de la configuration du système,
   - une description de la méthode de reproduction du problème et
   - le fichier du rapport d'analyse Client Security. Pour obtenir des instructions relatives à la sauvegarde du fichier, reportez-vous à la page suivante : *http://support.f-secure.com/enu/home/virusproblem/samples/index.shtml*.

3. Un nouveau virus ou cheval de Troie :

Si vous pensez qu'une infection inconnue s'est insinuée dans votre ordinateur et qu'aucun programme antivirus ne la détecte, envoyez-nous :

- Si vous exécutez Windows XP, le rapport **msinfo32**. Pour créer ce rapport :
  1. Sélectionnez **Démarrer** ➤ **Exécuter...**.
  2. Tapez `msinfo32` et cliquez sur **OK**.
  3. Lors de l'affichage du nœud **Résumé système**, sélectionnez **Fichier** ➤ **Enregistrer**.
- Certains fichiers de configuration Windows (`WIN.INI`, `SYSTEM.INI`) et les fichiers de configuration DOS (`Autoexec.bat`, `Config.sys`).
- Une exportation complète ou partielle du registre système (préparée avec l'utilitaire **Redit** inclus dans toutes les versions de Windows).
- Le contenu du dossier `\Start Menu\Programs\Startup\`.

4. Virus infectant des fichiers exécutables :

   Essayez de recueillir différents fichiers système infectés. Généralement, 3 à 5 échantillons différents suffisent. Si possible, ajoutez des copies saines de ces mêmes fichiers (provenant de sauvegardes). Pour ce faire, utilisez deux répertoires dans votre fichier zip, par exemple :

   `ORIGINAL\APPPEND.EXE`

   `ORIGINAL\COMMAND.COM`

   `INFECTED\APPEND.EXE`

   `INFECTED\COMMAND.COM`

5. Virus de macro :

   Envoyez une copie infectée du fichier `NORMAL.DOT` (le modèle général) en plus des fichiers `DOC` infectés. Dans le cas de virus Excel, envoyez le fichier `PERSONAL.XLS` s'il existe, en plus des fichiers `XLS` infectés. Si le virus de macro a également infecté d'autres types de fichier, envoyez un échantillon de chaque type de fichier.

6. Virus du secteur d'amorçage :

   Si l'infection touche un disque dur, employez l'utilitaire **GetMBR** pour collecter des échantillons du secteur d'amorçage. Une fois le script terminé, envoyez-nous le fichier `mbr.dmp` de la façon décrite dans ce chapitre. **GetMBR** est téléchargeable sur notre site FTP : *ftp://ftp.f-secure.com/anti-virus/tools/getmbr.zip*.

   Si l'infection se trouve sur une disquette, créez une image DCF de la disquette infectée et envoyez-la nous. Vous pouvez télécharger l'utilitaire DCF à partir de notre site ftp : *ftp://ftp.f-secure.com/anti-virus/tools/dcf53.zip*.

   Vous pouvez également envoyer la disquette infectée par courrier à notre bureau de Helsinki (voir l'adresse ci-dessous). Veuillez inclure une description du problème. Notez que nous ne renvoyons pas les disquettes.

7. Une infection ou une fausse alarme sur un CD :

   Si une infection ou une fausse alarme est relative à un CD, vous pouvez envoyer ce dernier à nos bureaux finlandais.

   Joignez une description du problème et une copie imprimée du rapport Client Security, si possible. Nous renverrons le CD s'il n'est pas infecté.

Comment envoyer un échantillon de virus ?

Vous trouverez dans cette section des détails sur les différentes manières d'envoyer des échantillons de virus.

Vous pouvez nous envoyer les échantillons de trois façons différentes :

- La plus répandue consiste à utiliser notre formulaire Web d'envoi. Celui-ci vous donne toutes les informations dont nous avons besoin pour traiter un échantillon. Il se trouve à l'adresse suivante : *http://www.f-secure.com/samples*.
- Si la taille de l'échantillon est supérieure à 5 Mo, vous devez télécharger l'échantillon sur notre site FTP à l'adresse suivante : *ftp://ftp.f-secure.com/incoming/*.
- Si l'échantillon se trouve sur un support physique, par exemple un CD, un DVD ou une clé USB, vous pouvez nous envoyer ce support à l'adresse suivante :

  Security Labs

  F-Secure Corporation

  Tammasaarenkatu 7

  PL 24

  00181 Helsinki

  Finlande

Que faire en cas d'apparition d'un virus ?

Vous pouvez utiliser cette liste des actions à effectuer et des choses à ne pas oublier en cas d'apparition d'un virus sur le réseau de l'entreprise.

1. Déconnectez immédiatement l'ordinateur infecté du réseau.

   Si l'infection se répand, mettez le réseau hors service sans délai. Bloquez le trafic sortant. Donnez instruction aux employés de signaler immédiatement toute activité suspecte sur leur ordinateur.

2. Essayez d'identifier s'il s'agit d'une infection réelle ou d'une fausse alarme potentielle.

   Analysez l'ordinateur avec la version la plus récente de Client Security et les définitions de virus les plus récentes. Si l'infection est identifiée avec précision, passez à la prochaine étape. Si l'infection est identifiée comme `un nouveau virus possible`, `could be an image of a boot sector virus` etc., envoyez un échantillon accompagné du rapport d'analyseClient Security via l'outil Web **Submit Malware Sample** se trouvant à l'adresse : *http://www.f-secure.com/samples*.

3. S'il s'agit d'une infection connue, accédez aux pages d'informations sur les virus F-Secure pour obtenir une description de l'antiprogramme.

   Téléchargez des outils de nettoyage (s'ils sont disponibles) et imprimez les instructions ad hoc. Si vous avez besoin d'une assistance de désinfection, contactez le support via notre page Web d'assistance : *http://support.f-secure.com*.

   Si vous avez besoin d'une aide d'urgence, indiquez-le dans votre message.

4. S'il s'agit d'un nouveau virus, essayez de localiser un échantillon et envoyez-le à F-Secure Security Labs via le formulaire Web d'envoi à l'adresse suivante : *http://www.f-secure.com/samples*.

   Fournissez autant d'informations que possible sur le problème. Il importe de savoir combien d'ordinateurs sont touchés par le virus.

5. Si un ordinateur est infecté par un antiprogramme qui se répand sur le réseau local, il est recommandé de mettre ce dernier hors service jusqu'à ce que tous les ordinateurs infectés aient été nettoyés.

   Le réseau ne peut être remis en service qu'après le nettoyage de tous les ordinateurs, car une seule machine infectée peut réinfecter l'ensemble du réseau en quelques minutes.

6. Attendez que le Security Labs vous envoie un rapport, puis suivez attentivement les instructions de désinfection fournies.

   Il est recommandé de sauvegarder les données importantes de l'ordinateur infecté avant de le nettoyer. Cette sauvegarde ne sera pas effectuée via le réseau ; utilisez des unités de sauvegarde externes. Sauvegardez uniquement les fichiers de données, pas les fichiers exécutables. Si vous devez restaurer la sauvegarde par la suite, tous les fichiers restaurés devront être soumis à une vérification d'infection.

7. Lorsqu'il vous est fourni une solution de nettoyage, testez-la sur un seul ordinateur dans un premier temps. Si le nettoyage fonctionne, vous pouvez ensuite l'appliquer à tous les ordinateurs infectés.

   Analysez les ordinateurs nettoyés avec Client Security et les définitions de virus les plus récentes pour vous assurer qu'aucun fichier infecté n'a été omis.

8. Ne réactivez le réseau qu'après le nettoyage de chacun des ordinateurs infectés.

   Si l'antiprogramme contenait des portes dérobées ou des capacités de vol de données, il est vivement recommandé de changer les mots de passe et noms d'accès pour toutes les ressources du réseau.

9. Informez le personnel de l'infection et mettez-le en garde contre l'exécution de pièces jointes inconnues et la visite de sites Internet suspects

   Vérifiez les paramètres de sécurité des logiciels installés sur les postes de travail. Assurez-vous que les analyseurs de courrier électronique et les pare-feux fonctionnent correctement sur les serveurs. Client Security est censé recevoir les mises à jour automatiquement. Cependant, il est conseillé de vérifier périodiquement le bon fonctionnement de ces mises à jour automatiques.

10. Avertissez vos partenaires de l'infection et recommandez-leur d'analyser leurs ordinateurs avec Client Security et les définitions de virus les plus récentes pour s'assurer qu'aucune infection n'a quitté l'enceinte de votre réseau.

Chapitre
11

Configuration du plug-in Cisco NAC

Sujets :

- *Installation du plug-in Cisco NAC*
- *Importations de définitions d'attributs de validation de posture*
- *Utiliser des attributs pour un jeton de posture d'application*

F-Secure participe au programme NAC (Network Admission Control) animé par Cisco Systems®. NAC peut être utilisé pour restreindre l'accès réseau des hôtes ayant des bases de données de définitions de virus, ou des modules antivirus ou pare-feu trop anciens.

Le plug-in F-Secure NAC communique avec l'agent CTA (Cisco® Trust Agent), un logiciel client sur les hôtes qui collecte les informations liées à la sécurité à partir de l'hôte et communique ces données au serveur ACS (Cisco Secure Access Control Server). Sur la base de ces données, une stratégie d'accès appropriée est appliquée à l'hôte.

Pour plus d'informations sur NAC, visitez le site *http://www.cisco.com/go/nac/*.

Le package d'installation de Client Security contient une option pour installer le plug-in Cisco NAC. Lorsque vous sélectionnez cette option , le CTA doit déjà être installé sur l'hôte. En outre, le serveur ACS doit être configuré pour surveiller les attributs de sécurité liés aux produit F-Secure.

Installation du plug-in Cisco NAC

Le plug-in Cisco NAC peut être installé sur les hôtes localement et à distance.

1. Installations locales : lors de l'installation de Client Security localement, sélectionnez **Plug-in Cisco NAC** dans la boîte de dialogue **Composants à installer**.
2. Installations à distance : lors de l'installation de Client Security à distance, sélectionnez **Plug-in Cisco NAC** dans la boîte de dialogue **Composants à installer**.

   Remarque: Pour plus d'informations, consultez la documentation Cisco NAC.

Importations de définitions d'attributs de validation de posture

Vous devez ajouter les définitions d'attributs de validation de posture associées aux produits F-Secure dans le fichier des définitions d'attributs de validation de posture Cisco Secure ACS.

1. Utilisez l'outil **CSUtil** sur le serveur Cisco Secure ACS.
2. Utilisez la commande suivante :

   ```
   CSUtil.exe -addAVP fsnacpva.def
   ```

   Le fichier `fsnacpva.def` est inclus dans le module d'installation du produit.

   Remarque: Pour plus d'informations sur **CSUtil**, reportez-vous à la documentation de Cisco ACS.

Utiliser des attributs pour un jeton de posture d'application

Dans cette section, vous trouverez des informations sur la configuration du serveur Cisco ACS de manière à surveiller les attributs de sécurité associés aux produits.

Pour configurer le serveur Cisco ACS de manière à surveiller les attributs de sécurité associés aux produits F-Secure, procédez comme suit :

1. Cliquez sur le bouton **External user databases** (Bases de données d'utilisateurs externes) dans l'interface utilisateur du serveur Cisco ACS.
   La page **External user databases** (Bases de données d'utilisateurs externes) s'ouvre.
2. Cliquez sur **Database configuration** (configuration de la base de données).
   La page **External user databases configuration** (configuration des bases de données d'utilisateurs externes) s'ouvre.
3. Cliquez sur **Network admission control** (contrôle d'admission au réseau).
4. Cliquez sur **Configurer**.
5. Sélectionnez **Create new local policy** (créer une nouvelle stratégie locale).
6. Vous pouvez utiliser les attributs de sécurité Client Security suivants dans les règles des *jetons de posture d'application* :

   - Attributs de validation de posture pour antivirus :

Nom-attribut	Type	Exemple
Nom-logiciel	chaîne	`F-Secure Anti-Virus`
Version-logiciel	version	`8.0.0.0`
Date-Dat	date	`[la date de la base de données]`
Protection-Activée	entier non signé	`1`=activé, `0`=désactivé

   - Attributs de validation de posture pour pare-feu :

Nom-attribut	Type	Exemple
Nom-logiciel	chaîne	`Protection Internet F-Secure`
Version-logiciel	version	`8.0.0.0`
Protection activée	entier non signé	`1`=activé, `0`=désactivé

Chapitre
12

Fonctions avancées : protection contre les virus et les logiciels espions

Sujets :

- *Configuration de l'analyse planifiée*
- *Paramètres DeepGuard avancés*
- *Configuration de Policy Manager Proxy*
- *Configuration des mises à jour automatiques sur les hôtes à partir de Policy Manager Proxy*
- *Exclure une application de l'analyseur du trafic Web*

Cette section contient des instructions relatives à certaines tâches d'administration avancées de la protection antivirus, telles que la configuration d'une analyse planifiée à partir de l'interface utilisateur en **mode avancé** et la configuration du proxy antivirus.

Configuration de l'analyse planifiée

Une tâche d'analyse planifiée peut être ajoutée à partir de l'interface utilisateur en **mode avancé**.

Dans cet exemple, une tâche d'analyse planifiée est ajoutée à une stratégie pour l'ensemble du domaine de stratégie. L'analyse doit être effectuée chaque semaine, le lundi à 20h00, à partir du 25 août 2009.

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu.
   L'interface utilisateur est ouverte en **mode avancé**.
2. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
3. Dans l'onglet **Stratégie**, sélectionnez **F-Secure** ➤ **F-Secure Anti-Virus**.
4. Sélectionnez la page **Tableau de planification**.
   Les tâches planifiées actuellement définies s'affichent dans le tableau de **planification**. Vous pouvez maintenant ajouter une analyse planifiée comme nouvelle tâche.
5. Cliquez sur le bouton **Ajouter**.
   Une nouvelle ligne est ajoutée au tableau de **planification**.
6. Cliquez sur la cellule **Nom** de la ligne que vous venez de créer, puis cliquez sur **Modifier**.
7. La cellule **Nom** est maintenant activée et vous pouvez entrer le nom à donner à la nouvelle tâche.
   Par exemple, `Analyse planifiée pour tous les hôtes`.
8. Cliquez ensuite sur la cellule **Paramètres de planification**, puis cliquez sur **Modifier**.
9. Vous pouvez maintenant entrer les paramètres de l'analyse planifiée.
   Pour planifier une analyse chaque semaine, le lundi à 20h00, à partir du 25 août 2009, les paramètres sont les suivants : `/t20:00 /b2009-08-25 /rweekly`

   Remarque: Lorsque la cellule **Paramètres de planification** est sélectionnée, les paramètres que vous pouvez utiliser et les formats correspondants s'affichent sous la forme d'un texte d'aide dans le volet **Messages** (sous le tableau **Tâches planifiées**).

10. Sélectionnez le type de tâche en cliquant sur la cellule **Type de tâche**, puis en cliquant sur **Modifier**.
11. Dans la liste déroulante qui s'ouvre, sélectionnez **Analyse des lecteurs locaux**.
    La tâche d'analyse est maintenant prête pour la distribution.
12. Cliquez sur pour enregistrer et distribuer la stratégie.

Exécution d'analyses planifiées pour des jours ouvrables et des jours spécifiques :

Lorsque vous configurez une analyse planifiée hebdomadaire, vous pouvez également définir des jours ouvrables spécifiques pour l'exécution de l'analyse. De même, lorsque vous configurez une analyse planifiée mensuelle, vous pouvez définir des jours spécifiques du mois pour l'exécution de l'analyse. Pour ces analyses, vous pouvez utiliser le paramètre `/Snn` :

- Pour des analyses planifiées hebdomadaires, vous pouvez utiliser `/rweekly` avec les paramètres `/s1` - `/s7`. `/s1` signifie lundi et `/s7` dimanche.

  Par exemple, `/t18:00 /rweekly /s2 /s5` signifie que l'analyse est exécutée chaque mardi et vendredi à 18 heures.
- Pour des analyses planifiées mensuelles, vous pouvez utiliser `/rmonthly` avec les paramètres `/s1` - `/s31`.

  Par exemple, `/t18:00 /rmonthly /s5 /s20` signifie que l'analyse est exécutée le 5 et le 20 de chaque mois, à 18 heures.

Remarque: Les analyses planifiées hebdomadaires sont automatiquement exécutées chaque lundi. Les analyses planifiées mensuelles sont automatiquement exécutées le premier jour de chaque mois.

Paramètres DeepGuard avancés

Cette section décrit les paramètres avancés de DeepGuard.

Notification d'un utilisateur d'un événement de refus

Vous pouvez configurer le produit afin d'avertir les utilisateurs lorsque DeepGuard refuse un événement qu'ils ont lancé.

Pour avertir l'utilisateur lorsque DeepGuard refuse automatiquement un événement :

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu.
   L'interface utilisateur est ouverte en **mode avancé**.
2. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
3. Dans l'onglet **Stratégie**, sélectionnez **F-Secure** ➤ **F-Secure DeepGuard** ➤ **Paramètres** ➤ **Afficher le panneau de notification lors d'événements de refus**.
4. Sélectionnez **Oui** dans la zone principale de l'application.
5. Cliquez sur pour enregistrer et distribuer la stratégie.

Permettre à un administrateur d'autoriser ou de refuser des événements provenant de programmes d'autres utilisateurs

Vous pouvez permettre à un utilisateur disposant de droits d'accès administrateur d'autoriser ou de refuser un événement provoqué par une application lancée par un autre utilisateur.

1. Sélectionnez **Affichage** ➤ **Menu avancé** dans le menu.
   L'interface utilisateur s'ouvre en **mode avancé**.
2. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
3. Dans l'onglet **Stratégie**, sélectionnez **F-Secure** ➤ **F-Secure DeepGuard** ➤ **Paramètres** ➤ **Contrôle de l'administrateur local**.
4. Sélectionnez **Tous les processus**.
5. Cliquez sur pour enregistrer et distribuer la stratégie.

Autorisation ou refus des événements requis automatiquement par une application spécifique

Vous pouvez choisir d'autoriser tous les événements d'une application sûre ou refuser tous les événements d'une application qui ne devrait pas être utilisée.

1. Tout d'abord, vous devez calculer l'identificateur de hachage SHA-1 de l'application.

   Il existe des calculateurs SHA-1 disponibles gratuitement sur Internet. Vous pouvez utiliser par exemple l'outil FCIV (File Checksum Integrity Verifier) de Microsoft. Il se trouve à l'adresse suivante : *http://support.microsoft.com/kb/841290*.

   Remarque: Un hachage SHA-1 identifie de façon unique la séquence d'instructions qui définit un programme. Si une nouvelle version du programme est disponible, vous devez répéter ce processus car le nouveau programme aura un hachage SHA-1 différent.

2. Une fois le hachage de l'identificateur SHA-1 calculé, sélectionnez **Affichage** ➤ **Mode avancé** dans le menu.
   L'interface utilisateur s'ouvre en **mode avancé**.
3. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.

4. Dans l'onglet **Stratégie**, sélectionnez **F-Secure** ➤ **F-Secure DeepGuard** ➤ **Paramètres** ➤ **Applications**.
5. Cliquez sur **Ajouter** pour ajouter la nouvelle règle.
6. Cliquez deux fois sur la cellule du **hachage SHA-1** de la nouvelle entrée et collez le hachage SHA-1 dans la cellule vide.
7. Cliquez deux fois sur la cellule **Remarques** de la nouvelle entrée et saisissez une remarque.
   Cette remarque vous permettra de vous souvenir de l'application identifiée par le hachage SHA-1.
8. Cliquez deux fois sur la cellule **Approuvée** de la nouvelle entrée :
   - Sélectionnez **Oui** pour autoriser tous les événements de l'application.
   - Sélectionnez **Non** pour refuser tous les événements de l'application.
9. Cliquez deux fois sur la cellule **Activée** de la nouvelle entrée.
10. Sélectionnez **Oui** pour activer la règle.
11. Cliquez sur  pour enregistrer et distribuer la stratégie.

La règle d'application ne peut pas être écrasée localement par l'utilisateur.

Configuration de Policy Manager Proxy

Policy Manager offre une solution aux problèmes de bande passante rencontrés dans les installations en réduisant sensiblement la charge sur les réseaux utilisant des connexions lentes.

Policy Manager Proxy met en mémoire cache les mises à jour récupérées à partir du serveur de mise à jour F-Secure central ou du Policy Manager Server de l'entreprise, et se trouve sur le même réseau distant que les hôtes qui l'emploient comme point de distribution des bases de données. Chaque réseau lent devrait idéalement comporter une installation de Policy Manager Proxy.

Les hôtes exécutant Client Security ou Anti-virus for Workstations récupèrent les mises à jour de définitions des virus par le biais de Policy Manager Proxy. Policy Manager Proxy contacte en fonction des besoins Policy Manager Server et le serveur de distribution F-Secure.

Les postes de travail des bureaux distants communiquent eux aussi avec le serveur Policy Manager Server du siège central, mais cette communication est limitée à l'administration des stratégies distantes, à la surveillance d'état et aux alertes. Comme le trafic intense de mise à jour de base de données est redirigé à travers Policy Manager Proxy dans le même réseau local, la connexion du réseau entre les postes de travail gérés et Policy Manager Server présente une charge substantiellement plus légère.

Remarque: Pour plus d'informations sur l'installation et la configuration de Policy Manager Proxy, consultez le Guide de l'administrateur Policy Manager Proxy.

Configuration des mises à jour automatiques sur les hôtes à partir de Policy Manager Proxy

La liste de proxies par le biais desquels les hôtes récupèrent les mises à jour peut être configurée dans l'onglet **Paramètres**.

Si vous devez effectuer cette configuration à partir de l'interface utilisateur locale d'un hôte géré, vous pouvez procéder comme suit :

1. Accédez à la page **Mises à jour automatiques** et cliquez sur **Paramètres avancés**.
2. Sélectionnez **Mises à jour automatiques** ➤ **Policy Manager Proxy**.

   La page **Policy Manager Proxy** permet de visualiser et de modifier les adresses à partir desquelles l'application Client Security locale obtient les mises à jour automatiques.

   Les adresses sont utilisées de haut en bas, c'est-à-dire que la première adresse de la liste est utilisée par défaut.
3. Cliquez sur **Ajouter** pour ajouter un nouveau serveur proxy à la liste.
4. Entrez le nom du premier proxy dans le champ, puis cliquez sur **OK**.
5. Répétez ces opérations pour les autres proxies à ajouter.

   Pour modifier l'ordre des serveurs, sélectionnez le serveur à déplacer et cliquez sur les flèches haut et bas situées à droite pour le déplacer.
6. Une fois tous les proxies ajoutés, cliquez sur **OK**.

Exclure une application de l'analyseur du trafic Web

Si l'analyse du trafic Web provoque des problèmes dans un programme répandu au sein de votre organisation, vous pouvez exclure cette application de l'analyseur du trafic Web.

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu.
2. Dans l'onglet **Stratégie**, sélectionnez **F-Secure Client Security** ➤ **Sélectionner un scanneur de protocoles** ➤ **Applications approuvées** ➤ **Liste des processus approuvés**.
3. Saisissez le nom du processus à exclure de l'analyseur de trafic Web.

   Pour saisir plusieurs processus, séparez le nom de chaque processus par une virgule. N'insérez aucun espace entre les noms de processus.

   Astuce: Sous Windows, vous pouvez trouver le nom de processus d'une application en utilisant l'explorateur de tâches Windows.

   Par exemple, si vous voulez exclure les applications Notepad et Skype de l'analyseur du trafic Web, vous devez saisir `notepad.exe,skype.exe`.
4. Cliquez sur pour enregistrer et distribuer la stratégie.

Chapitre

13

Fonctions avancées : protection Internet

Sujets :

- *Gestion à distance des propriétés de la protection Internet*
- *Configuration de la sélection automatique du niveau de sécurité*
- *Dépannage de problèmes de connexion*
- *Ajout de nouveaux services*
- *Installation de Dialup Control*

Cette section décrit certaines fonctions avancées de la protection Internet et contient également quelques informations de dépannage.

Gestion à distance des propriétés de la protection Internet

Cette section décrit la gestion à distance des propriétés de la protection Internet.

Utilisation de la consignation des paquets

La consignation de paquets est un outil de débogage très utile pour découvrir ce qui se passe sur le réseau local.

La consignation des paquets est un outil puissant qui peut être utilisé abusivement par un utilisateur pour épier les activités d'autres utilisateurs sur le réseau. Dans certains environnements d'entreprise, l'administrateur devra donc désactiver la consignation des paquets.

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu.
   L'interface utilisateur s'ouvre en **Mode avancé**.
2. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
3. Dans l'onglet **Stratégie**, sélectionnez **Protection Internet F-Secure**.
4. Sélectionnez l'onglet **Consignation**.
   Cette variable montre normalement l'état de la consignation des paquets : **Désactivé** signifiant qu'elle est désactivée, tandis que **Activé** indique que la consignation est en cours sur l'hôte.
5. Pour désactiver complètement la journalisation, assurez-vous qu'elle est paramétrée sur **Désactivé**, puis cochez la case **Final**.
6. Distribuez la stratégie pour appliquer la modification.

Pour annuler cette modification par la suite, désactivez la case **Final** et distribuez la nouvelle stratégie.

Remarque: Utilisez cette variable avec prudence car, par exemple, si elle est définie sur **Activé** pour l'ensemble du domaine, une session de consignation sera lancée sur tous les hôtes concernés.

Utilisation de l'interface approuvée

Le mécanisme d'interface approuvée est utilisé pour permettre l'utilisation de l'hôte protégé par le pare-feu comme serveur de partage de connexion.

Les règles de pare-feu ne sont pas appliquées au trafic traversant l'interface approuvée. Mal utilisée, cette fonction peut exposer l'ordinateur hôte à toute forme d'attaque à partir du réseau : il est donc de bonne pratique de désactiver ce mécanisme s'il n'est pas absolument nécessaire.

L'interface approuvée s'active comme suit :

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu.
   L'interface utilisateur s'ouvre en **Mode avancé**.
2. Sélectionnez le sous-domaine dans lequel vous souhaitez activer l'interface approuvée dans l'arborescence **Domaines de stratégie**.
3. Dans l'onglet **Stratégie**, sélectionnez **Protection Internet de F-Secure** ➤ **Paramètres** ➤ **Moteur pare-feu** ➤ **Autoriser interface approuvée** .
4. Sélectionnez **Activé** pour activer l'interface approuvée pour le sous-domaine sélectionné.
   Cela permet aux utilisateurs finaux du sous-domaine de configurer une interface réseau comme interface approuvée.
5. Enregistrez et distribuez la stratégie pour appliquer la modification.

Utilisation du filtrage des paquets

Ce mécanisme de sécurité fondamental du pare-feu filtre tout le trafic réseau IP en fonction des informations contenues dans les en-têtes de protocole de chaque paquet.

Vous pouvez activer ou désactiver le filtrage des paquets à partir de l'onglet **Avancé** dans la section des paramètres **Protection du réseau**. Sa désactivation est parfois nécessaire à des fins de test, mais elle présente un risque pour la sécurité. Dans la plupart des environnements d'entreprise, vous devrez donc vous assurer que le filtrage des paquets est toujours activé.

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu.
   L'interface utilisateur s'ouvre en **Mode avancé**.
2. Sélectionnez **Racine** dans l'onglet **Domaines de stratégie**.
3. Dans l'onglet **Stratégie**, sélectionnez **Protection Internet F-Secure** ➤ **Paramètres** ➤ **Moteur pare-feu** ➤ **Moteur pare-feu**.
4. Pour faire en sorte que le filtrage des paquets soit toujours activé, définissez cette variable sur **Oui** et cochez la case **Final**.
5. Distribuez la stratégie pour appliquer la modification.

Configuration de la sélection automatique du niveau de sécurité

Dans l'exemple suivant, la sélection automatique du niveau de sécurité est configurée pour un sous-domaine qui contient uniquement des ordinateurs portables de sorte que, lorsque les ordinateurs sont connectés au réseau de l'entreprise, ils utilisent le niveau de sécurité **Bureau** ; lorsqu'une connexion commutée est utilisée, le niveau de sécurité est changé en **Mobile**.

Avant de commencer, vous devez connaître l'adresse IP du serveur DNS et l'adresse de la passerelle par défaut, car elles permettent de définir les critères de sélection automatique du niveau de sécurité. Vous pouvez obtenir ces adresses en exécutant la commande `ipconfig -all` dans l'invite de commande.

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu.
   L'interface utilisateur en **Mode avancé** s'ouvre.
2. Sélectionnez le sous-domaine dans l'arborescence **Domaines de la stratégie**.
3. Dans l'onglet **Stratégie**, sélectionnez **F-Secure** ➤ **Protection Internet F-Secure**.
4. Sélectionnez la page **Sélection automatique du niveau de sécurité**.
5. Assurez-vous que la sélection automatique du niveau de sécurité est activée.
   Pour l'activer, sélectionnez l'option **Modifiable par l'utilisateur** ou **Contrôle total de l'administrateur** dans la liste déroulante **Mode Sélection automatique**.
6. Cliquez sur **Ajouter** pour ajouter le premier niveau de sécurité, dans cet exemple **Bureau**.
7. Pour entrer des données dans une cellule, sélectionnez la cellule et cliquez sur **Modifier**.
   Vous devez ajouter les données suivantes pour le niveau de sécurité **Bureau** :
   - **Priorité** : les règles sont contrôlées dans l'ordre défini par les numéros de priorité, en commençant par le plus petit numéro.
   - **Niveau de sécurité** : entrez l'ID (composé du numéro et du nom) du niveau de sécurité, par exemple : `40burea` .
   - **Méthode 1** : sélectionnez l'**adresse IP du serveur DNS** dans la liste déroulante.
   - **Argument 1** : entrez l'adresse IP de votre serveur DNS local, par exemple : `10.128.129.` .
   - **Méthode 2** : sélectionnez **Adresse IP de la passerelle par défaut** dans la liste déroulante.
   - **Argument 2** : entrez l'adresse IP de votre passerelle par défaut, par exemple : `10.128.130.1`.

   Remarque: Vous ne pouvez utiliser qu'un seul argument, par exemple une adresse IP, dans le champ **Argument**. Lorsqu'il existe plusieurs passerelles par défaut dans votre société et que vous souhaitez les utiliser toutes dans le cadre de la sélection automatique du niveau de sécurité, vous pouvez créer une règle distincte pour chacune d'elles dans le tableau.

   Le premier niveau de sécurité est maintenant prêt.
8. Cliquez sur **Ajouter** pour ajouter le second niveau de sécurité, dans cet exemple **Mobile**.
9. Pour entrer des données dans une cellule, sélectionnez la cellule et cliquez sur **Modifier** .
   Vous devez ajouter les données suivantes pour le niveau de sécurité **Mobile** :
   - **Priorité** : les règles sont contrôlées dans l'ordre défini par les numéros de priorité, en commençant par le plus petit numéro.
   - **Niveau de sécurité** : entrez l'ID du niveau de sécurité ici, par exemple : `20mobile`.
   - **Méthode 1** : sélectionnez **Accès à distance** dans la liste déroulante.
   - **Argument 1** : vous n'êtes pas obligé de renseigner ce champ.
   - **Méthode 2** : sélectionnez **Toujours** dans la liste déroulante.
   - **Argument 2** : vous n'êtes pas obligé de renseigner ce champ.

   La configuration est maintenant prête.
10. Cliquez sur  pour enregistrer et distribuer la stratégie.

Dépannage de problèmes de connexion

Si vous rencontrez des problèmes de connexion, par exemple si un hôte ne peut pas accéder à Internet et si vous soupçonnez la protection Internet d'être à l'origine de ces problèmes, vous pouvez utiliser la liste de contrôle suivante.

1. Vérifiez que l'ordinateur est correctement connecté.
2. Vérifiez que le problème ne provient pas du câble réseau.
3. Vérifiez qu'Ethernet est actif et fonctionne correctement.
4. Vérifiez que l'adresse DHCP est correcte.

   Pour ce faire, entrez la commande `ipconfig` dans l'invite de commande.
5. Ensuite, envoyez une commande ping à la passerelle par défaut.

   Si vous n'en connaissez pas l'adresse, vous pouvez la trouver en entrant la commande `ipconfig -all` dans l'invite de commande. Ensuite, envoyez un ping à la passerelle par défaut pour voir si elle répond.
6. Si la navigation Internet normale ne fonctionne pas, vous pouvez essayer d'envoyer un ping à un serveur DNS :

   - Exécutez `nslookup` pour vous assurer que le service DNS fonctionne.
   - Vous pouvez également essayer d'échanger un ping avec une adresse Web connue pour vous assurer que l'ordinateur distant n'est pas hors service.
7. Ensuite, vérifiez si quelque chose a changé dans le domaine géré de façon centrale ; une nouvelle stratégie est-elle utilisée et cette stratégie contient-elle des paramètres susceptibles de causer ces problèmes ?

   - Vérifiez dans les règles de pare-feu que les connexions HTTP sortantes sont autorisées.
   - Vérifiez dans le contrôle des applications local que l'adresse IP à laquelle l'utilisateur tente de se connecter n'a pas été accidentellement ajoutée à la liste des adresses refusées.
8. Si rien d'autre n'y fait, déchargez les produits F-Secure ou mettez la protection Internet en mode Tout autoriser.

Si le problème persiste, il provient probablement du routage ou d'un autre composant dans l'ordinateur auquel l'utilisateur tente de se connecter.

Ajout de nouveaux services

Un service (abréviation de service de réseau) correspond à un service disponible sur le réseau, par exemple, le partage de fichiers, l'accès distant à la console ou la navigation sur le Web.

Les services sont le plus souvent décrits par le protocole et le port qu'ils utilisent.

Création d'un service Internet basé sur le protocole HTTP par défaut

Dans cet exemple, on suppose qu'un serveur Web tourne sur un ordinateur et qu'il est configuré pour utiliser un port Web non standard.

En règle générale, un serveur Web utiliserait le port TCP/IP 80, mais dans ce cas précis, il a été configuré de manière à utiliser le port 8000. Pour autoriser les connexions entre ce serveur et les postes de travail, vous allez devoir créer un service. Le service HTTP standard ne fonctionne pas ici, car nous n'utilisons plus le port HTTP standard. Ce nouveau service est le `port HTTP 8000` qui est basé sur le serveur `HTTP` par défaut.

1. Sélectionnez le sous-domaine pour lequel vous souhaitez créer le nouveau service dans l'onglet **Domaines de stratégie**.
2. Accédez à l'onglet **Paramètres** et ouvrez la page **Services de pare-feu**.
   Cette page contient la table des **Services de pare-feu**.
3. Cliquez sur le bouton **Ajouter** pour lancer l'assistant **Services de pare-feu**.
4. Entrez un nom de service :
   a) Renseignez le champ **Nom du service** en attribuant un nom unique au service. Deux services ne peuvent pas porter le même nom.
   Par exemple, `Port HTTP 8000`.
   b) Entrez un commentaire décrivant le service dans le champ **Commentaire sur le service**.
   Le commentaire s'affichera dans la table **Services du pare-feu**.
5. Sélectionnez un numéro de protocole IP :
   a) Sélectionnez un numéro de protocole pour ce service dans la liste déroulante **Protocole** .
   Vous pouvez sélectionner les protocoles les plus fréquemment utilisés (TCP, UDP, ICMP). Si votre service utilise un autre protocole, référez-vous au tableau ci-dessous et entrez le numéro approprié.
   Dans cet exemple, sélectionnez **TCP (6)** dans la liste déroulante **Numéro de protocole IP :**.

Nom du protocole	Numéro de protocole	Nom complet
ICMP	1	Protocole ICMP
IGMP	2	Internet Group Management Protocol
IPIP	4	IPIP Tunnels (IP in IP)
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
PUP	12	Xerox PUP routing protocol
UDP	17	User Datagram Protocol
IDP	22	Xerox NS Internet Datagram Protocol
IPV6	41	IP Version 6 encapsulation in IP version 4
RSVP	46	Resource Reservation Protocol

Nom du protocole	Numéro de protocole	Nom complet
GRE	47	Cisco Generic Routing Encapsulation (GRE) Tunnel
ESP	50	Encapsulation Security Payload protocol
AH	51	Authentication Header protocol
PIM	103	Protocol Independent Multicast
COMP	108	Compression Header protocol
RAW	255	Raw IP packets

6. Sélectionnez les ports émetteurs :

   Si votre service utilise le protocole TCP ou UDP, vous devez définir les ports émetteurs couverts par le service. Le format de saisie des ports et séries de ports est le suivant :

   - `>port` : tous les ports supérieurs à `port`
   - `>=port` : tous les ports égaux et supérieurs à `port`
   - `<port` : tous les ports inférieurs à `port`
   - `<=port` : tous les ports égaux et inférieurs à `port`
   - `port` : uniquement le `port`
   - `minport-maxport` : `minport` et `maxport` plus tous les ports entre eux. Notez qu'il n'y a pas d'espace de part et d'autre du tiret.

   Vous pouvez définir des combinaisons de ces éléments, séparées par des virgules. Par exemple, les ports 10, 11, 12, 100, 101, 200 et supérieurs à 1023 peuvent être définis sur `10-12, 100-101, 200, >1023`.

   Dans cet exemple, définissez le port émetteur sur `>1023`.
7. Sélectionnez les ports récepteurs :

   Si le service utilise le protocoleTCP ou UDP, définissez les ports répondeurs du service.

   Dans cet exemple, définissez le port récepteur comme `8000`.
8. Sélectionnez un numéro de classification pour ce service dans la liste déroulante.

   Vous pouvez accepter la valeur par défaut.
9. Sélectionnez si un filtrage supplémentaire doit être appliqué au trafic autorisé par le service que vous créez, outre le filtrage normal des paquets et le filtrage dynamique.
   Dans cet exemple, vous pouvez accepter la valeur par défaut, qui est **Désactivé**.

   > **Remarque:** Lorsque le service utilise le protocole TCP et que la fonction Contrôle des applications n'est pas activée, vous pouvez sélectionner **Mode FTP actif** dans le menu déroulant **Filtrage supplémentaire**. Le **mode FTP actif** exige un traitement spécial de la part du pare-feu, car les informations concernant le port à ouvrir pour la connexion sont incluses dans les données transférées.

10. Vous pouvez maintenant vérifier la règle.

    Si vous devez apporter un changement quelconque à la règle, cliquez sur **Précédent** dans la règle.
11. Cliquez sur **Terminer** pour fermer l'Assistant Règle.
    La règle que vous venez de créer est maintenant affichée dans le tableau **Règles du pare-feu**.
12. Mise en application de la nouvelle règle :

    Pour mettre en application ce nouveau service, vous devez créer une nouvelle règle de protection Internet autorisant l'utilisation du service de pare-feu **HTTP 8000** dans le niveau de sécurité de la protection Internet actuellement utilisé. Dans ce cas, vous pouvez sélectionner le nouveau service sur la page **Assistant Règle ➤ Service** et vous ne devez définir aucune alerte sur la page **Assistant Règle ➤ Options avancées**.

Installation de Dialup Control

Dialup Control vous permet de créer des listes de numéros de téléphone autorisés et bloqués depuis le modem de liaison des utilisateurs.

Pour activer Dialup Control :

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu pour basculer sur l'interface utilisateur en **Mode avancé**.
2. Dans l'onglet **Stratégie**, sélectionnez **F-Secure** ➤ **Protection Internet F-Secure** ➤ **Paramètres** ➤ **Dialup control** ➤ **Dialup control**.
3. Sélectionnez **Activé** pour mettre en marche Dialup Control.
4. Cliquez sur pour enregistrer et distribuer la stratégie.

Autorisation et blocage des numéros de téléphone

Vous pouvez autoriser des numéros de téléphone spécifiques ou bloquer leur utilisation pour les connexions commutées.

Pour ajouter un numéro autorisé ou bloqué :

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu pour basculer sur l'interface utilisateur en **Mode avancé**.
2. Dans l'onglet **Stratégie**, sélectionnez **F-Secure** ➤ **Protection Internet F-Secure** ➤ **Paramètres** ➤ **Dialup Control** ➤ **Numéros de téléphone**.
3. Cliquez sur **Ajouter**.
4. Cliquez deux fois sur la cellule **Priorités** de la nouvelle ligne afin de définir la priorité de la règle.

   Si deux règles correspondent à un numéro de téléphone, la règle avec la priorité dont le numéro est le moins élevé s'applique, c'est-à-dire qu'une règle avec une priorité de `1` écrasera une règle avec une priorité de `3`.
5. Cliquez deux fois sur la cellule **Numéro de téléphone** de la nouvelle ligne pour ajouter les numéros de téléphone auxquels la règle s'applique.

   Vous pouvez utiliser les caractères suivants pour appliquer une règle à plusieurs numéros de téléphone :

Caractère	S'applique à:	Exemple
?	Correspond à tout chiffre seul	`1?3` correspond aux nombres suivants : 103, 113, 123,133,143, 153,163,173,183,193.
*	Correspond à tout nombre de chiffres	`0800*` correspond à tous les numéros de téléphone qui commencent par 0800

6. Sélectionnez **Autoriser** ou **Refuser** pour autoriser ou empêcher le modem d'appeler les numéros de téléphone correspondants.
7. Cliquez deux fois sur la cellule **Commentaire** de la nouvelle ligne et ajoutez une description pour expliquer le but de la règle aux autres utilisateurs.
8. Sélectionnez **Oui** pour appliquer la nouvelle règle.
9. Cliquez sur pour enregistrer et distribuer la stratégie.

Utilisation de l'enregistrement des appels

Vous pouvez utiliser l'enregistrement des appels pour conserver un journal de tous les numéros composés qui ont été utilisés.

Pour activer l'enregistrement des numéros composés :

1. Sélectionnez **Affichage** ➤ **Mode avancé** dans le menu pour basculer sur l'interface utilisateur en **Mode avancé**.
2. Dans l'onglet **Stratégie**, sélectionnez **F-Secure** ➤ **Protection Internet F-Secure** ➤ **Paramètres** ➤ **Dialup control** ➤ **Enregistrement des numéros**.
3. Sélectionnez **Activé** pour enregistrer les numéros que le modem appelle.
4. Cliquez sur  pour enregistrer et distribuer la stratégie.

Chapitre
14

Modification de prodsett.ini

Sujets :

- *Paramètres prodsett.ini configurables*

Cette section présente la liste des paramètres pouvant être modifiés dans `prodsett.ini`.

Avertissement: Ne modifiez pas les paramètres de `prodsett.ini` qui ne sont pas inclus dans cette section.

Remarque: Dépendance entre les paramètres `RequestInstallMode` et `InstallMode` : les paramètres

L'icône `RequestInstallMode` ont préséance sur la sélection des composants dont `InstallMode=0`.

Paramètres prodsett.ini configurables

Vous pouvez modifier les paramètres décrits ici dans le fichier `prodsett.ini`.

[F	Paramètres communs
CD-Key=XXXX-XXXX-XXXX-XXXX-XXXX	Entrez ici la clé d'abonnement du logiciel d'installation.
SetupLanguage=ENG	Langue d'installation appliquée. Si le paramètre est vide ou défini sur `AUTO`, la langue d'installation est choisie automatiquement au niveau de l'hôte en fonction des paramètres régionaux système par défaut. Le choix est limité au jeu de langues prises en charge (voir SupportedLanguages).
SetupMode=1	`1` = client réseau (valeur par défaut). Si `SetupMode=1`, les paramètres de gestion centralisée correspondant doivent être définis dans la section [PMSUINST.DLL]. `2` = Mode d'installation autonome.
SupportedLanguages=ENG FRA DEU FIN SVE ITA	Liste des langues prises en charge par le logiciel d'installation. Vous pouvez réduire la palette de langues en omettant les langues inutiles et en recompactant le module. Lorsque vous ajoutez la prise en charge d'une nouvelle langue dans le logiciel, ajoutez cette langue ici pour rendre le changement effectif.
InstallLanguages=ENG FRA DEU FIN SVE ITA	Liste des langues installées sur l'hôte. La valeur de ce paramètre est généralement identique à `SupportedLanguages`. Vous pouvez réduire la palette de langues si vous voulez que certaines langues dont vous n'avez pas besoin ne soient pas installées. Lorsque vous ajoutez la prise en charge d'une nouvelle langue dans le logiciel, ajoutez cette langue ici pour rendre le changement effectif pour le logiciel installé. Les fichiers linguistiques de la langue définie par le paramètre SetupLanguage sont toujours installés indépendamment du paramètre InstallLanguages.
SecurityPolicy=0 | 1 | 2	Les fichiers et dossiers installés en NTFS et les clés de registre du produit sont protégés par les autorisations de sécurité NT conformément à la stratégie de sécurité définie (`SecurityPolicy`) : `0` = pas de stratégie particulière ; les fichiers et dossiers héritent des autorisations de sécurité du parent.

[F	Paramètres communs
	1 = stratégie moins stricte ; les fichiers et dossiers sont protégés par des autorisations donnant un accès complet aux utilisateurs autorisés et aux administrateurs, et un accès en lecture seule à tous les autres. 2 = stratégie stricte ; les fichiers et dossiers sont protégés par des autorisations donnant un accès complet aux administrateurs, un accès en lecture-écriture aux utilisateurs avancés, un accès en lecture seule aux utilisateurs et aucun accès à tous les autres. Remarque : quand `SecurityPolicy = 1` ou `2` , le programme d'installation écrase les listes de contrôle d'accès (ACL) des fichiers, dossiers et clés de registre existant. Si vous avez personnalisé la configuration des listes de contrôle d'accès, par exemple, en y ajoutant des utilisateurs, vous devez procéder à leur reconfiguration après l'installation.

[Silent Setup]	Paramètres utilisés par l'installation automatique
DestinationDirUnderProgramFiles=F-Secure	Chemin de destination par défaut. Ne modifiez pas ce paramètre, à moins que votre entreprise ne suive une stratégie d'installation spécifique.
Reboot=2	`1` = Redémarrer automatiquement l'ordinateur après l'installation. **Attention:** Cette option exécute un redémarrage forcé sur l'hôte sans inviter l'utilisateur à enregistrer son travail. N'utilisez cette option que si vous êtes absolument sûr que ce type de redémarrage est sans risque pour l'ordinateur de destination. `2` = Redémarrer après confirmation de l'utilisateur (valeur par défaut). **Remarque:** Cette option exécute un redémarrage normal de l'hôte et donc, dans certains cas, l'utilisateur peut retarder le redémarrage ou même l'empêcher complètement. `3` = Ne pas redémarrer l'ordinateur après l'installation.

[FSMAINST.DLL]	Paramètres pour la prise en charge de Management Agent
RequestInstallMode=1	Ce composant est systématiquement installé lors de l'installation d'un client réseau. Il ne nécessite pas la modification des paramètres `RequestInstallMode` ou `InstallMode`.

[FSMAINST.DLL]	Paramètres pour la prise en charge de Management Agent
ManagementKey=\\serveur\chemin\admin.pub	Emplacement de la clé publique de gestion.
ManagedStandAlone=	Paramètre significatif uniquement dans les installations autonomes. `0` = Installations autonomes normales, aucun fichier de stratégie ne peut être importé (valeur par défaut). `1` = L'administration des composants installés est effectuée via des stratégies importées manuellement.
win2000renamefiles=fsrec.2k|fsrec.sys;fsfilter.2k|fsfilter.sys;fsgk.2k|fsgk.sys InstallFSPKIH=0 InstallNetworkProvider=0 InstallGINA=0 RedefineSettings=0 ServiceProviderMode=0 MibVersion= GatekeeperVersion= StatisticsFilterPattern1=	Ne modifiez pas ces paramètres !
UseOnlyUID=	`0` = Management Agent utilise uniquement toutes les identités disponibles (nom DNS, adresse IP, nom WINS, Identité unique) pour s'identifier la première fois auprès du Policy Manager Server. `1` = Management Agent utilise uniquement son identité unique pour s'identifier au Policy Manager Server.
Debug=1	`0` = Ne pas générer d'informations de débogage (valeur par défaut). `1` = Ecrire les informations de débogage dans le journal de débogage pendant l'installation et la désinstallation.
InstallMode=0 | 1	Ce composant est systématiquement installé lors de l'installation d'un client réseau. Il ne nécessite pas la modification des paramètres `RequestInstallMode` ou `InstallMode`.

[PMSUINST.DLL]	Paramètres pour la prise en charge de Policy Manager
RequestInstallMode=0	Ce composant est systématiquement installé lors de l'installation d'un client réseau. Il ne nécessite pas la modification des paramètres`RequestInstallMode` ou `InstallMode`.

[PMSUINST.DLL]	**Paramètres pour la prise en charge de Policy Manager**
FsmsServerUrl=http://fsmsserver	URL vers Policy Manager Server.
FsmsExtensionUri=/fsms/fsmsh.dll	Ne modifiez pas ce paramètre.
FsmsCommdirUri=/commdir	Ne modifiez pas ce paramètre.
Debug=1	`0` = Ne pas générer d'informations de débogage (valeur par défaut). `1` = Ecrire les informations de débogage dans le journal de débogage pendant l'installation et la désinstallation.
InstallMode=0 | 1	Ce composant est systématiquement installé lors de l'installation d'un client réseau. Il ne nécessite pas la modification des paramètres `RequestInstallMode` ou `InstallMode`.

[FSAVINST.DLL]	**Paramètres pour Client Security - Protection antivirus**
RequestInstallMode=1	`0` = Installer ce composant tel que défini dans le `InstallMode` paramètre. `1` = Installer si une version précédente de ce composant est détectée ou si aucune version n'est détectée (valeur par défaut). `2` = Installer ce composant si aucune version existante n'est installée, ou si la même version ou une version plus ancienne existe.
EnableRealTimeScanning=1	`0` = Désactiver l'analyse en temps réel `1` = Activer l'analyse en temps réel (valeur par défaut)
Debug=1	`0` = Ne pas générer d'informations de débogage (valeur par défaut). `1` = Ecrire les informations de débogage dans le journal de débogage pendant l'installation et la désinstallation.
InstallMode=0 | 1	`0` = Ne pas installer ce composant (valeur par défaut). `1` = Installer ce composant, sauf si une version plus récente existe déjà.

[FSSGSUP.DLL]	**Paramètres du module de détection et d'élimination des conflits**
RequestInstallMode=1	Ce composant est systématiquement exécuté à l'installation. Il ne nécessite pas la modification des

[FSSGSUP.DLL]	Paramètres du module de détection et d'élimination des conflits
	paramètres `RequestInstallMode` ou `InstallMode`.
Debug=0 | 1	`0` = Ne pas générer d'informations de débogage (valeur par défaut). `1` = Ecrire les informations de débogage dans le journal de débogage pendant l'installation et la désinstallation.
InstallMode=0 | 1	Ce composant est systématiquement exécuté à l'installation. Il ne nécessite pas la modification des paramètres `RequestInstallMode` ou `InstallMode`.
SidegradeAction=0	`0` = Il ne nécessite pas la modification des paramètres (valeur défaut). `1` = Annuler l'installation si un logiciel faisant conflit est installé.

[ES_Setup.DLL]	Paramètres d'installation de l'analyse de courrier électronique
RequestInstallMode=1	`0` = Installer ce composant tel que défini dans le `InstallMode` paramètre. `1` = Installer si une version précédente de ce composant est détectée ou si aucune version n'est détectée (valeur par défaut). `2` = Installer ce composant si aucune version existante n'est installée, ou si la même version ou une version plus ancienne existe.
Debug=0 | 1	`0` = Ne pas générer d'informations de débogage (valeur par défaut). `1` = Ecrire les informations de débogage dans le journal de débogage pendant l'installation et la désinstallation.
InstallMode=0 | 1	`0` = Ne pas installer ce composant (valeur défaut). `1` = Installer ce composant, sauf si une version plus récente existe déjà.

[FWESINST.DLL]	Paramètres pour le composant interne commun FWES.
RequestInstallMode=1	`0` = Installer ce composant tel que défini dans le `InstallMode` paramètre.

[FWESINST.DLL]	Paramètres pour le composant interne commun FWES.
	1 = Installer si une version précédente de ce composant est détectée ou si aucune version n'est détectée (valeur par défaut). 2 = Installer ce composant si aucune version existante n'est installée, ou si la même version ou une version plus ancienne existe.
Debug=0 | 1	0 = Ne pas générer d'informations de débogage (valeur par défaut). 1 = Ecrire les informations de débogage dans le journal de débogage pendant l'installation et la désinstallation.
InstallMode=0 | 1	0 = Ne pas installer ce composant (valeur par défaut). 1 = Installer ce composant, sauf si une version plus récente existe déjà.

[FWINST.DLL]	Paramètres de Client Security- Protection Internet
RequestInstallMode=1	0 = Installer ce composant tel que défini dans le`InstallMode` paramètre. 1 = Installer si une version précédente de ce composant est détectée ou si aucune version n'est détectée (valeur par défaut). 2 = Installer ce composant si aucune version existante n'est installée, ou si la même version ou une version plus ancienne existe.
Debug=0 | 1	0 = Ne pas générer d'informations de débogage (valeur par défaut). 1 = Ecrire les informations de débogage dans le journal de débogage pendant l'installation et la désinstallation.
InstallMode=0 | 1	0 = Ne pas installer ce composant (valeur par défaut). 1 = Installer ce composant, sauf si une version plus récente existe déjà.
InstallDC=0 | 1	0 = Ne pas installer le contrôle d'accès à distance (valeur par défaut). 1 = Installer le contrôle d'accès à distance
InstallNetworkQuarantine=0 | 1	0 = Ne pas installer la quarantaine réseau (valeur par défaut). 1 = Installer la quarantaine réseau.

[FWINST.DLL]	Paramètres de Client Security- Protection Internet
DisableWindowsFirewall=0 | 1	`0` = Ne pas installer le pare-feu Windows (sur XP SP2 ou versions ultérieures) (valeur par défaut). `1` = Désactiver le pare-feu Windows après l'installation de la protection Internet.

[FSBWINST.DLL]	Paramètres pour la prise en charge de Automatic Update Agent
RequestInstallMode=1	`0` = Installer ce composant tel que défini dans le `InstallMode` paramètre. `1` = Installer si une version précédente de ce composant est détectée ou si aucune version n'est détectée (valeur par défaut). `2` = Installer ce composant si aucune version existante n'est installée, ou si la même version ou une version plus ancienne existe.
InstallMode=0 | 1	`0` = Ne pas installer ce composant (valeur par défaut). `1` = Installer ce composant, sauf si une version plus récente existe déjà.

[FSPSINST.DLL]	Paramètres de Client Security- Analyseur de réseau
RequestInstallMode=1	`0` = Installer ce composant tel que défini dans le `InstallMode` paramètre. `1` = Installer si une version précédente de ce composant est détectée ou si aucune version n'est détectée (valeur par défaut). `2` = Installer ce composant si aucune version existante n'est installée, ou si la même version ou une version plus ancienne existe.
Debug=0 | 1	`0` = Ne pas générer d'informations de débogage (valeur par défaut). `1` = Ecrire les informations de débogage dans le journal de débogage pendant l'installation et la désinstallation.
InstallMode=0 | 1	`0` = Ne pas installer ce composant (valeur par défaut). `1` = Installer ce composant, sauf si une version plus récente existe déjà.
DisableScanningForApps= Wget.exe,mplayer.exe	Désactive l'analyse réseau pour certains exécutables. C'est une liste de noms d'exécutables sans chemin d'accès, utilisant la virgule comme séparateur.

[FSPSINST.DLL]	Paramètres de Client Security- Analyseur de réseau
	👉 **Remarque:** aucun espace n'est autorisé entre les éléments.
EnableHTTPScanning=1	`0` = Analyse HTTP désactivée `1` = Analyse HTTP activée
StartImmediatelyForApps= iexplore.exe,firefox.exe, netscape.exe,opera.exe, msimn.exe,outlook.exe, mozilla.exe	Ce paramètre définit les exécutables devant démarrer immédiatement l'analyse HTTP. Les autres processus passent en mode d'analyse uniquement après le premier accès à un port de serveur externe 80. C'est une liste de noms d'exécutables sans chemin d'accès, utilisant la virgule comme séparateur. 👉 **Remarque:** aucun espace n'est autorisé entre les éléments.

[FSNACINS.DLL]	Paramètres du plug-in Cisco NAC
RequestInstallMode=1	`0` = Installer ce composant tel que défini dans le `InstallMode` paramètre. `1` = Installer si une version précédente de ce composant est détectée ou si aucune version n'est détectée (valeur par défaut). `2` = Installer ce composant si aucune version existante n'est installée, ou si la même version ou une version plus ancienne existe.
CTAversion=1.0.55	`CTAversion` définit la version de l'agent d'approbation Cisco inclus dans le package. Le package d'installation de l'agent d'approbation Cisco peut être mis à jour en remplaçant le fichier`ctasetup.msi` dans le répertoire où réside le fichier`prodsett.ini`.
Debug=0 | 1	`0` = Ne pas générer d'informations de débogage (valeur par défaut). `1` = Ecrire les informations de débogage dans le journal de débogage pendant l'installation et la désinstallation.
InstallMode=0 | 1	`0` = Ne pas installer ce composant (valeur par défaut). `1` = Installer ce composant, sauf si une version plus récente existe déjà.

Chapitre
15

Messages d'alerte et d'erreur de l'analyse du courrier électronique

Sujets :

- *Messages d'erreur et d'alerte*

Cette section fournit une liste des messages d'alerte et d'erreur que l'analyse du courrier électronique génère.

Messages d'erreur et d'alerte

Vous trouverez ci-dessous une liste de messages générés par l'analyse du courrier électronique.

Titre du message	ID du message	Définition	Contenu du message
Echec de la session d'analyse du courrier électronique: erreur système	602		La connexion au serveur<nom du serveur> a été interrompue par l'analyse du courrier électronique en raison d'une erreur système. La fonction d'analyse du courrier électronique reste opérationnelle.
Dysfonctionnement de l'analyse du courrier électronique: erreur système	603		La fonction d'analyse du courrier électronique n'est pas opérationnelle en raison d'une erreur grave. Si le problème persiste, contactez l'administrateur système.
Echec du filtrage des messages de l'analyse du courrier électronique: erreur système	604		Impossible d'analyser un message en raison d'une erreur du système de filtrage des messages. La session n'a pas été annulée, mais le message concerné n'a pas été analysé.
Echec de l'initialisation de l'analyse du courrier électronique	610		Echec de l'initialisation de la fonction d'analyse du courrier électronique, motif: <pour obtenir la raison, voir ci-dessus>
Alerte	620-623	Lorsqu'un virus est détecté, il est traité en fonction de la configuration définie dans la configuration **avancée** F-Secure Client Security. Possibilités d'actions effectuées: • L'infection a uniquement été signalée.	Alerte : virus trouvé dans le courrier électronique. Infection : <Nom du virus> Pièce jointe : <Partie du message du courrier électronique, fichier joint qui était infecté> Action : <Action effectuée>

Titre du message	ID du message	Définition	Contenu du message
		• La pièce jointe a été nettoyée. • La pièce jointe a été supprimée. • Le message électronique infecté a été bloqué.	Message<ID du message> de : <En-tête du courrier électronique : adresse électronique de l'expéditeur> à : < En-tête du courrier électronique : adresses électroniques des destinataires> objet : < En-tête du courrier électronique : titre indiquant le sujet du message >
Alerte	630-633	Lorsqu'un message déformé est trouvé, il est traité en fonction de la configuration **avancée** de F-Secure Client Security. Possibilités d'actions effectuées: • La partie déformée du message a uniquement été signalée. • La partie déformée du message a été supprimée. • Le message électronique déformé a été bloqué.	Alerte : courrier électronique déformé. Description :<description de la déformation> Partie du message : <partie déformée du message> Action : <Action effectuée> Message< ID du message> de : <En-tête du courrier électronique : adresse électronique de l'expéditeur> à : < En-tête du courrier électronique : adresses électroniques des destinataires> objet : < En-tête du courrier électronique : titre indiquant le sujet du message >

Titre du message	ID du message	Définition	Contenu du message
Echec de l'analyse d'une pièce jointe à un message électronique	640-643	Lorsqu'une analyse échoue, le message est traité en fonction de la configuration définie dans la configuration **avancée**. Raisons de l'échec de l'analyse • Dépassement du délai d'analyse au niveau du fichier • Dépassement du délai d'analyse au niveau de la messagerie • Pièce jointe contenue dans un fichier zip protégé par mot de passe • Erreur à l'analyse de la pièce jointe (espace disque insuffisant, mémoire insuffisante, etc.) Possibilités d'actions effectuées • L'échec de l'analyse a uniquement été signalé. • La pièce jointe a été supprimée. • Le message a été bloqué.	Echec de l'analyse d'une pièce jointe à un message électronique Raison :`<Description de l'échec de l'analyse>` Pièce jointe : `<Pièce jointe ayant causé l'échec de l'analyse>` Action : `<Action effectuée>` Message`< ID du message>` de : `<En-tête du courrier électronique : adresse électronique de l'expéditeur>` à : `< En-tête du courrier électronique : adresses électroniques des destinataires>` objet : `< En-tête du courrier électronique : titre indiquant le sujet du message >`

Chapitre
16

Produits détectés ou supprimés lors de l'installation du client

Sujets :

- *Liste de produits*

Les produits répertoriés dans cette section sont soit détectés de sorte que l'utilisateur puisse les désinstaller manuellement, soit ils sont désinstallés automatiquement pendant le processus d'installation de F-SecureClient Security.

Liste de produits

Vous trouverez ci-dessous une liste des produits détectés et supprimés lors de l'installation.

- Agnitum Outpost Firewall Pro 1.0
- AOL Safety and Security Center
- avast! Antivirus
- AVG Anti-Virus 7.0
- AVG Free Edition
- AVG Anti-Virus 7.0
- AVG 7.5
- Avira AntiVir PersonalEdition Classic
- Avira AntiVir PersonalEdition Premium
- Avira AntiVir Windows Workstation
- Avira Premium Security Suite
- BitDefender Antivirus v10
- BitDefender Antivirus Plus v10
- BitDefender 8 Free Edition
- BitDefender 9 Internet Security
- BitDefender Internet Security v10
- BitDefender 9 Professional Plus
- BitDefender 9 Standard
- BitDefender Total Security 2008
- Bsecure Internet Protection Services v.4.5
- BullGuard 7.0
- CA Anti-Virus
- CA eTrust Antivirus
- eTrust EZ Antivirus
- EZ Firewall
- CA Internet Security Suite
- Pare-feu du client VPN Cisco
- VirusScan de Dr Solomon
- EarthLink Protection Control Center
- Logiciel EarthLink
- EarthLink Toolbar
- EMBARQ Toolbar (géré par EarthLink)
- PC Antivirus
- F-PROT Antivirus for Windows
- FortiClient
- F-Secure Anti-Spyware
- F-Secure Anti-Virus Client Security
- Produit F-Secure non compatible
- Produit endommagé ou désinstallé de façon incomplète
- Client F-Secure VPN+
- G DATA AntiVirenKit (version allemande uniquement)
- G DATA InternetSecurity (version allemande uniquement)
- G DATA TotalCare (version allemande uniquement)
- AntiVirenKit 2005
- H+BEDV AntiVir Personal Edition

- iProtectYou 7.09
- Jiangmin Antivirus Software (version anglaise uniquement)
- K7 TotalSecurity 2006
- Kaspersky Anti-Spam Personal
- Kaspersky Anti-Virus 6.0 (version anglaise uniquement)
- Kaspersky Internet Security 6.0 (version anglaise uniquement)
- Kaspersky Internet Security 6.0 (version anglaise uniquement)
- Kaspersky(TM) Anti-Virus Personal 4.0
- Kaspersky(TM) Anti-Virus Personal Pro 4.0
- Kaspersky(TM) Anti-Virus Personal 4.5
- Kaspersky Anti-Virus Personal Pro
- Kaspersky Anti-Virus Personal
- Kerio Personal Firewall
- Kingsoft Internet Security (version anglaise uniquement)
- McAfee SecurityCenter
- McAfee VirusScan
- McAfee VirusScan Enterprise
- McAfee VirusScan Home Edition
- McAfee Internet Security
- McAfee Uninstall Wizard
- McAfee Personal Firewall
- McAfee Personal Firewall Plus
- McAfee Privacy Service
- McAfee SecurityCenter
- McAfee SpamKiller
- McAfee VirusScan Professional Edition
- McAfee Total Protection
- McAfee Browser Protection Service
- McAfee Virus and Spyware Protection Service
- McAfee Personal Firewall Express
- McAfee Firewall Protection Service
- McAfee Firewall
- Windows Live OneCare
- Agent NAI ePolicy Orchestrator
- NIC v5.50
- Norman Personal Firewall 1.42
- Norman Virus Control
- Système antivirus NOD32 (versions en anglais, français, allemand, hongrois, roumain et espagnol, chinois simplifiée, chinois traditionnel, tchéque, croate, italien, japonais, néerlandais, polonais, portugais, russe et slovène uniquement)
- PureSight Parental Control
- Radialpoint Security Services
- Radialpoint Servicepoint Agent 1.5.11
- Sophos Anti-Virus
- Sophos AutoUpdate
- Sophos Remote Management System
- Sunbelt Personal Firewall
- Norton AntiVirus 2003
- Norton AntiVirus 2005
- Norton 360

- Norton AntiVirus 2004 (Symantec Corporation)
- Norton AntiVirus
- Norton AntiVirus Corporate Edition
- Norton Internet Security
- Norton Internet Security 2005
- Norton Internet Security 2006 (Symantec Corporation)
- Norton Internet Security 2007
- Norton Internet Security 2008
- Norton Security Online
- Norton SystemWorks 2004 Professional (Symantec Corporation)
- Norton SystemWorks 2005 (Symantec Corporation)
- Norton Personal Firewall (Symantec Corporation)
- Norton Personal Firewall 2005
- Symantec AntiVirus
- Symantec AntiVirus Client
- Symantec Client Security
- Symantec Endpoint Protection
- LiveUpdate 1.7 (Symantec Corporation)
- LiveUpdate 1.80 (Symantec Corporation)
- LiveUpdate 2.6 (Symantec Corporation)
- LiveUpdate 1.6 (Symantec Corporation)
- LiveUpdate
- LiveUpdate 2.0 (Symantec Corporation)
- LiveUpdate 3.3 (Symantec Corporation)
- Panda Antivirus 2007
- Panda Antivirus + Firewall 2007
- Panda ClientShield
- Panda Internet Security 2008
- Panda Antivirus Platinum
- Panda Platinum Internet Security
- Panda Platinum 2005 Internet Security (version anglaise uniquement)
- Panda Platinum 2006 Internet Security
- Panda Internet Security 2007
- Panda Titanium Antivirus 2004
- Panda Titanium Antivirus 2005 (versions en anglais, français et anglais uniquement)
- Panda Titanium 2006 Antivirus + Antispyware
- Trend Micro Officescan (Windows 2000 uniquement)
- Trend Micro OfficeScan Client
- PC-cillin 2003
- Trend Micro PC-cillin Internet Security 12
- Trend Micro PC-cillin Internet Security 2005
- Trend Micro PC-cillin Internet Security 2006
- Trend Micro Internet Security
- Trend Micro AntiVirus 2007
- Trend Micro PC-cillin Internet Security 2007
- Trend Micro Internet Security Pro
- ZoneAlarm
- ZoneAlarm Security Suite
- ZoomTownInternetSecurity v.4.5